МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра информационной безопасности

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

По направлению подготовки 10.03.01 «Информационная безопасность»
профиль Безопасность автоматизированных систем

Уровень квалификации выпускника (*бакалавр*)
Форма обучения (*очная*)

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Организация защиты персональных данных
Рабочая программа дисциплины

Составитель:
к.и.н., доцент, заведующая кафедрой
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры информационной безопасности
№ 10 от 20.05.2021

ОГЛАВЛЕНИЕ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Пояснительная записка

Цель курса: формирование знаний и умений по организации проведения комплекса мероприятий по обеспечению конфиденциальности обработки персональных данных с использованием правовых, организационных и организационно-технических мер, способы снижения рисков утечки персональных данных и наложения штрафных санкций со стороны государственных регуляторов. На практических примерах разобраться в действиях операторов персональных данных в рамках трудовых отношений с собственным персоналом, гражданско-правовых отношениях, связанных с передачей и представлением персональных данных третьим лицам, в том числе органам государственной власти.

Задача курса:

- сформировать знания базовых теоретических понятий, лежащих в основе по обеспечению конфиденциальности обработки персональных данных;
- овладеть комплексом мероприятий по обеспечению конфиденциальности обработки персональных данных с использованием правовых, организационных и организационно-технических мер;
- овладеть практическими вопросами защиты персональных данных;
- овладеть необходимой юридической терминологией;
- сформировать умение разработать внутренние локальные нормативные документы по обеспечению конфиденциальности обработки и защиты персональных данных ;
- сформировать умение провести классификацию информационных систем, создать модели угроз, описать систему защиты, подготовить уведомление в уполномоченный орган по защите прав субъектов персональных данных.

1.1. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине *(модулю)*:

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-4.1 - Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;	*ОПК-4.1.1 Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации*	Знать: базовые международные и российские регуляторы по информационной безопасности; Уметь: работать со стандартами и нормативными документами; Владеть: навыками использования международных и национальных стандартов в

		своей профессиональной деятельности Знать сущность информации, методы и способы её отражения и передачи; Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов Владеть: навыками использовать основы правовых знаний в различных сферах деятельности
	ОПК-4.1.2 Умеет разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при ее эксплуатации (включая управление инцидентами информационной безопасности)	
	ОПК-4.1.3 Владеет навыками планирования мероприятий по обеспечению защиты информации и организацию работы персонала автоматизированной системы с учетом требований по защите информации	
ПК-10 - Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10.1 Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Знать: навыками по моделированию источников угроз и угроз безопасности объектов информатизации Уметь: организовать работу по обеспечению безопасности объектов информатизации от воздействия источников угроз и угроз. Владеть: состава и порядка разработки нормативных документов по обеспечению безопасности объектов информатизации.
	ПК-10.2 Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации	
	ПК-10.3 Владеет навыком	

	разработки аналитического обоснования необходимости создания системы защиты информации в организации	
ПК-11 - Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	ПК-11.1 Знает методики проведения теоретических исследований уровней защищенности информационной безопасности объектов и систем	Знать: особенности практической деятельности всех перечисленных в Гражданском кодексе РФ юридических лиц, классифицируемых по основной цели деятельности, организационно-правовой форме и характеру прав, возникающих у их учредителей (участников) в связи с участием последних в образовании имущества учреждаемого ими юридического лица; Уметь: осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм Владеть: способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю
	ПК-11.2 Умеет составлять и оформлять аналитический отчет по проведенным испытаниям, делать выводы по оценке защищенности на основании аналитического отчета	
	ПК-11.3 Владеет навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищенности	

1.1.Место дисциплины в структуре основной образовательной программы

Дисциплина (модуль) «Защита персональных данных» входит в вариативную часть по выбору студента цикла дисциплин подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность». Дисциплина реализуется кафедрой Информационной безопасности.

Для освоения дисциплины (модуля) необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Основы управленческой деятельности», «Основы информационной безопасности»,

«Организационное и правовое обеспечение информационной безопасности», «Информационная безопасность автоматизированных систем».

В результате освоения дисциплины (модуля) формируются знания, умения и владения, необходимые для прохождения дисциплин «Управление информационной безопасностью» и «Аттестация объектов информатизации».

2. Структура дисциплины (модуля) для очной формы обучения

Общая трудоёмкость дисциплины составляет 3 з.е.,114 ч., в том числе контактная работа обучающихся с преподавателем 60 ч., самостоятельная работа обучающихся 36 ч. , контроль – 18ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятель-ная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Введение.	5	2		-			2	Опрос
2	Общая характеристика института защиты персональных данных	5	4		6			4	Опрос
3	Основные понятия, термины и определения в соответствии с ФЗ "О персональных данных" от 27 июля 2006 г., № 152-ФЗ	5	4		6			6	Опрос
4	Основные понятия и определения в соответствии с Главой 14 Трудового кодекса Российской Федерации от 30 декабря 2001 года № 197-ФЗ	5	4		6			6	Опрос
5	Нормативные документы Федеральных органов власти в области защиты персональных данных и порядок работы с персональными данными на предприятии	5	4		6			6	Опрос Ситуационная задача
6	Организационно-техническая защита персональных данных в информационных системах	5	2		6			6	Опрос Тестирование
7	Лицензирование	5	4		6			6	Опрос

	деятельности по технической защите конфиденциальной информации								
8	экзамен	5					18		Итоговая контрольная работа
	Итого		**24**		**36**		**18**	**36**	

3. Содержание дисциплины (модуля)

