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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

Кафедра «Аудит и экономический анализ»
экономического факультета

Образовательная программа

38.05.01 Экономическая безопасность

Специализация
«Судебная экономическая экспертиза»

Уровень высшего образования
Специалитет

Форма обучения
Очная, заочная

Статус дисциплины: базовая

Махачкала, 2018год

Рабочая программа дисциплины «Основы информационной безопасности» составлена в 2018 году в соответствии с требованиями ФГОС ВО по специальности 38.05.01 Экономическая безопасность (уровень специалитета) от «16» января 2017 года, №20

Разработчик: кафедра «Аудит и экономический анализ» ДГУ
к.э.н., доцент Султанов Г.С.

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 «Основы информационной безопасности» входит в состав базовой части образовательной программы специальности 38.05.01 Экономическая безопасность, специализация «Судебная экономическая экспертиза».

Дисциплина реализуется на экономическом факультете кафедрой «Аудит и экономический анализ».

Содержание дисциплины охватывает круг вопросов, связанных обеспечением защиты информации на различных уровнях.

Дисциплина нацелена на формирование следующих компетенций выпускника: общекультурных- ОК-12; общепрофессиональных - ОПК-3.

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

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости: текущего контроля в форме контрольной работы и промежуточного контроля в форме экзаменов.

Объем дисциплины 4 зачетных единиц, в том числе в академических часах по видам учебных занятий 144 ч.

форма обучения – очная

Семестр	Учебные занятия								Форма промежуточной аттестации (экзамен)
	Общий объем	в том числе							
		Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		Всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
2	144	72	36	-	36	-	-	72	Экзамен

форма обучения – заочная

курс	Учебные занятия								Форма промежуточной аттестации (экзамен)
	Общий объем	в том числе							
		Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		Всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
3	144	18	8	-	10	-	-	117	Экзамен

1. Цели освоения дисциплины

Целью освоения учебной дисциплины «Основы информационной безопасности» является формирование у студентов целостного представления предусматривается изучение вопросов защиты информации на различных уровнях. В результате изучения дисциплины студенты должны уметь: применять методы и приемы защиты от несанкционированного доступа, получить навыки шифрации и дешифрации информации методами криптографического преобразования данных.

2. Место дисциплины в структуре ОПОП специалитета

Дисциплина «Основы информационной безопасности » относится к базовой части образовательной программы по специальности 38.05.01 Экономическая безопасность.

Для усвоения курса «Основы информационной безопасности» необходимо знание дисциплин: «Математика», «Информатика».

Освоение данной дисциплины необходимо как предшествующее для изучения дисциплин: «Основы экономической безопасности», «Экономическая безопасность», «Финансовая безопасность», «Коммерческая тайна», «Защита государственной тайны», «Защита персональных данных».

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**
ОК-12	способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	*Знает*: понятия «Информация», различие понятия информационного воздействия и информационного взаимодействия, свойства информации в форме сведений и в форме сообщений, виды информации как объекта исследования, основные международные правовые акты по защите информации, основные положения и принципы международных соглашений, соответствие российских и международных правовых отношений, российские общегосударственные правовые документы по защите информации, российские отраслевые нормативные документы по защите информации *Умеет*: применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации *Владеет*: практическими навыками

		работы с различными информационными ресурсами и технологиями
ОПК-3	способность применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов	*Знает*: основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов *Умеет*: выделять основные составляющие национальных интересов в информационной сфере безопасности, относить информационные ресурсы к различным классам *Владеет*: практическими навыками использования новейших технологий в области информационной безопасности

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 4 зачетных единиц, 144 академических часов.

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. Основные понятия, определения и угрозы информационной безопасности									
1	Информация. Информационная сфера	2	1	2	2			2	Опрос, дискуссия, входное тестирование
2	Национальные интересы и безопасность России	2	2	2	2			4	Фронтальный опрос, тестирование, предоставление докладов и рефератов
3	Информационная война. Информационное оружие	2	3	2	2			4	Опрос, тестирование, решение ситуаций, предоставление докладов
4	Угрозы безопасности России.	2	4	4	4			6	Фронтальный опрос, тестирование, предоставление докладов и рефератов
	Итого по модулю 1	**2**	**36**	**10**	**10**			**16**	Контрольная работа
Модуль 2. Защита от несанкционированного доступа, компьютерные вирусы и									

антивирусные программы									
5	Показатели защищенности СВТ	2	5	2	2			2	Опрос, дискуссия тестирование, решение кейсов, предоставление докладов и рефератов
6	Защита информации в АСОД	2	6	2	2			2	Фронтальный опрос, тестирование, решение кейсов, предоставление докладов и рефератов
7	Виды доступа. Уровни доступа. Контроль доступа	2	7	2	2			2	Опрос, дискуссия тестирование, предоставление докладов и рефератов
8	Проблема вирусного заражения	2	8	2	2			2	Опрос, тестирование, решение ситуаций, предоставление докладов и рефератов
9	Перспективные методы антивирусной защиты	2	9	2	2			2	Фронтальный опрос, тестирование, решение кейсов, предоставление докладов
10	Основные классы антивирусных программ	2	10	2	2			2	Опрос, дискуссия тестирование, предоставление докладов и рефератов
	Итого по модулю 2	**2**	**36**	**12**	**12**			**12**	Контрольная работа
Модуль 3. Защита от утечки информации по техническим каналам и организационно-правовое обеспечение информационной безопасности									
11	Криптографические методы защиты информации	2	11-12	4	4			2	Фронтальный опрос, тестирование, решение кейсов, предоставление докладов и рефератов
9	Проблемы защиты информации в сетях ЭВМ	2	13-14	2	2			2	Опрос, дискуссия тестирование, решение кейсов, предоставление докладов и рефератов
10	Организационная защита информации. Комплексное обеспечение безопасности	2	15-16	4	4			2	Фронтальный опрос, тестирование, решение кейсов, предоставление докладов и рефератов
11	Правовые основы защиты информации	2	17-18	4	4			2	Опрос, тестирование, решение ситуаций, предоставление докладов и рефератов
	Итого по модулю 3	**2**	**36**	**14**	**14**			**8**	Контрольная работа

	Модуль 4 Подготовка к экзамену	2						**36**	Экзамен
	ИТОГО		**144**	**36**	**36**			**72**	

Форма обучения - заочная

№ п/п	**Разделы и темы дисциплины**	**год**	**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. Основные понятия, определения и угрозы информационной безопасности									
1	Информация. Информационная сфера	3	1	-	-			8	Опрос, дискуссия, входное тестирование
2	Национальные интересы и безопасность России	3	2	-	2			8	Фронтальный опрос, тестирование, предоставление докладов и рефератов
3	Информационная война. Информационное оружие	3	3	2	-			8	Опрос, тестирование, решение ситуаций, предоставление докладов
4	Угрозы безопасности России.	3	4	-	-			8	Фронтальный опрос, тестирование, предоставление докладов и рефератов
	Итого по модулю 1	3	**36**	**2**	**2**			**32**	Контрольная работа
Модуль 2. Защита от несанкционированного доступа, компьютерные вирусы и антивирусные программы									
5	Показатели защищенности СВТ	3	5	-	-			6	Опрос, дискуссия тестирование, решение кейсов, предоставление докладов и рефератов
6	Защита информации в АСОД	3	6	2	-			6	Фронтальный опрос, тестирование, решение кейсов, предоставление докладов и рефератов
7	Виды доступа. Уровни доступа. Контроль доступа	3	7	-	-			4	Опрос, дискуссия тестирование, предоставление докладов и рефератов

8	Проблема вирусного заражения	3	8	2	2			4	Опрос, тестирование, решение ситуаций, предоставление докладов и рефератов
9	Перспективные методы антивирусной защиты	3	9	-	2			4	Фронтальный опрос, тестирование, решение кейсов, предоставление докладов
10	Основные классы антивирусных программ	3	10	-	2			4	Опрос, дискуссия тестирование, предоставление докладов и рефератов
	Итого по модулю 2	3	**36**	**4**	**4**			**28**	Контрольная работа
Модуль 3. Защита от утечки информации по техническим каналам и организационно-правовое обеспечение информационной безопасности									
11	Криптографические методы защиты информации	3	11-12	-	2			8	Фронтальный опрос, тестирование, решение кейсов, предоставление докладов и рефератов
9	Проблемы защиты информации в сетях ЭВМ	3	13-14	-	-			8	Опрос, дискуссия тестирование, решение кейсов, предоставление докладов и рефератов
10	Организационная защита информации. Комплексное обеспечение безопасности	3	15-16	2	-			6	Фронтальный опрос, тестирование, решение кейсов, предоставление докладов и рефератов
11	Правовые основы защиты информации	3	17-18	-	2			8	Опрос, тестирование, решение ситуаций, предоставление докладов и рефератов
	Итого по модулю 3	3	**36**	**2**	**4**			**30**	Контрольная работа
	Модуль 4 Подготовка к экзамену	3						**27**	**9** - Экзамен
	ИТОГО		**144**	**8**	**10**			**117**	**9**

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

4.3.1. Содержание лекционных занятий по дисциплине.

Модуль 1. Основные понятия, определения и угрозы информационной безопасности

Тема 1. Информация. Информационная сфера

Введение. Предмет и задачи информационной безопасности. Значение и содержание дисциплины. Эволюция подходов к обеспечению информационной безопасности.

Содержание понятия «Информация». Формы информации. Информация как объект исследования. Понятия информационного воздействия и информационного взаимодействия. Составляющие информационной сферы. Свойства информации в форме сведений и в форме сообщений.

Тема 2. Национальные интересы и безопасность России

Принципы соблюдения информационной безопасности. Две классификации национальных интересов. Основные составляющие национальных интересов в информационной сфере.

Общие методы обеспечения информационной безопасности. Понятие информационных ресурсов. Основные классы информационных ресурсов

Тема 3. Информационная война. Информационное оружие

Интересы и угрозы в области информационной безопасности. Составляющие национальной безопасности. Проблемы информационной войны. Классификация информационного оружия. Основные объекты воздействия в информационной войне. Цели информационной войны. Понятия начала и окончания войны.

Тема 4. Угрозы безопасности России.

Виды угроз безопасности России. Классификация угроз. Понятие «Интегральная информационная безопасность». Схема основных элементов и объектов защиты в АСОД. Угрозы безопасности в АСОД.

Мировые стандарты в области информационной безопасности. Основные компоненты критериев безопасности ITSEC. Процесс управления рисками. Общая схема анализа безопасности.

Модуль 2. Защита от несанкционированного доступа, компьютерные вирусы и антивирусные программы

Тема 5. Показатели защищенности СВТ

Функции и задачи защиты информации. Функции непосредственной защиты. Механизмы защиты. Управление механизмами защиты.

Основные группы факторов, влияющие на информационную безопасность технической системы. Класс и показатели защищенности СВТ (АС).

Тема 6. Защита информации в АСОД

Понятие защиты информации. Понятие защиты информации в АСОД. Основные методы защиты информации в вычислительных сетях. Методы, применяемые для установления подлинности различных объектов

Тема 7. Виды доступа. Уровни доступа. Контроль доступа

Виды доступа к информации. Обязательное доведение. Свободный доступ. Ограничения и запреты. Виды информации с ограниченным доступом.

Методы защиты информации от преднамеренного доступа (при применении простых средств хранения и обработки информации). Идентификация и аутентификация пользователя.

Тема 8. Проблема вирусного заражения

Компьютерный вирус (закладка): понятие, пути распространения, проявление действия вируса. проникновения Структура современных вирусов: модели поведения вирусов; деструктивные действия вируса; разрушение программ защиты, схем контроля или изменение состояния программной среды. Воздействия на программно-аппаратные средства защиты информации. Последствия от вирусных вторжений и катастроф

Тема 9. Перспективные методы антивирусной защиты

Перспективные методы антивирусной защиты. Антивирусные проверки на ПК, на файловых серверах и серверах приложений, на прокси-серверах, на межсетевых экранах. Борьба со спамом. Базовые однолинейные методы. Спаморборона.

Тема 10. Основные классы антивирусных программ

Программы-детекторы, программы-доктора, программы - ревизоры, программы-фильтры. Антивирусные программы. Профилактика заражения вирусом.

Модуль 3. Защита от утечки информации по техническим каналам и организационно-правовое обеспечение информационной безопасности

Тема 11. Криптографические методы защиты информации

Периоды развития криптологии. Первые шифры. Два направления в криптологии. Цели криптографии и криптоанализа. Разделы криптографии. Стеганография. Закрытие информацию методами замены, перестановки, с помощью аналитических преобразований.

Тема 12. Проблемы защиты информации в сетях ЭВМ

Защита информации в ПК. Сервисы безопасности. Архитектура механизмов защиты в сетях. Международные стандарты. Межсетевые экраны. Прокси - серверы.

Тема 13. Организационная защита информации. Комплексное обеспечение безопасности

Сущность ОЗИ и ее место в комплексной системе защиты информации. Виды ОЗИ. Лицензирование деятельности предприятия по проведению

работ, связанных с использование сведений составляющих государственную тайну.

Организация физической охраны предприятия. Источники. Состав и назначение должностных инструкций. Порядок создания, утверждения и исполнения должностных инструкций.

Тема 14. Правовые основы защиты информации

Опыт законодательного регулирования информатизации в России и за рубежом. Концепция правового обеспечения информационной безопасности в России.

Стандарты и нормативно-методические документы в области обеспечения информационной безопасности. Государственная система обеспечения информационной безопасности. Международные правовые акты по защите информации.

4.3.2. Содержание практических занятий по дисциплине.

Модуль 1. Основные понятия, определения и угрозы информационной безопасности

Тема 1. Информация. Информационная сфера

1. Предмет и задачи информационной безопасности.
2. Эволюция подходов к обеспечению информационной безопасности.
3. Свойства информации в форме сведений и в форме сообщений.

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

Тема 2. Национальные интересы и безопасность России

1. Принципы соблюдения информационной безопасности.
2. Основные составляющие национальных интересов в информационной сфере.
3. Общие методы обеспечения информационной безопасности.

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

Тема 3. Информационная война. Информационное оружие

1. Интересы и угрозы в области информационной безопасности.
2. Проблемы информационной войны. Классификация информационного оружия.

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

Тема 4. Угрозы безопасности России.

Виды угроз безопасности России. Классификация угроз.

Понятие «Интегральная информационная безопасность».

Мировые стандарты в области информационной безопасности.

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

Модуль 2. Защита от несанкционированного доступа, компьютерные вирусы и антивирусные программы

Тема 5. Показатели защищенности СВТ

1. Функции и задачи защиты информации.
2. Основные группы факторов, влияющие на информационную безопасность технической системы.

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

Тема 6. Защита информации в АСОД

1. Понятие защиты информации. Понятие защиты информации в АСОД.
2. Основные методы защиты информации в вычислительных сетях.

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

Тема 7. Виды доступа. Уровни доступа. Контроль доступа

1. Виды доступа к информации. Виды информации с ограниченным доступом.
2. Методы защиты информации от преднамеренного доступа (при применении простых средств хранения и обработки информации).

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

Тема 8. Проблема вирусного заражения

1. Компьютерный вирус (закладка): понятие, пути распространения, проявление действия вируса. проникновения
2. Структура современных вирусов: модели поведения вирусов; деструктивные действия вируса; разрушение программ защиты, схем контроля или изменение состояния программной среды.
3. Последствия от вирусных вторжений и катастроф

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

Тема 9. Перспективные методы антивирусной защиты

Перспективные методы антивирусной защиты.

Антивирусные проверки на ПК, на файловых серверах и серверах приложений, на прокси-серверах, на межсетевых экранах.

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

Тема 10. Основные классы антивирусных программ

1. Понятие и виды антивирусных программ.
2. Профилактика заражения вирусом.

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

Модуль 3. Защита от утечки информации по техническим каналам и организационно-правовое обеспечение информационной безопасности

Тема 11. Криптографические методы защиты информации

1. Периоды развития криптологии. Цели криптографии и криптоанализа.
2. Закрытие информации методами замены, перестановки, с помощью аналитических преобразований.

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

Тема 12. Проблемы защиты информации в сетях ЭВМ

1. Защита информации в ПК.
2. Сервисы безопасности. Архитектура механизмов защиты в сетях.

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

Тема 13. Организационная защита информации. Комплексное обеспечение безопасности

Сущность ОЗИ и ее место в комплексной системе защиты информации.

Виды ОЗИ.

Организация физической охраны предприятия.

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

Тема 14. Правовые основы защиты информации

1. Концепция правового обеспечения информационной безопасности в России.
2. Стандарты и нормативно-методические документы в области обеспечения информационной безопасности.
3. Государственная система обеспечения информационной безопасности.
4. Международные правовые акты по защите информации.

Ссылки на учебную литературу, указанную в п. 8: (1,2,3,4,5).

5. **Образовательные технологии**

Учебный процесс в современном вузе должен быть направлен не столько на передачу знаний и развитие умений и навыков у студентов, сколько на формирование у них адекватного условиям инновационной экономики реального поведения, соответствующего отношения к своей будущей рациональной практике производственной деятельности. Это обеспечивается применением основного метода обучения – обсуждением конкретных ситуаций, или применением метода case-study на практических занятиях. С помощью case-study обучающиеся обретают нечто, что меняет их видение мира и себя, что даёт им возможность действовать не так, как ранее, что придаёт им некие новые качества, которыми они не обладали ранее. Использование метода конкретных ситуаций (МКС) основывается на вере в то, что управление есть больше навык и умение, чем знание. Лучший способ развития навыков и умений – это тренировка через моделирование действий (подобно пианисту).

Именно благодаря МКС студент становится активным творцом знаний, решений, информации. Этот метод обеспечивает процесс обучения действием на основе стимулирования самостоятельной работы студентов (написания дома письменного анализа конкретных ситуаций - ПАКСов), развития умения решать проблемы, активного вовлечения студентов в обсуждение конкретных реальных ситуаций на учебном занятии. Акцент делается на изменение позиции обучающегося в реальном мире, на созидание, на развитие способностей воображения, способностей достигать результатов, т.е. на учение.

На метод проекта в образовании стали возлагать огромные надежды, связанные с его возможностями организовывать обучение в процессе деятельности, развивать способность применять знания, умения и навыки для решения практических, жизненно важных задач. В этом смысле проектирование (метод проекта) стало рассматриваться как средство для развития компетенций. При этом список компетенций, формируемых в процессе проектирования, как правило, уточняется, изменяется в разных образовательных практиках.

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 студентов, предусмотренная учебным планом в объеме не менее 50% от общего количества часов, направлена на более глубокое усвоение изучаемого курса, формирование навыков исследовательской работы и ориентирование студентов на умение применять теоретические знания на практике. Задания для самостоятельной работы составлены по разделам, которые требуют дополнительной проработки и анализа материала в объеме запланированных часов.

Самостоятельная работа по дисциплине «Информационная безопасность» (36 часов) предусматривает:

Разделы дисциплины	Виды самостоятельной работы (и ссылки на литературу[1])	Количество часов	Форма контроля
Раздел 1. Основные понятия, определения и угрозы информационной безопасности	проработка учебного материала, решение задач, выполнение кейса, обработка аналитических данных, подготовка докладов к участию в тематических дискуссиях, работа с тестами и вопросами. (1, 2, 3, 4, 5, 6, 7, 8,9, 10, 11)	16	Конспектирование первоисточников и другой учебной литературы
Раздел 2. Защита от	проработка учебного материала, решение задач, выполнение	12	Тестирование, дискуссия,

несанкционированного доступа, компьютерные вирусы и антивирусные программы	кейса, обработка аналитических данных, подготовка докладов к участию в тематических дискуссиях, работа с тестами и вопросами. (1, 2, 3, 4, 5, 6, 7, 8,9, 10, 11)		опрос, проверка домашнего задания, обсуждение докладов
Раздел 3. Защита от утечки информации по техническим каналам и организационно-правовое обеспечение информационной безопасности	проработка учебного материала, работа с электронными источниками, решение задач, выполнение кейса, контрольных работ, подготовка рефератов, работа с тестами и вопросами (1, 2, 3, 4, 5, 6, 7, 8,9, 10, 11)	8	Тестирование дискуссия, опрос, проверка домашнего задания, обсуждение докладов
Итого		**36**	

Примерная тематика рефератов по модулям и темам дисциплины

1.Методы борьбы с фишинговыми атаками.

2.Законодательство о персональных данных.

3.Защита авторских прав.

4.Назначение, функции и типы систем видеозащиты.

5.Как подписывать с помощью ЭЦП электронные документы различных форматов.

6.Обзор угроз и технологий защиты Wi-Fi-сетей.

7.Проблемы внедрения дискового шифрования.

8.Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.

9.Особенности процессов аутентификации в корпоративной среде.

10.Квантовая криптография.

11.Утечки информации: как избежать. Безопасность смартфонов.

12.Безопасность применения пластиковых карт - законодательство и практика.

13.Защита CD- и DVD-дисковот копирования.

14.Современные угрозы и защита электронной почты.

15.Программные средства анализа локальных сетей на предмет уязвимостей.

16.Безопасность применения платежных систем - законодательство и практика.

17.Аудит программного кода по требованиям безопасности.

18.Антишпионское ПО (antispyware).

19.Обеспечение безопасности Web-сервисов.

20.Защита от внутренних угроз.

21.Технологии RFID.

22.Уничтожение информации на магнитных носителях.
23.Ботнеты - плацдарм современных кибератак.
24.Цифровые водяные знаки в изображениях.
25.Электронный документооборот. Модели нарушителя.
26.Идентификация по голосу. Скрытые возможности.
27.Безопасность океанских портов.
28.Безопасность связи.
29.Безопасность розничной торговли.
30.Банковская безопасность.
31.Информатизация управления транспортной безопасностью.
32.Биопаспорт.
33.Обзор современных платформ архивации данных.
34.Что такое консалтинг в области ИБ.
35.Бухгалтерская отчетность как источник рассекречивания информации.
36.Управление рисками: обзор употребительных подходов.
37.Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.
38.Распределенные атаки на распределенные системы.
39.Оценка безопасности автоматизированных систем.
40.Windows и Linux: что безопаснее?
41.Функциональная безопасность программных средств.
42.Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.
43.Информационная безопасность: экономические аспекты.

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 и наименование компетенции из ФГОС ВО	**Код и наименование индикатора достижения компетенций** *(в соответствии с ОПОП (при наличии))*	**Планируемые результаты обучения**	**Процедура освоения**
ОК-12	способность работать с различными информационными	*Знает*: понятия «Информация», различие понятия информационного воздействия и	Дискуссия, письменный опрос, устный опрос

	ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	информационного взаимодействия, свойства информации в форме сведений и в форме сообщений, виды информации как объекта исследования, основные международные правовые акты по защите информации, основные положения и принципы международных соглашений, соответствие российских и международных правовых отношений, российские общегосударственные правовые документы по защите информации, российские отраслевые нормативные документы по защите информации *Умеет*: применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации *Владеет*: практическими навыками работы с различными информационными ресурсами и технологиями	
ОПК-3	способность применять основные закономерности создания и принципы функционирования систем экономической безопасности хозяйствующих субъектов	*Знает*: основные закономерности создания и принципы функционирования систем информационной безопасности хозяйствующих субъектов *Умеет*: выделять основные составляющие национальных интересов в информационной сфере безопасности, относить информационные ресурсы к различным классам *Владеет*: практическими навыками использования новейших технологий в области информационной безопасности	Устный опрос, письменный опрос, дискуссия

7.2. Типовые контрольные задания

Примерные тестовые задания

1. Сведения (сообщения, данные) независимо от формы их представления:

1. Информация
2. Информационные технологии
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Обладатель информации

2. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов:

1. Информация
2. Информационные технологии
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Обладатель информации

3. Л**ицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации:**

1. Источник информации
2. Потребитель информации
3. Уничтожитель информации
4. Носитель информации
5. Обладатель информации

4.Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники это:

1. База данных
2. Информационная технология
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Медицинская информационная система

5. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя это:

1. Электронное сообщение
2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации

6. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц это:

1. Уничтожение информации

2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации

7. Возможность получения информации и ее использования это:

1. Сохранение информации
2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации

8. Обеспечение информационной безопасности есть обеспечение…

1. Независимости информации
2. Изменения информации
3. Копирования информации
4. Сохранности информации
5. Преобразования информации

9. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети:

1. Электронное сообщение
2. Информационное сообщение
3. Текстовое сообщение
4. Визуальное сообщение
5. SMS-сообщение

10. Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные это:

1. Информационная система персональных данных
2. База данных
3. Централизованное хранилище данных
4. Система Статэкспресс
5. Сервер

11. К сведениям конфиденциального характера относятся:

1. Информация о распространении программ
2. Информация о лицензировании программного обеспечения
3. Информация, размещаемая в газетах, Интернете
4. Персональные данные
5. Личная тайна

12. Отношения, связанные с обработкой персональных данных, регулируются законом…

1. «Об информации, информационных технологиях»
2. «О защите информации»
3. Федеральным законом «О персональных данных»
4. Федеральным законом «О конфиденциальной информации»
5. «Об утверждении перечня сведений конфиденциального характера»

13. Действия с персональными данными (согласно закону), включая сбор, систематизацию, накопление, хранение, использование, распространение - это:

1. «Исправление персональных данных»
2. «Работа с персональными данными»
3. «Преобразование персональных данных»
4. «Обработка персональных данных»
5. «Изменение персональных данных»

14. Действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных:

1. Выделение персональных данных
2. Обеспечение безопасности персональных данных
3. Деаутентификация
4. Деавторизация
5. Деперсонификация

15. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на:

1. **Многопользовательские**
2. Однопользовательские
3. Без разграничения прав доступа
4. С разграничением прав доступа
5. Системы, не имеющие подключений

16. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом:

1. Авторизация
2. Аутентификация
3. Обезличивание
4. Деперсонализация
5. Идентификация

17. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации:

1. Авторизация
2. Обезличивание
3. Деперсонализация
4. Аутентификация
5. Идентификация

18. Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых действий в системах с ограниченным доступом

1. Авторизация

2. Идентификация
3. Аутентификация
4. Обезличивание
5. Деперсонализация

19. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название:

1. Токен
2. Password
3. Пароль
4. Login
5. Смарт-карта

20. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:

1. Идентификация
2. Аутентификация
3. Авторизация
4. Экспертиза
5. Шифрование

Примерный перечень вопросов к экзамену

1. Предмет и задачи информационной безопасности.
2. Эволюция подходов к обеспечению информационной безопасности.
3. Содержание понятия «Информация». Формы информации.
4. Информация как объект исследования.
5. Понятия информационного воздействия и информационного взаимодействия.
6. Свойства информации в форме сведений и в форме сообщений.
7. Национальные интересы и безопасность России.
8. Принципы соблюдения информационной безопасности. Классификация
9. Основные составляющие национальных интересов в информационной сфере.
10. Общие методы обеспечения информационной безопасности.
11. Понятие информационных ресурсов. Основные классы информационных ресурсов
12. Виды информационных угроз.
13. Интересы и угрозы в области информационной безопасности.
14. Составляющие национальной безопасности.
15. Проблемы информационной войны.
16. Классификация информационного оружия. Основные объекты воздействия в информационной войне.

17. Цели информационной войны. Понятия начала и окончания войны.

18. Виды угроз безопасности России. Классификация угроз.

19. Понятие «Интегральная информационная безопасность».

20. Схема основных элементов и объектов защиты в АСОД. Угрозы безопасности в АСОД.

21. Мировые стандарты в области информационной безопасности.

22. Основные компоненты критериев безопасности ITSEC.

23. Процесс управления рисками.

24. Общая схема анализа безопасности.

25. Защита от несанкционированного доступа.

26. Показатели защищенности СВТ.

27. Функции и задачи защиты информации.

28. Функции непосредственной защиты информации.

29. Механизмы защиты информации. Управление механизмами защиты.

30. Основные группы факторов, влияющие на информационную безопасность технической системы.

31. Понятие защиты информации.

32. Понятие защиты информации в АСОД.

33. Основные методы защиты информации в вычислительных сетях.

34. Методы, применяемые для установления подлинности различных объектов.

35. Виды доступа к информации. Обязательное доведение. Свободный доступ.

36. Ограничения и запреты. Виды информации с ограниченным доступом.

37. Методы защиты информации от преднамеренного доступа (при применении простых средств хранения и обработки информации).

38. Идентификация и аутентификация пользователя.

39. Уровни доступа и контроль доступа к информации.

40. Компьютерный вирус (закладка): понятие, пути распространения, проявление действия вируса. проникновения

41. Структура современных вирусов: модели поведения вирусов; деструктивные действия вируса; разрушение программ защиты, схем контроля или изменение состояния программной среды.

42. Воздействия на программно-аппаратные средства защиты информации.

43. Последствия от вирусных вторжений и катастроф.

44. Перспективные методы антивирусной защиты.

45. Антивирусные проверки на ПК, на файловых серверах и серверах приложений, на прокси-серверах, на межсетевых экранах.

46. Методы и способы борьбы со спамом. Базовые однолинейные методы. Спаморборона.

47. Многоплатформенные антивирусные и антиспамовые решения компании Sophos.

48. Программы-детекторы, программы-доктора, программы - ревизоры, программы-фильтры.

49. Интегрированные антиспамовые и антивирусные решения от компании Sybari.

50. Антивирусные программы семейства Dr.Web® для рабочих станций.

51. Программы – антивирусы: Aidstest, Adinf, Norton Antivirus, AVP. Профилактика заражения вирусом.

52. Защита от утечки информации по техническим каналам.

53. Криптографические методы защиты информации.

54. Периоды развития криптологии, направления и разделы криптологии.

55. Цели криптографии и криптоанализа.

56. Разделы криптографии. Стеганография.

57. Закрытие информацию методами моноалфавитной и полиалфавитной подстановки, перестановки, с помощью аналитических преобразований, методом гаммирования.

58. Система с открытым ключом. Электронно-цифровая подпись.

59. Приемы хеширования.

60. Работа с криптоцениром MS OutLook.

61. Защита информации в ПК. Сервисы безопасности.

62. Архитектура механизмов защиты в сетях.

63. Проблемы защиты информации в сетях ЭВМ.

64. Международные стандарты. Межсетевые экраны. Прокси серверы.

65. