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 «**Аудит и экономический анализ**»
Экономическогофакультета

Специальность
38.05.01 Экономическая безопасность

Специализация «Судебная экономическая экспертиза»

Уровень высшего образования
специалитет

Форма обучения
очная, заочная

Статус дисциплины: **вариативная**

Махачкала, 2018год

Рабочая программа дисциплины «Защита персональных данных» составлена в 2018 году в соответствии с требованиями ФГОС ВО по специальности 38.05.01 Экономическая безопасность (уровень специалитета), утвержденный приказом Минобрнауки РФ от «16» января 2017 года, №20

Разработчик: кафедра «Аудит и экономический анализ» ДГУ к.э.н., доцент Мамаева У.З.

Рабочая программа дисциплины одобрена:
на заседании кафедры «Аудит и экономический анализ»
от «27» июня 2018 г., протокол № 10
Зав. кафедрой _____ Гаджиев Н.Г.
(подпись)

на заседании Методической комиссии экономического факультета
от «30» июня 2018 г., протокол № 10
Председатель _____ Сулейманова Д.А.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением «30» августа 2018г. _____
(подпись

СОДЕРЖАНИЕ

Аннотация рабочей программы дисциплины

Дисциплина «Защита персональных данных» входит в состав вариативной части образовательной программы специальности 38.05.01 Экономическая безопасность, специализация «Судебная экономическая экспертиза».

Содержание дисциплины охватывает круг вопросов, связанных с организацией и способами защиты и экономической безопасности персональных данных, принятия решений по предупреждению, локализации и нейтрализации угроз.

Дисциплина нацелена на формирование следующих компетенций выпускника: профессиональные компетенции –ПК-4, ПК-40.

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

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме контрольной работы и промежуточный контроль в форме зачета.

Объем дисциплины 3 зачетные единицы, в том числе в академических часах 108 часов по видам учебных занятий.

Семестр	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	Всего	в том числе							
		Контактная работа обучающихся с преподавателем						СРС, в том числе зачет	
		Всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
8	108	42	14	-	28	-	-	66	Зачет
ИТОГО	108	42	14	-	28	-	-	66	Зачет

1. Цели освоения дисциплины

Цели освоения дисциплины соотносятся с общими целями ОПОП ВО-по направлению38.05.01 Экономическая безопасность.

Цель освоения дисциплины «Защита персональных данных» является развитие делового и логического мышления студентов, ознакомление студентов с основами теории, необходимыми для решения прикладных задач путем использования нормативно-правовых документов в профессиональной деятельности, защиты своих прав в соответствии с гражданским, гражданско-процессуальным и трудовым законодательство , путем анализа и оценки результатов и последствий деятельности (бездействия) с правовой точки зрения.

2.Место дисциплины в структуре ОПОП специалитета

Дисциплина «Защита персональных данных» относится дисциплинам по выбору образовательной программы специальности 38.05.01 Экономическая безопасность, специализация «Судебная экономическая экспертиза».

Для успешного освоения дисциплины студенты должны иметь знания, полученные в рамках ранее пройденных дисциплин: «Теневая экономика как угроза экономической безопасности», «Правоохранительная деятельность по обеспечению экономической безопасности государства», «Основы экономической безопасности», «Оценка и защита интеллектуальной собственности», «Основы информационной безопасности».

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

Код компетенции из ФГОС ВО	**Наименование компетенции из ФГОС ВО**	Планируемые результаты обучения
ПК-4	способность выполнять необходимые для составления экономических разделов планов расчеты, обосновывать их и представлять результаты работы в соответствии с принятыми стандартами	Знать: методику составления экономических разделов планов расчеты, обосновывать их и представлять результаты работы в соответствии с принятыми стандартами Уметь: выполнять необходимые для составления экономических разделов планов расчеты, обосновывать их и представлять результаты работы в соответствии с принятыми стандартами Владеть: способностью выполнять необходимые для составления экономических разделов планов расчеты, обосновывать их и представлять результаты работы в соответствии с принятыми стандартами
ПК-40	способность осуществлять экспертную оценку факторов риска, способных создавать социально-экономические ситуации критического ха-	Знать: методику экспертной оценки факторов риска, способных создавать социально-экономические ситуации критического характера, оценивать возможные экономические потери в

	рактера, оценивать возможные экономические потери в случае нарушения экономической и финансовой безопасности, определять необходимые компенсационные резервы	случае нарушения экономической и финансовой безопасности, определять необходимые компенсационные резервы Уметь осуществлять экспертную оценку факторов риска, способных создавать социально-экономические ситуации критического характера, оценивать возможные экономические потери в случае нарушения экономической и финансовой безопасности, определять необходимые компенсационные резервы Владеть: способностью осуществлять экспертную оценку факторов риска, способных создавать социально-экономические ситуации критического характера, оценивать возможные экономические потери в случае нарушения экономической и финансовой безопасности, определять необходимые компенсационные резервы

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 3зачетных единиц, 108 академических часа.

4.2. Структура дисциплины(форма обучения – очная).

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные занятия	КСР		
	Модуль 1. Теоретические основы безопасности персональных данных								
1	Базовые вопросы управления безопасностью персональных данных. Процессный подход	8	1-2	2	4			6	Опросы, представление докладов, участие в дискуссиях, тест
2	Область деятельности безопасности персональных данных. Ролевая структура безопасности персональ-	8	3-5	2	4			6	Опросы, представление докладов, участие в дискуссиях, тест

	ных данных. Политика безопасности персональных данных								
3	Рискология безопасности персональных данных	8	6-8	2	4			6	Опросы, представление докладов, участие в дискуссиях, тест
	Итого по модулю 1:		36	6	12			18	Контрольная работа
	Модуль 2. Основные процессы безопасности персональных данных								
4	Эксплуатация и независимый аудит безопасности персональных данных	8	9-11	2	2			12	Опросы, представление докладов, участие в дискуссиях, тест
5	Внедрение разработанных процессов безопасности персональных данных	8	12-13	2	4			14	Опросы, представление докладов, участие в дискуссиях, тест
	Итого по модулю 2:		36	4	6			26	Контрольная работа
	Модуль 3. Правовое регулирование безопасности персональных данных.								
6	Обеспечение соответствия требованиям законодательства РФ системы безопасности персональных данных	8	14-16	2	6			12	Опросы, представление докладов, участие в дискуссиях, тест
7	Правовая защита служебной тайны, основу которой составляет конфиденциальная информация	8	17-18	2	4			10	Опросы, представление докладов, участие в дискуссиях, тест
	Итого по модулю 3:		36	4	10			22	Контрольная работа
	Итого	8	108	14	28			66	

Структура дисциплины(форма обучения –заочная).

№ п/п	Разделы и темы дисциплины	Курс	Всего	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные занятия	КСР		

	Модуль 1. Теоретические основы безопасности персональных данных								
1	Базовые вопросы управления безопасностью персональных данных. Процессный подход	5	14	2	2			10	Опросы, представление докладов, участие в дискуссиях, тест
2	Область деятельности безопасности персональных данных. Ролевая структура безопасности персональных данных. Политика безопасности персональных данных	5	14	2	2			10	Опросы, представление докладов, участие в дискуссиях, тест
3	Рискология безопасности персональных данных	5	12		2			10	Опросы, представление докладов, участие в дискуссиях, тест
	Итого по модулю 1:		36	4	6			30	Контрольная работа
	Модуль 2. Основные процессы безопасности персональных данных								
4	Эксплуатация и независимый аудит безопасности персональных данных	5	18					18	Опросы, представление докладов, участие в дискуссиях, тест
5	Внедрение разработанных процессов безопасности персональных данных	5	18					18	Опросы, представление докладов, участие в дискуссиях, тест
	Итого по модулю 2:		36					36	Контрольная работа
Модуль 3. Правовое регулирование безопасности персональных данных.									
6	Обеспечение соответствия требованиям законодательства РФ системы безопасности персональных данных	5	18					18	Опросы, представление докладов, участие в дискуссиях, тест
7	Правовая защита служебной тайны, основу которой составляет конфиденциальная информация	5	18					18	Опросы, представление докладов, участие в дискуссиях, тест
	Итого по модулю 3:		36					36	Контрольная работа
	Итого	5	108	4	6			98	

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

4.3.1. Содержание лекционных занятий по дисциплине.

Модуль 1. Теоретические основы безопасности персональных данных

Тема 1. Базовые вопросы управления безопасностью персональных данных. Процессный подход

Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний. Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБДПД. Понятие системы управления. Понятие ИБДПД. Место ИБДПД в рамках общей системы управления предприятием. Стандартизация в области построения систем управления. История развития. Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере ИБДПД). Основные процессы ИБДПД и требования, предъявляемые к ним каждым из стандартов.

Тема 2. Область деятельности безопасности персональных данных. Ролевая структура безопасности персональных данных. Политика безопасности персональных данных

Понятие области деятельности ИБДПД. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные конфиденциальной информации как научная дисциплина. Отличие государственной тайны от других видов тайн (коммерческой, профессиональной тайны, а также конфиденциальной информации). подразделения организации, кадры). Описание области деятельности (структура и содержание документа).Понятие роли. Использование ролевого принципа в рамках ИБДПД. Преимущества использования ролевого принципа. Ролевая структура ИБДПД (основные и дополнительные роли).Роль высшего руководства организации в ИБДПД. Этапы разработки и функционирования ИБДПД, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.).Понятие Политики ИБДПД. Цели Политики ИБДПД. Структура и содержание Политики ИБДПД. Источники информации для разработки Политики ИБДПД.

Тема 3. Рискология безопасности персональных данных

Цель процесса анализа рисков ИБДПД. Этапы и участники процесса анализа рисков ИБДПД. Разработка Методики анализа рисков ИБДПД. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Выбор угроз ИБДПД и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБДПД. Планирование мер по обработке выявленных рисков ИБДПД. Утверждение результатов анализа рисков ИБДПД у высшего руководства. Использование результатов анализа рисков ИБДПД.

Модуль 2. Основные процессы безопасности персональных данных

Тема 4.Эксплуатация и независимый аудит безопасности персональных данных

Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБДПД на соответствие требованиям нормативных документов. Этапы проведения аудита ИБДПД. Результаты аудита ИБДПД и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации ИБДПД перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации.

Тема 5. Внедрение разработанных процессов безопасности персональных данных

Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения. Сложности, возникающие при внедрении процессов управления ИБДПД, и способы их решения. Контроль над внедрением процессов. Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа.

Модуль 3. Правовое регулирование безопасности персональных данных.

Тема 6.Обеспечение соответствия требованиям законодательства РФ системы безопасности персональных данных

Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках ИБДПД (авторское право, защита персональных данных и т.д.). Разработка процессов или дополнение существующих процессов управления ИБДПД с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

Тема 7. Правовая защита служебной тайны, основу которой составляет конфиденциальная информация

Налоговая тайна как вид служебной тайны содержащей персональные данные. Юридические санкции применяемые в области защиты персональных данных на предприятии. Практика совершенства института сведений ограниченного распространения как основа формирования и совершенствования института служебной тайны.

4.3.2. Содержание практических занятий по дисциплине.

Модуль 1. Теоретические основы защиты государственной тайны

Модуль 1. Теоретические основы безопасности персональных данных

Тема 1. Базовые вопросы управления безопасностью персональных данных. Процессный подход

Вопросы к теме:

1. Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний.
2. Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБДПД. Понятие системы управления. Понятие ИБДПД. Место ИБДПД в рамках общей системы управления предприятием. Стандартизация в области построения систем управления. История развития. Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода.
3. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере ИБДПД). Основные процессы ИБДПД и требования, предъявляемые к ним каждым из стандартов.

Ссылка на учебно-методическую литературу, указанную в п.8 (1,2,3,4,5,6)

Тема 2. Область деятельности безопасности персональных данных. Ролевая структура безопасности персональных данных. Политика безопасности персональных данных

Вопросы к теме:

1. Понятие области деятельности ИБДПД. Механизм выбора области деятельности.
2. Состав области деятельности (процессы, структурные конфиденциальной информации как научная дисциплина. Отличие государственной тайны от других видов тайн (коммерческой, профессиональной тайны, а также конфиденциальной информации). подразделения организации, кадры). Описание области деятельности (структура и содержание документа).Понятие роли.
3. Использование ролевого принципа в рамках ИБДПД. Преимущества использования ролевого принципа. Ролевая структура ИБДПД (основные и дополнительные роли).Роль высшего руководства организации в ИБДПД. Этапы разработки и функционирования ИБДПД, на которых важно участие руководства организации.
4. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.).Понятие Политики ИБДПД. Цели Политики ИБДПД. Структура и содержание Политики ИБДПД. Источники информации для разработки Политики ИБДПД.

Ссылка на учебно-методическую литературу, указанную в п.8 (1,2,3,4,5,6)

Тема 3. Рискология безопасности персональных данных

Вопросы к теме:

1. Цель процесса анализа рисков ИБДПД. Этапы и участники процесса анализа рисков ИБДПД. Разработка Методики анализа рисков ИБДПД. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации.
2. Выбор угроз ИБДПД и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБДПД. Планирование мер по обработке выявленных рисков ИБДПД.
3. Утверждение результатов анализа рисков ИБДПД у высшего руководства. Использование результатов анализа рисков ИБДПД.

Ссылка на учебно-методическую литературу, указанную в п.8 (1,3,4,5,6)

Модуль 2. Основные процессы безопасности персональных данных

Тема 4.Эксплуатация и независимый аудит безопасности персональных данных

Вопросы к теме:

1. Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБДПД на соответствие требованиям нормативных документов. Э
2. тапы проведения аудита ИБДПД. Результаты аудита ИБДПД и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001.
3. Период эксплуатации ИБДПД перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации.

Ссылка на учебно-методическую литературу, указанную в п.8 (1,2,3,4,5,6)

Тема 5. Внедрение разработанных процессов безопасности персональных данных

Вопросы к теме:

1. Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения.
2. Сложности, возникающие при внедрении процессов управления ИБДПД, и способы их решения. Контроль над внедрением процессов. Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости».
3. Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа.

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

Модуль 3. Правовое регулирование безопасности персональных

данных.

Тема 6.Обеспечение соответствия требованиям законодательства РФ системы безопасности персональных данных

Вопросы к теме:

1. Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках ИБДПД (авторское право, защита персональных данных и т.д.).
2. Разработка процессов или дополнение существующих процессов управления ИБДПД с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

Ссылка на учебно-методическую литературу, указанную в п.8 (1,2,3,4,5,6)

Тема 7. Правовая защита служебной тайны, основу которой составляет конфиденциальная информация

Вопросы к теме:

1. Налоговая тайна как вид служебной тайны содержащей персональные данные.
2. Юридические санкции применяемые в области защиты персональных данных на предприятии.
3. Практика совершенства института сведений ограниченного распространения как основа формирования и совершенствования института служебной тайны.

Ссылка на учебно-методическую литературу, указанную в п.8 (1,2,3,5,6)

5. **Образовательные технологии**

Современные образовательные технологии в преподавании дисциплины «Защита персональных данных»ориентированы на реализацию инновационных методов обучения как слагаемых учебного процесса. Они учитывают преимущества компетентностного подхода к изучению дисциплины, обеспечивают повышение качества знаний, необходимых для профессиональной деятельности бухгалтеров.

При ведении семинарских занятий по данной дисциплине используются такие стандартные методы обучения, как тестирование, фронтальный опрос, индивидуальный опрос, метод малых групп и т.п.

При ведении занятий определенное количество часов отведено интерактивным формам. Лекции при этом проводятся с использованием средств визуализации лекционного материала (мультимедийных презентаций) и применением таких методов и технологий, как дискуссия, проблемная лекция и т.п. При проведении семинаров в интерактивной форме используются следующие методы: дебаты, круглый стол, мини-конференция и т.п.

Кроме того, в процессе изучения дисциплины с целью повышения качества обучения предполагается использование научно-исследовательской работы студентов.

Предусмотрены также встречи с представителями контрольно-счетных органов РД.

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Для теоретического и практического усвоения дисциплины большое значение имеет самостоятельная работа студентов, она осуществляться студентами индивидуально и под руководством преподавателя.

Самостоятельная работа по дисциплине,предусмотренная учебным планом в объеме66 часов, направлена на более 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 «Защита персональных данных» выступают следующие:

1) проработка учебного материала;
2) работа с электронными источниками;
3) выполнение кейс-заданий и решение задач;
4) обработка аналитических данных;
5) подготовка докладов к участию в тематических дискуссия;
6) работа с тестами и вопросами;
7) написание рефератов.

Виды и формыконтроля самостоятельной работы студентов в рамках освоения дисциплины «Защита персональных данных»

Разделы дисциплины	Виды самостоятельной работы (и ссылки на литературу[1])	Количество часов	Форма контроля
Раздел 1. Теоретические основы безопасности персональных данных	проработка учебного материала, работа с электронными источниками, подготовка докладов к участию в тематических дискуссиях, работа с тестами и вопросами, написание рефератов. *(1,2,3,4,5,6)*	18	Дискуссия, опрос,защита рефератов
Раздел 2. Основные процессы безопасности персональных данных	проработка учебного материала,работа с электронными источниками, подготовка докладов к участию в тематических дискуссиях,работа с тестами и вопросами, написание рефератов. *(1,2,3,4,5,6)*	26	Дискуссия, опрос, проверка домашнего задания, защита рефератов
Раздел 3. Правовое регулирование безопасности персональных данных	проработка учебного материала, решение задач, выполнение кейс-заданий, выполнение рефератов и докладов, работа с бухгалтерской отчетностью, обработка аналитических данных, подготовка докладов к участию в тематических дискуссиях, работа с тестами и вопросами, написа-	22	Дискуссия, опрос,защита рефератов

[1] Дается ссылка на учебно-методическую литературу, указанную в п. 8.

	ние рефератов. *(1,2,3,4,5,6)*		
Итого		66	

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;
- написаниеиоформление текста (5-15машинописных страниц);
- подготовка тезисов доклада (на 7-10 минут);
- устное изложение в виде доклада, в том числе виде презентации.

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

Материал в реферате располагается в следующей 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 студенту выставляется соответствующий балл за СРС(1-10 баллов).

Примерная тематика рефератов по модулям и темам дисциплины

Модуль 1. Теоретические основы безопасности персональных данных

Тема 1. Базовые вопросы управления безопасностью персональных данных. Процессный подход

1. Место ИБДПД в рамках общей системы управления предприятием.
2. Стандартизация в области построения систем управления.
3. История развития.
4. Основные процессы ИБДПД и требования, предъявляемые к ним каждым из стандартов.

Тема 2. Область деятельности безопасности персональных данных. Ролевая структура безопасности персональных данных. Политика безопас-

ности персональных данных

1. Понятие области деятельности ИБДПД.
2. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные конфиденциальной информации как научная дисциплина.
3. Ролевая структура ИБДПД (основные и дополнительные роли).Роль высшего руководства организации в ИБДПД.

Тема 3. Рискология безопасности персональных данных

1. Цель процесса анализа рисков ИБДПД.
2. Этапы и участники процесса анализа рисков ИБДПД. Разработка Методики анализа рисков ИБДПД.
3. Планирование мер по обработке выявленных рисков ИБДПД.

Модуль 2. Основные процессы безопасности персональных данных

Тема 4.Эксплуатация и независимый аудит безопасности персональных данных

1. Внешние аудиты ИБДПД на соответствие требованиям нормативных документов.
2. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001.

Тема 5. Внедрение разработанных процессов безопасности персональных данных

1. Этапы внедрения процессов и их последовательность.
2. Обучение сотрудников, как один из этапов внедрения..

Модуль 3. Правовое регулирование безопасности персональных данных.

Тема 6.Обеспечение соответствия требованиям законодательства РФ системы безопасности персональных данных

1. Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках ИБДПД (авторское право, защита персональных данных и т.д.). Р
2. азработка процессов или дополнение существующих процессов управления ИБДПД с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

Тема 7. Правовая защита служебной тайны, основу которой составляет конфиденциальная информация

1. Налоговая тайна как вид служебной тайны содержащей персональные данные.
2. Юридические санкции применяемые в области защиты персональных данных на предприятии.

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

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

Перечень компетенций с указанием этапов их формирования приведен в описании образовательной программы.

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения	Процедура освоения
ПК-4	способность выполнять необходимые для составления экономических разделов планов расчеты, обосновывать их и представлять результаты работы в соответствии с принятыми стандартами	Знать: методику составления экономических разделов планов расчеты, обосновывать их и представлять результаты работы в соответствии с принятыми стандартами Уметь: выполнять необходимые для составления экономических разделов планов расчеты, обосновывать их и представлять результаты работы в соответствии с принятыми стандартами Владеть: способностью выполнять необходимые для составления экономических разделов планов расчеты, обосновывать их и представлять результаты работы в соответствии с принятыми стандартами	Опросы, представление докладов, участие в дискуссиях, тест
ПК-40	способность осуществлять экспертную оценку факторов риска, способных создавать социально-экономические ситуации критического характера, оценивать возможные экономические потери в случае нарушения экономической и финансовой безопасности, определять необходимые компенсационные резервы	Знать: методику экспертной оценки факторов риска, способных создавать социально-экономические ситуации критического характера, оценивать возможные экономические потери в случае нарушения экономической и финансовой безопасности, определять необходимые компенсационные резервы Уметь осуществлять экспертную оценку факторов риска, способных создавать социально-экономические ситуации критического характера, оценивать возможные экономические потери в случае нарушения экономической и финансовой безопасности, определять необходимые компенсационные резервы Владеть: способностью осуществлять экспертную оценку факторов	Опросы, представление докладов, участие в дискуссиях, тест

		риска, способных создавать социально-экономические ситуации критического характера, оценивать возможные экономические потери в случае нарушения экономической и финансовой безопасности, определять необходимые компенсационные резервы	

7.2. Типовые контрольные задания

Примерные тестовые задания

1. Невыплаченные дивиденды акционеров, без удержания подоходного налога, на увеличение уставного капитала при изменении организационно-правовой формы направляться:

а) не могут;
б) могут, если произошла перерегистрация уставного капитала;
в) могут.

2. Перечень сведений, составляющих коммерческую тайну определяет:

а) собственник имущества;
б) правление предприятия;
в) руководитель предприятия.

3. Внесение изменений и дополнений в устав акционерного общества осуществляется по решению:

а) совета директоров общества;
б) исполнительного органа общества;
в) общего собрания общества.

Примерные вопросы для подготовки к промежуточной аттестации по итогам освоения дисциплины (зачет, 8 семестр)

1. Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины.
2. Сущность и функции управления. Наука управления.
3. Принципы, подходы и виды управления. Цели и задачи управления ИБДПД. Понятие системы управления.
4. Понятие ИБДПД. Место ИБДПД в рамках общей системы управления предприятием.
5. Стандартизация в области построения систем управления. История развития.
6. Понятие процесса.
7. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере ИБДПД).

8. Основные процессы ИБДПД и требования, предъявляемые к ним каждым из стандартов.

9. Понятие области деятельности ИБДПД. Механизм выбора области деятельности.

10. Состав области деятельности (процессы, структурные конфиденциальной информации как научная дисциплина.

11. Понятие тайны в свете современного законодательства, отличие государственной тайны от других видов тайн (коммерческой, профессиональной тайны, а также конфиденциальной информации).

12. Подразделения организации, кадры). Описание области деятельности (структура и содержание документа).

13. Понятие роли. Использование ролевого принципа в рамках ИБДПД.

14. Преимущества использования ролевого принципа. Ролевая структура ИБДПД (основные и дополнительные роли). Роль высшего руководства организации в ИБДПД.

15. Этапы разработки и функционирования ИБДПД, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.).

16. Понятие Политики ИБДПД. Цели Политики ИБДПД. Структура и содержание Политики ИБДПД. Источники информации для разработки Политики ИБДПД.

17. Цель процесса анализа рисков ИБДПД. Этапы и участники процесса анализа рисков ИБДПД. Разработка Методики анализа рисков ИБДПД.

18. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации.

19. Выбор угроз ИБДПД и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБДПД. Планирование мер по обработке выявленных рисков ИБДПД.

20. Утверждение результатов анализа рисков ИБДПД у высшего руководства. Использование результатов анализа рисков ИБДПД.

21. Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами ИБДПД).

22. Процессы улучшения ИБДПД («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»).

23. Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса».

24. Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности».

25. Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБДПД на соответствие требованиям нормативных документов.

26. Этапы проведения аудита ИБДПД. Результаты аудита ИБДПД и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК

27001. Период эксплуатации ИБДПД перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации.

27. Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения.

28. Сложности, возникающие при внедрении процессов управления ИБДПД, и способы их решения. Контроль над внедрением процессов.

29. Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа.

30. Цели и задачи процесса «Управления инцидентами ИБДПД, важность процесса с точки зрения управления ИБДПД Входные/выходные данные процесса. Участники процесса.

31. Обязательные этапы процесса. Связи с другими процессами ИБДПД. Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами ИБДПД.

32. Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках ИБДПД (авторское право, защита персональных данных и т.д.).

33. Разработка процессов или дополнение существующих процессов управления ИБДПД с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

34. Налоговая тайна как вид служебной тайны содержащей персональные данные.

35. Юридические санкции применяемые в области защиты персональных данных на предприятии.

Практика совершенства института сведений ограниченного распространения как основа формирования и совершенствования института служебной тайны.

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

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

Текущий контроль по дисциплине включает:

- посещение занятий - 22 балла,
- участие на практических занятиях - 60 баллов,
- выполнение домашних (аудиторных) контрольных работ - 18баллов.

Промежуточный контроль по дисциплине включает:

- письменная контрольная работа - 100 баллов

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) основная литература:

1. Исаев А.С. Правовые основы организации защиты персональных данных [Электронный ресурс] : учебное пособие / А.С. Исаев, Е.А. Хлюпина. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2014. — 106 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/67564.html
2. Артемьев, В.Р. Информационно-коммерческая безопасность предпринимательской деятельности / В.Р. Артемьев. - Москва : Лаборатория книги, 2010. - 38 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=87020
3. Петренко В.И. Защита персональных данных в информационных системах [Электронный ресурс] : учебное пособие / В.И. Петренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 201 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66023.html

б) дополнительная литература:

1. Правовое регулирование информационных отношений в области государственной и коммерческой тайны, персональных данных : учебное пособие / О.В. Ахрамеева, И.Ф. Дедюхина, О.В. Жданова и др. ; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Ставропольский государственный аграрный университет, Кафедра государственного и муниципального управления и права. - Ставрополь : Ставропольский государственный аграрный университет, 2015. - 59 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438603
2. Макаров А.М. Организация защиты персональных данных [Электронный ресурс] : лабораторный практикум / А.М. Макаров, И.В. Калиберда, К.О. Бондаренко. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 92 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/62971.html
3. Костомаров К.В. Банк России в сфере защиты персональных данных клиентов коммерческих банков [Электронный ресурс] : экономический и юридический аспекты / К.В. Костомаров, Е.А. Качанова. — Электрон. текстовые данные. — Екатеринбург: Уральский институт управления РАНХиГС, 2015. — 139 с. — 978-5-8056-0321-2. — Режим доступа: http://www.iprbookshop.ru/72351.html

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

1. Официальный сайтМинистерства экономического развития РФ[Электронный ресурс]– URL:http://www.economy.gov.ru(дата обращения 15.06.2018)
Официальный сайт Министерства финансовРФ[Электронный ресурс]– URL:http://www.economy.gov.ru/https://www.minfin.ru/ru/ (дата обращения 15.08.2018)
2. Информационный Портал «Бухгалтерия Онлайн»URL: http://www.buhonline.ru(дата обращения 10.06.2018).
3. Государственные программы Российской Федерации: Официальный портал госпрограмм РФ. [Электронный ресурс]. URL: http://programs.gov.ru/portal(дата обращения 12.03.2018).
4. Сайт Института профессиональных бухгалтеров России [Электронный ресурс]. URL: http://www.ipbr.ru (дата обращения 11.04.2018).
5. Справочно-правовая система «КонсультантПлюс»[Электронный ресурс]– URL: http://www.consultant.ru(дата обращения 08.06.2018).
6. Информационно-правовой портал «Гарант.ру» [Электронный ресурс]– URL:http://www.garant.ru(дата обращения 05.06.2018).
7. Электронный каталог НБ ДГУ [Электронный ресурс]: база данных содержит сведения о всех видах литературы, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. – Махачкала, 2018. – URL: http://elib.dgu.ru (дата обращения 21.03.2018).
8. eLIBRARY.RU[Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва. – URL: http://elibrary.ru/defaultx.asp (дата обращения 05.02.2018).
9. Moodle[Электронный ресурс]: система виртуального обучения: [база данных] / Даг. гос. ун-т. – г. Махачкала. – Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://moodle.dgu.ru/(дата обращения 21.03.2018).

10. Методические указания для обучающихся по освоению дисциплины.

Оптимальным путем освоения дисциплины является посещение всех лекций и семинаров и выполнение предлагаемых заданий в виде рефератов, докладов, тестов, кейс-заданий и устных вопросов.

На лекциях рекомендуется деятельность студента в форме активного слушания, т.е. предполагается возможность задавать вопросы на уточнение понимания темы и рекомендуется конспектирование основных положений лекции. На практических занятиях деятельность студента заключается в активном обсуждении вопросов темы, тематических докладов, рефератов, решении ситуационных задач, кейсов, 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 (законодательном документе), рекомендованном в качестве основной литературы. Студент может ознакомиться и с дополнительной литературой: периодические издания, интернет- источники.

Форма работы с литературой можетбыть разнообразной – начиная от комментированного чтения и кончая выполнением различных заданий на основе прочитанной литературы. Например; составление плана, подбор выписок из литературы по заданным вопросам; конспектирование текста.

Подготовка к экзамену предполагает изучение конспектов лекций, рекомендуемой литературы, повторение материалов практических занятий

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

При подготовке к практическим занятиям, а также при написании рефератов могут использоваться поисковые сайты сети «Интернет», информационно-справочная система «Консультант+», а также Интернет-ресурсы, перечисленные в разделе 9 данной программы.

Кроме того, может использоваться учебный курс, размещенный на платформе MoodleДГУ,http://moodle.dgu.ru/

Для проведения индивидуальных консультаций может использоваться также электронная почта.

Программное обеспечение: MicrosoftWindows 7, MicrosoftWord используется для создания текстовых файлов (рефератов, курсовых, выпускных квалификационных работ);MicrosoftExcel 2007 для составления аналитических таблиц и расчета показателей; PowerPoint – для создания презентаций, визуального сопровождения докладов, MicrosoftInternetExplorer –в целях поиска информации для самостоятельной работы.

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

Лекционный зал на 50-60 человек, стандартная учебная аудитория для группы на 20-25 чел, мультимедиапроектор, ноутбук, доска, наглядные пособия, специализированная мебель: столы, стулья.