№	Наименование раздела дисциплины	Содержание
	Тема 1. ВВЕДЕНИЕ	Предмет, задачи и содержание дисциплины, методы изучения. Защита персональных данных как один из инструментов обеспечения безопасности организации в решении проблем, возникших перед российскими предприятиями в связи с принятием Федерального закона «О персональных данных». Взаимосвязь дисциплины с правовыми, организационными, экономическими, социальными, социально-психологическими и техническими дисциплинами учебного плана по направлению подготовки 090900 «Информационная безопасность». Разделы программы, тематика лекций и занятий, календарный план их изучения. Методика самостоятельной работы студентов по изучению дисциплины. Формы проверки знаний. Источники и литература.
	Тема 2. ОБЩАЯ ХАРАКТЕРИСТИКА ИНСТИТУТА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ	Международное законодательство и национальное законодательство зарубежных стран о защите персональных данных. Защита персональных данных как реализация конституционных прав граждан на неприкосновенность частной жизни. Персональные данные как юридическая категория. Общие положения законодательной и нормативно-правовой базы Российской Федерации в области защиты конфиденциальной информации
	Тема 3. ОСНОВНЫЕ ПОНЯТИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ В СООТВЕТСТВИИ С ФЗ "О ПЕРСОНАЛЬНЫХ ДАННЫХ"	Основные понятия. Персональные данные в Федеральном законе «О персональных данных». Содержание категории «персональные данные». Область применения закона и установленные

	ОТ 27 ИЮЛЯ 2006 Г., №152-ФЗ.	ограничения. Соотношение персональных данных с другими категориями конфиденциальной информации. Персональные данные и их взаимосвязь с государственной, коммерческой, налоговой, банковской, адвокатской тайной, тайной связи и другими категориями конфиденциальных сведений. Принципы обработки персональных данных. Обработка персональных данных: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (передача), обезличивание, блокирование, уничтожение. Условия обработки персональных данных с согласия субъекта. Обработка биометрических данных. Обработка персональных данных третьим лицом в интересах оператора. Трансграничная передача персональных данных. Специальные категории персональных данных и особенности их обработки. Права субъектов персональных данных и их соблюдение при обработке. Обязанности оператора персональных данных в ходе сбора и обработки персональных данных, ответы на запросы субъектов. Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований по обращению с персональными данными.
	Тема 4. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ В СООТВЕТСТВИИ ГЛАВОЙ 14 ТРУДОВОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 30 ДЕКАБРЯ 2001 ГОДА N 197-ФЗ	Понятие персональных данных работника. Обработка персональных данных работника на предприятии. Общие требования при обработке персональных данных работника и гарантии их защиты. Хранение и использование персональных данных работников на предприятии. Передача персональных данных работника в пределах одной организации. Передача персональных данных работника третьей стороне. Права работников в целях обеспечения защиты персональных данных, хранящихся у

		работодателя. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника.
	Тема 5. НОРМАТИВНЫЕ ДОКУМЕНТЫ ФЕДЕРАЛЬНЫХ ОРГАНОВ ВЛАСТИ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПОРЯДОК РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ НА ПРЕДПРИЯТИИ	Компетенции уполномоченного органа по защите прав субъектов персональных данных. Мероприятия по защите сведений конфиденциального характера. Практические шаги по приведению порядка обработки в соответствие с требованиями законодательства. Правовые основания обработки персональных данных. Получение согласия субъектов на обработку. Содержание договоров с субъектами в части обработки персональных данных. Формирование перечня персональных данных. Ограничение доступа к персональным данным. Учет лиц, допущенных к персональным данным. Определение порядка обращения с такими сведениями, контроля за его соблюдением. Организация доступа пользователей к ИСПДн. Внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие. Особенности обработки персональных данных при обработке в информационных системах персональных данных. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Подготовка уведомлений об обработке персональных данных в уполномоченный орган. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.
	Тема 6. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ	Требования Федерального закона и Постановления Правительства РФ 2007 г. №781 к обеспечению безопасности персональных данных. Обязательные механизмы защиты. Порядок классификации информационных систем персональных данных. Организационно-технические мероприятия оператора по защите персональных данных.

		Модель угроз персональным данным. Типовая модель угроз. Перечень источников угроз. Уровень исходной защищенности. Методика актуализации угроз. Каналы утечки информации при обработке персональных данных в информационных системах. Обеспечение безопасности персональных данных в ИСПДн. Контроль за безопасностью обработки персональных данных. Разбирательство нарушений системы безопасности.
	Тема 7. ЛИЦЕНЗИРОВАНИЕ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ	Понятие технической защиты как лицензируемого вида деятельности. Лицензионные требования по обработке конфиденциальной информации, в том числе персональных данных. Проверка сведений о лицензиате и лицензионный контроль за деятельность, связанную с обработкой персональных данных. Ответственность за незаконную деятельность в области защиты информации. Незаконное предпринимательство. Оценка и управление риском, связанным с отсутствием лицензии на техническую защиту конфиденциальной информации, обработку персональных данных.

4. Образовательные технологии

При реализации рабочей программы дисциплины «Организация защиты персональных данных» используются следующие образовательные технологии:

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Введение.	Лекция 1.	Лекция. Дискуссия.
2	Общая характеристика института защиты персональных данных	Лекция 2. Практическое занятие 1.	Лекция. Выполнение практического задания по методу анализа конкретных

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
			ситуаций (АКС)
3	Основные понятия, термины и определения в соответствии с ФЗ "О персональных данных" от 27 июля 2006 г., № 152-ФЗ	Лекция 3. Практическое занятие 2.	Лекция. Выполнение практического задания по методу анализа конкретных ситуаций (АКС)
4	Основные понятия и определения в соответствии с Главой 14 Трудового кодекса Российской Федерации от 30 декабря 2001 года № 197-ФЗ	Лекция 4. Практическое занятие 3.	Лекция. Выполнение практического задания по методу анализа конкретных ситуаций (АКС)
5	Нормативные документы Федеральных органов власти в области защиты персональных данных и порядок работы с персональными данными на предприятии	Лекция 5. Практическое занятие 4.	Лекция. Выполнение практического задания по методу анализа конкретных ситуаций (АКС)
6	Организационно-техническая защита персональных данных в информационных системах	Лекция 6. Практическое занятие 5.	Лекция. Выполнение практического задания по методу анализа конкретных ситуаций (АКС)
7	Лицензирование деятельности по технической защите конфиденциальной информации	Лекция 7. Практическое занятие 6.	Лекция. Выполнение практического задания по методу анализа конкретных ситуаций (АКС)

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Система текущего и промежуточного контроля знаний студентов по дисциплине «Организация защиты персональных данных» предусматривает следующее распределение:

за работу на практических занятиях по темам №№ 2-7 – до 3 баллов за каждое занятие;

за работу на практических занятиях – по теме № 5 - до 4 баллов за каждое занятие;

за контрольную работу – до 11 баллов

за тестирование – 15 баллов

за итоговую работу – до 40 баллов

Итого: 100 баллов за семестр (дисциплину).

Тестирование проводится после изучения темы № 4.

Контрольная работа проводится после изучения темы № 7.

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	*Контролируемые разделы дисциплины*	*Код контролируемой компетенции*	*Наименование оценочного средства*
1.	1-3	ОПК-4.1; ПК-10; ПК-11	План практического занятия
2.	4-5	ОПК-4.1; ПК-10; ПК-11	План практического занятия
3.	6-7	ОПК-4.1; ПК-10; ПК-11	Тест План практического занятия Контрольная работа

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной,

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		сформированы на уровне – «высокий».
82-68/ C	зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D, E	зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F, FX	не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине *(модулю)*

Текущий контроль (вариант опросного задания)

Вопросы	***Реализуемая компетенция***
1. Какие гарантии защиты персональных данных работников установлены ТК РФ?	ОПК-4.1; ПК-10; ПК-11
2. В процессе переезда из одного административного здания в другое была испорчена (нарушена целостность обложки и листов, размыты печати и частично текст) трудовая книжка Иванова И.И. Какие действия должна предпринять администрация предприятия? Нарушены ли права обладателя трудовой книжки? Какие требования должен/может предъявить Иванов И.И. к администрации предприятия?	ПК-5; ПК-10; ПК-11; ПК-15
3. В ходе предоставления в налоговую инспекцию персональных данных на Кирилова А.И. сотрудники отдела кадров попросил дать расписку о не возражении по этому факту. Кирилов А.И. уведомил в устной речи об отказе от своих прав на сохранение и защиту своих персональных данных, так как, его имя и так достаточно известно. Все эти данные можно найти в различных публичных изданиях, а также в Интернете. Как должна повести себя администрация в связи с таким заявлением Кирилова А.И.? Имеет ли право Кирилов А.И. отказаться от своих прав на сохранение и защиту своих персональных данных? Обосновать.	ОПК-4.1; ПК-10; ПК-11

Текущий контроль (вариант теста) – проверка сформированности компетенций - ОПК-4.1; ПК-10; ПК-11

1. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных утверждены…….?

Укажите номер правильного ответа

1. Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119
2. Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17
3. Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21
4. Приказом Федеральная служба безопасности Российской Федерации от 10 июля 2014 г. № 378

2. Требования к защите персональных данных при их обработке в информационных системах персональных данных утверждены….?

Укажите номер правильного ответа

1. Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119
2. Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17

3. Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21
4. Приказом Федеральная служба безопасности Российской Федерации от 10 июля 2014 г. № 378

3. Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные…..

Укажите номер правильного ответа

1. Субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных»
2. Касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных
3. Только сотрудников работающих в этой информационной системе
4. Которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных

4. Кто обеспечивает безопасность персональных данных при их обработке в информационной системе ?

Укажите номер правильного ответа

1. Обладатель информации или заказчик информации,
2. Оператор этой системы, который обрабатывает персональные данные или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора
3. Обладатель информации или лицо, осуществляющее обработку персональных данных.
4. Любой из сотрудников, работающих в информационной системе

5. Под актуальными угрозами безопасности персональных данных понимается…..

Укажите номер правильного ответа

1. Условия и факторы, создающие актуальную опасность несанкционированного доступа к персональным данным
2. Совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия
3. Действия (бездействия) которые могут способствовать уничтожению, изменению, блокированию, копированию, распространению персональных данных
4. Оценка возможного вреда информационной системе

6. Для обеспечения защиты информации, содержащейся в информационной системе, проводятся мероприятия по…….

Укажите номер правильного ответа

1 Разработке системы защиты информации информационной системы
1. Реализации правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия

пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения
2. Проверке полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер защиты информации;
3. Отработке действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

7. Кто формирует требования к защите информации, содержащейся в информационной системе?

Укажите номер правильного ответа

1. Оператор
2. Проектировщик
3. Заказчик
4. Руководитель подразделения

8. Ввод в действие информационной системы осуществляется в соответствии с……

Укажите номер правильного ответа

1. Приказом руководителя организации
2. Заключением аттестационной комиссии
3. Законодательством Российской Федерации об информации, информационных технологиях и о защите информации, с учетом ГОСТ 34.601 и при наличии аттестата соответствия
4. Приказом Директора Федеральной службы по техническому и экспортному контролю

9. Меры по регистрации событий безопасности должны обеспечивать...

Укажите номер правильного ответа

1. Управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил
2. Сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них
3. Установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения
4. Обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия

Примерные темы курсовых работ - *проверка сформированности компетенций* ОПК-4.1; ПК-10; ПК-11

Понятие и классификация персональных данных. Персональные данные как юридическая категория

1. Международное законодательство в области защиты персональных данных
2. Национальное законодательство зарубежных стран о защите персональных данных

3. Защита персональных данных как реализация конституционных прав граждан на неприкосновенность частной жизни

4. Общие положения законодательной и нормативно-правовой базы Российской Федерации в области защиты конфиденциальной информации

5. Персональные данные в Федеральном законе «О персональных данных» и Трудовом кодексе РФ.

6. Содержание категории «персональные данные». Соотношение персональных данных с другими категориями конфиденциальной информации

7. Персональные данные и их взаимосвязь с государственной, коммерческой, налоговой, банковской, адвокатской тайной, тайной связи и другими категориями конфиденциальных сведений

8. Принципы и условия обработки персональных данных. Специальные категории персональных данных и особенности их обработки

9. Трансграничная передача персональных данных

10. Контроль и надзор за обработкой персональных данных

11. Понятие персональных данных работника в соответствии Главой 14 Трудового кодекса Российской Федерации

12. Требования при обработке и хранения персональных данных работника на предприятии и гарантии их защиты

13. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя

14. Порядок работы с персональными данными на предприятии

15. Мероприятия по защите сведений конфиденциального характера, основные локальные нормативные документы. Меры по охране конфиденциальности

16. Формирование перечня персональных данных. Разрешительная система доступа к персональным данным

17. Локальные нормативные документы по защите конфиденциальности сведений, их содержание, порядок разработки и ввода в действие

18. Контроль за соблюдением режима конфиденциальности на предприятии

19. Персональные данные в системе документооборота предприятия. Порядок организации конфиденциального делопроизводства по обработке персональных данных работника

20. Персональные данные в автоматизированных системах и приложениях. Подготовка уведомлений об обработке персональных данных в уполномоченный орган

21. Основные положения по обеспечению безопасности персональных данных при их обработке в информационных системах, обязательные механизмы защиты

22. Классификация информационных систем персональных данных

23. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

24. Каналы утечки информации при обработке персональных данных в информационных системах

25. Предотвращение несанкционированного доступа к персональным данным и обнаружение фактов такого доступа

26. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним

27. Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных

28. Контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией

29. Ответственность за нарушение требований по обращению с персональными данными; за нарушение норм, регулирующих обработку и защиту персональных данных работника

Курсовые работы являются составной частью самостоятельной учебно-исследовательской работы студента и предназначены для углубленного изучения дисциплин учебного плана, развития индивидуальных творческих способностей студента.

Цель курсовой работы – подготовка к самостоятельному решению задач, связанных с организационным процессом защиты персональных данных.

Достижение цели курсового проектирования осуществляется за счет решения задач по разработке построения системы защиты персональных данных на объекте информатизации, выполняемых во взаимосвязанной последовательности из ряда тем:

Порядок обработки персональных данных в соответствие с требованиями законодательства

Правовые основания обработки персональных данных. Получение согласия субъектов на обработку. Содержание договоров с субъектами в части обработки персональных данных.

Формирование перечня персональных данных.

Ограничение доступа к персональным данным. Организация доступа пользователей к ИСПДн.

Учет лиц, допущенных к персональным данным.

Определение порядка обращения с персональными данными.

Контроля за обработкой персональных данных.

Задачами преподавателя по проверке курсовой работы:

– оценить уровень овладения студентом профессиональными компетенциями;

– проверить подготовленность студента к выполнению выпускной квалификационной работы.

Задачами работы студента над курсовыми работами являются:

- углубленное изучение выбранной темы;
- приобретение умения вести поиск необходимого фактического материала, его анализа и систематизации, формулирования научных целей и выводов;
- развития навыков грамотного и логически доказательного изложения текста;
- получение опыта правильного оформления научной работы.

Курсовая работа представляет собой исследование по одной из научных проблем или отдельной теме учебной дисциплины.

Курсовая работа может быть написана как одна из глав будущей дипломной работы студента. По содержанию курсовая работа может иметь как теоретический, так и прикладной характер. Научный материал, который студент должен использовать при написании курсовой работы, отбирается индивидуально по каждой теме.

Тема курсовой работы может развивать и углублять тему ранее написанного студентом реферата.

Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Курсовая работа	Самостоятельная работа	Работа с литературой

Система оценивания

Форма контроля	Количество баллов
Содержание работы соответствует выбранной теме, раскрывает ее полно и всесторонне, демонстрирует свободное владение материалом	30
Использована обязательная и дополнительная литература, соответствующие информационные ресурсы	10
Работа написана грамотным литературным языком с соблюдением стилистических норм и корректным использованием профессиональной терминологии.	10

Структура работы соответствует плану, обнаруживает стройную логическую последовательность разделов.	10
Оформление соответствует актуальным требованиям к оформлению курсовой работы.	20
Защита курсовой работы	20
Итого оценка за курсовую работу	100

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

Требования к оформлению курсовой работы содержатся в Методических рекомендациях «Порядок подготовки, оформления и защиты курсовых и выпускных квалификационных работ (с различными видами доступа) для направления подготовки 10.03.01 «Информационная безопасность» (квалификация (степень) «бакалавр») профили: «Организация и технология защиты информации» и «Комплексная защита объектов информатизации», М.: РГГУ, 2016 г.

Промежуточная аттестация (примерные контрольные вопросы по курсу) - проверка сформированности компетенций ОПК-4.1; ПК-10; ПК-11

1. Понятие и классификация персональных данных.
2. Персональные данные как юридическая категория.
3. Международное законодательство в области защиты персональных данных.
4. Национальное законодательство зарубежных стран о защите персональных данных.
5. Защита персональных данных как реализация конституционных прав граждан на неприкосновенность частной жизни.
6. Общие положения законодательной и нормативно-правовой базы Российской Федерации в области защиты конфиденциальной информации.
7. Персональные данные в Федеральном законе «О персональных данных» и Трудовом кодексе РФ.
8. Содержание категории «персональные данные». Соотношение персональных данных с другими категориями конфиденциальной информации.
9. Персональные данные и их взаимосвязь с государственной, коммерческой, налоговой, банковской, адвокатской тайной, тайной связи и другими категориями конфиденциальных сведений.
10. Принципы обработки персональных данных.
11. Особенности обработки персональных данных.

12. Условия обработки персональных данных с согласия субъекта. Обработка биометрических данных.

13. Обработка персональных данных третьим лицом в интересах оператора.

14. Трансграничная передача персональных данных.

15. Специальные категории персональных данных и особенности их обработки.

16. Контроль и надзор за обработкой персональных данных.

17. Понятие персональных данных работника в соответствии Главой 14 Трудового кодекса Российской Федерации.

18. Общие требования при обработке персональных данных работника на предприятии и гарантии их защиты.

19. Хранение и использование персональных данных работников на предприятии.

20. Передача персональных данных работника третьей стороне.

21. Права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя.

22. Работа с персональными данными на предприятии.

23. Мероприятия по защите сведений конфиденциального характера, основные локальные нормативные документы. Меры по охране конфиденциальности.

24. Формирование перечня персональных данных

25. Разрешительная система доступа к персональным данным.

26. Локальные нормативные документы по защите конфиденциальности сведений, их содержание, порядок разработки и ввода в действие.

27. Контроль за соблюдением режима конфиденциальности на предприятии.

28. Персональные данные в системе документооборота предприятия. Порядок организации конфиденциального делопроизводства по обработке персональных данных работника.

29. Особенности учета и уничтожения бланков строгой отчетности.

30. Персональная ответственность за обеспечением защиты персональных данных работника.

31. Персональные данные в автоматизированных системах и приложениях. Подготовка уведомлений об обработке персональных данных в уполномоченный орган.

32. Основные положения по обеспечению безопасности персональных данных при их обработке в информационных системах, обязательные механизмы защиты.

33. Классификация информационных систем персональных данных.

34. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

35. Каналы утечки информации при обработке персональных данных в информационных системах.

36. Предотвращение несанкционированного доступа к персональным данным и обнаружение фактов такого доступа.

37. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

38. Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.

39. Контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

40. Ответственность за нарушение требований по обращению с персональными данными; за нарушение норм, регулирующих обработку и защиту персональных данных работника.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

а) источники

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (принят ГД ФС РФ 21.12.2001), Глава 14. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34683/

Федеральный закон от 19.12.2005 N 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_57153/

Федеральный закон от 27.07.2004 N 79-ФЗ "О государственной гражданской службе Российской Федерации", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48601/

Указ Президента Российской Федерации от 06.03.97 № 188 “Об утверждении перечня сведений конфиденциального характера”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_13532/

Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_75586/

Указ Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении положения о персональных данных государственного служащего Российской Федерации и ведения его личного дела», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_53747/

Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) "О сертификации средств защиты информации", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_7054/

"Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008), Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_99662/

Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/#dst100009

"Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСТЭК РФ 14.02.2008), Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_77814/

б) основная литература:

Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом : учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - ISBN 978-5-9275-2501-0. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1021578

б) дополнительная литература

Курникова И.А. Доступ к персональным данным: законодательство и практика (отечественный и зарубежный опыт). Методическое пособие. М.: Росархив, ВНИИДАД, 2005, 128 с.

Корнеев И.К., Степанов Е.А., «Защита информации в офисе», Учебник. М.-ООО «ТК Велби» Изд-во Проспект, 2008. – 336 с

Лагутина Т.М., Тимофеева С.В. Конфиденциальность информации. Тайна сведений. Справочник для работника, работодателя и кадровой службы. – СПб, «Издательский дом Герда», 2009. – 464 с.

Степанов Е.А., И.К.Корнеев Информационная безопасность и защита информации. Учебное пособие. – М.: ИНФРА-М, 2001 – 304 с – (Серия «Высшее образование»)

6.2. Перечень БД и ИСС

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7. Материально-техническое обеспечение дисциплины/модуля

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащен

Перечень ПО

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

- для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:

- устройством для сканирования и чтения с камерой SARA CE;
- дисплеем Брайля PAC Mate 20;
- принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;

- акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемыми эргономическими партами СИ-1;

- компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий - *проверка сформированности компетенций* ОПК-4.1; ПК-10; ПК-11

Планы практических занятий

Практическое задание 1. (Тема 2.). Общая характеристика института защиты персональных данных **- (2 часа) - *проверка сформированности компетенций*** ОПК-4.1; ПК-10; ПК-11

Вопросы для изучения и обсуждения:

1. Международное законодательство зарубежных стран о защите персональных данных.

2. Национальное законодательство зарубежных стран о защите персональных данных.

3. Персональные данные как юридическая категория.

Контрольные вопросы:

1. Каковы особенности защиты персональных данных как реализация конституционных прав граждан на неприкосновенность частной жизни?
2. Каковы положения законодательной базы Российской Федерации в области защиты конфиденциальной информации?
3. Какова нормативно-правовая база Российской Федерации в области защиты конфиденциальной информации?

Список источников и литературы:

а) источники

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (принят ГД ФС РФ 21.12.2001), Глава 14. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34683/

Федеральный закон от 19.12.2005 N 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_57153/

б) основная литература:

Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом : учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - ISBN 978-5-9275-2501-0. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1021578

Практическое задание 2. (Тема 3.). Основные понятия, термины и определения в соответствии с ФЗ "О персональных данных" от 27 июля 2006 г., № 152-ФЗ **- (4 часа) -** ***проверка сформированности компетенций*** **-** ОПК-4.1; ПК-10; ПК-11

Вопросы для изучения и обсуждения:

1. Область применения закона "О персональных данных" от 27 июля 2006 г., №152-ФЗ и установленные ограничения.

2. Соотношение персональных данных с другими категориями конфиденциальной информации.

3. Контроль и надзор за обработкой персональных данных.

Контрольные вопросы:

1. Каковы принципы обработки персональных данных?

2. Каковы условия обработки персональных данных?

3. Каковы обязанности оператора персональных данных в ходе сбора и обработки персональных данных?

4. Какие специальные категории персональных данных вы знаете?

5. Какова ответственность за нарушение требований по обращению с персональными данными?

Список источников и литературы:

а) источники

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

Практическое задание 3. (Тема 4.). Основные понятия и определения в соответствии с Главой 14 Трудового кодекса Российской Федерации от 30 декабря 2001 года № 197-ФЗ **- (4 часа) -** ***проверка сформированности компетенций*** **-** ОПК-4.1; ПК-10; ПК-11

Вопросы для изучения и обсуждения:

1. Общие требования при обработке персональных данных работника.

2. Передача персональных данных работника третьей стороне.

3. Права работников в целях обеспечения защиты персональных данных.

Контрольные вопросы:

1. Что понимается под обработкой персональных данных работника на предприятии?

2. Каков порядок хранения и использования персональных данных работников на предприятии?

3. Как осуществляется передача персональных данных работника в пределах одной организации?

4. Какова ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника на предприятии.

Список источников и литературы:

а) источники

Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (принят ГД ФС РФ 21.12.2001), Глава 14. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34683/

Федеральный закон от 19.12.2005 N 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_57153/

Федеральный закон от 27.07.2004 N 79-ФЗ "О государственной гражданской службе Российской Федерации", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48601/

Курникова И.А. Доступ к персональным данным: законодательство и практика (отечественный и зарубежный опыт). Методическое пособие. М.: Росархив, ВНИИДАД, 2004, 128 с.

Практическое задание 4. (Тема 5.). Нормативные документы Федеральных органов власти в области защиты персональных данных и порядок работы с персональными данными на предприятии **- (4 часа) -** ***проверка сформированности компетенций*** **-** ОПК-4.1; ПК-10; ПК-11

Вопросы для изучения и обсуждения:

1. Компетенции уполномоченного органа по защите прав субъектов персональных данных.

2. Практические шаги по приведению порядка обработки в соответствие с требованиями законодательства.

3. Формирование перечня персональных данных.

Контрольные вопросы:

1. Каков порядок доступа к персональным данным на предприятии?

2. Каково содержание договоров с субъектами в части обработки персональных данных?

3. Каковы внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие?

4. Каковы особенности обработки персональных данных при обработке в информационных системах персональных данных.

Список источников и литературы:

а) источники

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

Федеральный закон от 27.07.2004 N 79-ФЗ "О государственной гражданской службе Российской Федерации", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48601/

Указ Президента Российской Федерации от 06.03.97 № 188 “Об утверждении перечня сведений конфиденциального характера”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_13532/

Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_75586/

Указ Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении положения о персональных данных государственного служащего Российской Федерации и ведения его личного дела», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_53747/

Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) "О сертификации средств защиты информации", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_7054/

"Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008), Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_99662/

Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/#dst100009

"Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСТЭК РФ 14.02.2008), Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_77814/

Практическое задание 5. (Тема 6.). Организационно-техническая защита персональных данных в информационных системах **- (2 часа) -** ***проверка сформированности компетенций*** ОПК-4.1; ПК-10; ПК-11

Вопросы для изучения и обсуждения:

1. Порядок классификации информационных систем персональных данных.

2. Организационно-технические мероприятия оператора по защите персональных данных.

3. Модель угроз персональным данным. Типовая модель угроз. Перечень источников угроз. Уровень исходной защищенности. Методика актуализации угроз.

Контрольные вопросы:

1. Какие каналы утечки информации при обработке персональных данных в информационных системах вы знаете?

2. Каковы обязательные механизмы защиты в соответствии с Постановления Правительства РФ 2007 г. №781?

3. Каков порядок разбирательств по нарушению системы безопасности?

Список источников и литературы:

а) источники

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_75586/

Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) "О сертификации средств защиты информации", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_7054/

"Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008), Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_99662/

Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/#dst100009

"Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСТЭК РФ 14.02.2008), Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_77814/

Практическое задание 6. (Тема 7.). Лицензирование деятельности по технической защите конфиденциальной информации **- (4 часа) -** ***проверка сформированности компетенций*** ОПК-4.1; ПК-10; ПК-11

Вопросы для изучения и обсуждения:

1. Лицензионные требования.

2. Ответственность за незаконную деятельность в области защиты информации.

Контрольные вопросы:

1. Какова проверка сведений о лицензиате?

2. Как проходит лицензионный контроль деятельности в области защиты персональных данных?

3. Дать оценку управления риском, связанным с отсутствием лицензии на техническую защиту конфиденциальной информации?

Список источников и литературы:

а) источники

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_75586/

Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) "О сертификации средств защиты информации", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_7054/

"Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008), Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_99662/

Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/#dst100009

"Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСТЭК РФ 14.02.2008), Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_77814/

9.2. Методические рекомендации по организации самостоятельной работы

Трудоемкость освоения дисциплины «Организация защиты персональных данных» составляет 114 часов, из них 36 часов отведены на самостоятельную работу студента (СР).

Вид работы	Содержание (перечень вопросов)	Трудоем-кость самостоятельной работы (в часах)	Рекомендации
Подготовка к лекции Тема 2. «Общая характеристика института защиты персональных данных»	Международное и национальное законодательство зарубежных стран о защите персональных данных. Особенности защиты персональных данных. Основные положения законодательной базы Российской Федерации в	10	Проанализировать материал из законодательных, нормативных документов, учебников: Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации. 2006. № 31 (ч.I). Ст. 3451). Федеральный закон от 19 декабря 2005 № 160-ФЗ «О

	области защиты конфиденциальной информации.		ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» (Российская газета. 22 декабря 2005. № 288). Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (ред. от 21.10.2008). Бачило И.Л., Сергиенко Л.А., Кристальный Б.В., Арешев А.Г. Персональные данные в структуре информационных ресурсов. Основы правового регулирования, Минск, 2006. С.474. Курникова И.А. Доступ к персональным данным: законодательство и практика (отечественный и зарубежный опыт). Методическое пособие. М.: Росархив, ВНИИДАД, 2004, 128 с.
Подготовка к лекции Тема 3 «Основные понятия, термины и определения в соответствии с ФЗ "О персональных данных" от 27 июля 2006 г., № 152-ФЗ»	Персональные данные в Федеральном законе «О персональных данных». Содержание категории «персональные данные». Область применения закона и установленные ограничения. Принципы обработки персональных данных. Условия обработки персональных данных. Обработка персональных данных третьим лицом в интересах оператора.	10	Проанализировать материал из законодательных, нормативных документов, учебников: Закон РФ от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ 31.07.2006, N 31 (1 ч.), ст. 3448. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации. 2006. № 31 (ч.I). Ст. 3451). Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «О Перечне сведений конфиденциального характера» с изменениями, внесенными

			Указом Президента Российской Федерации от 23 сентября 2005 г. № 1111 (Собрание законодательства Российской Федерации. 1997. № 10. Ст. 1127). Бачило И.Л., Сергиенко Л.А., Кристальный Б.В., Арешев А.Г. Персональные данные в структуре информационных ресурсов. Основы правового регулирования, Минск, 2006. С.474. Курникова И.А. Доступ к персональным данным: законодательство и практика (отечественный и зарубежный опыт). Методическое пособие. М.: Росархив, ВНИИДАД, 2004, 128 с. Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом : учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - ISBN 978-5-9275-2501-0. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1021578
Подготовка к лекции Тема 4 «Основные понятия и определения в соответствии с Главой 14 Трудового кодекса Российской Федерации от 30 декабря 2001 года № 197-ФЗ»	Понятие персональных данных работника. Обработка персональных данных работника на предприятии. Хранение и использование персональных данных работников на предприятии. Передача персональных данных работника в пределах одной организации. Передача персональных	10	Проанализировать материал из законодательных, нормативных документов, учебников: Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации. 2006. № 31 (ч.I). Ст. 3451). Указ Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении положения о персональных данных государственного служащего Российской

	данных работника третьей стороне.		Федерации и ведения его личного дела» (ред. от 23.10.(Собрание законодательства Российской Федерации. 2005. № 30 (ч.II). Ст. 3165). Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (принят ГД ФС РФ 21.12.2001), глава 14. Комментарии официальных органов к трудовому кодексу Российской Федерации. Библиотека журнала "Трудовое право Российской Федерации», - М: Инфра-М, 2009, С.864.
Подготовка к лекции Тема 5 «Нормативные документы Федеральных органов власти в области защиты персональных данных и порядок работы с персональными данными на предприятии»	Компетенции уполномоченного органа по защите прав субъектов персональных данных. Мероприятия по защите сведений конфиденциального характера. Правовые основания обработки персональных данных. Получение согласия субъектов на обработку. Содержание договоров с субъектами в части обработки персональных данных.	8	Проанализировать материал из законодательных, нормативных документов, учебников: Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации. 2006. № 31 (ч.I). Ст. 3451). Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (ред. от 21.10.2008). Постановление Правительства РФ от 26 июня 1995 г. N 608 "О сертификации средств защиты информации" (ред. от 17.12.2004) (Собрание законодательства Российской Федерации. 1995, N 27, ст. 2579). Приказ Председателя Гостехкомиссии России от 27.10.1995 № 1999 «Об утверждении Положения о сертификации средств защиты информации по требованиям безопасности информации».

Подготовка к практическому занятию Тема 5 «Нормативные документы Федеральных органов власти в области защиты персональных данных и порядок работы с персональными данными на предприятии»	Практические шаги по приведению порядка обработки в соответствие с требованиями законодательства. Формирование перечня персональных данных. Учет лиц, допущенных к персональным данным. Определение порядка обращения с такими сведениями, контроля за его соблюдением. Организация доступа пользователей к ИСПДн. Внутренние нормативные документы по охране конфиденциальности сведений, их содержание, порядок разработки и ввода в действие.	10	Проанализировать материал из законодательных, нормативных документов, учебников: Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации. 2006. № 31 (ч.I). Ст. 3451). Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (ред. от 21.10.2008). Постановление Правительства РФ от 26 июня 1995 г. N 608 "О сертификации средств защиты информации" (ред. от 17.12.2004) (Собрание законодательства Российской Федерации. 1995, N 27, ст. 2579). Приказ Председателя Гостехкомиссии России от 27.10.1995 № 1999 «Об утверждении Положения о сертификации средств защиты информации по требованиям безопасности информации». Корнеев И.К., Степанов Е.А., «Защита информации в офисе», Учебник. М.-ООО «ТК Велби» Изд-во Проспект, 2008. – 336 с.
Подготовка к лекции Тема 6 «Организационно-техническая защита персональных данных в информационных системах»	Порядок классификации информационных систем персональных данных. Организационно-технические мероприятия оператора по защите персональных данных Каналы утечки информации при обработке персональных данных в информационных	10	Проанализировать материал из законодательных, нормативных документов, учебников: Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации. 2006. № 31 (ч.I). Ст. 3451). Указ Президента Российской Федерации от 17 марта 2008 г. №

	системах.		351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (ред. от 21.10.2008). Постановление Правительства РФ от 26 июня 1995 г. N 608 "О сертификации средств защиты информации" (ред. от 17.12.2004) (Собрание законодательства Российской Федерации. 1995, N 27, ст. 2579). Приказ Председателя Гостехкомиссии России от 27.10.1995 № 1999 «Об утверждении Положения о сертификации средств защиты информации по требованиям безопасности информации». Постановление Правительства РФ от 17 ноября 2007 г. N 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
Подготовка к лекции Тема 7 «Лицензирование деятельности по технической защите конфиденциальной информации»	Лицензионные требования по обработке персональных данных. Проверка сведений о лицензиате и лицензионный контроль за деятельность, связанную с обработкой персональных данных. Ответственность за незаконную деятельность в области защиты информации.	18	Проанализировать материал из законодательных, нормативных документов, учебников: Постановление Правительства РФ от 26 июня 1995 г. N 608 "О сертификации средств защиты информации" (ред. от 17.12.2004) (Собрание законодательства Российской Федерации. 1995, N 27, ст. 2579). Постановление Правительства Российской Федерации от 15 августа 2006 г. N 504 «Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации» (Собрание законодательства Российской Федерации. 2006. N 34. Ст. 3691, Российская газета. 29 августа

			2006 г. N 190). Приказ Председателя Гостехкомиссии России от 27.10.1995 № 1999 «Об утверждении Положения о сертификации средств защиты информации по требованиям безопасности информации». Постановление Правительства РФ от 17 ноября 2007 г. N 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Организация защита персональных данных» реализуется в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация (степень) «бакалавр»), утвержденного и введенного в действие приказом Министерства образования и науки РФ от 01 декабря 2016 г. № 1515.

Дисциплина «Организация защита персональных данных» входит в вариативную часть цикла по выбору студентов дисциплин подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность».

Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности Института информационных наук и технологий безопасности.

Содержание дисциплины охватывает круг вопросов, связанных с организацией обработки персональных данных, в соответствии с требованиями российского законодательства, применительно к различным категориям исполнителей на предприятии (от руководителей предприятий и структурных подразделений до непосредственно отвечающих за защиту информации и работающих с персональными данными). Анализируются изменения российского законодательства в части персональных данных, последствия внесения этих изменений для деятельности операторов, способы минимизации рисков, связанных с обработкой персональных данных и затрат на их защиту.

Цель курса - формирование знаний и умений для организации комплекса мероприятий по обеспечению конфиденциальности обработки персональных данных с использованием правовых, организационных и организационно-технических мер, определенных с учетом актуальности угроз безопасности персональных данных и используемых информационных технологий, способы снижения рисков утечки персональных данных.

Структура курса предполагает рассмотрение теоретических и практических аспектов в работе с персональными данными на предприятии, а также разбор на практических примерах действий операторов персональных данных в рамках трудовых отношений с собственным персоналом, гражданско-правовых отношениях, связанных с передачей и представлением персональных данных третьим лицам, в том числе органам государственной власти.

Дисциплина направлена на формирование следующих компетенций выпускника:

- ОПК-4.1 - Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах;

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- Умеет разрабатывать документы в области обеспечения безопасности информации в автоматизированной системе при ее эксплуатации (включая управление инцидентами информационной безопасности)
- Владеет навыками планирования мероприятий по обеспечению защиты информации и организацию работы персонала автоматизированной системы с учетом требований по защите информации

- ПК-10 - Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации
- Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации

- ПК-11 - Способен проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает методики проведения теоретических исследований уровней защищенности информационной безопасности объектов и систем
- Умеет составлять и оформлять аналитический отчет по проведенным испытаниям, делать выводы по оценке защищенности на основании аналитического отчета
- Владеет навыками использования профиля защиты и задания по безопасности, формулирования выводов по оценке защищенности

По дисциплине предусмотрена промежуточная аттестация в форме экзамена

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы.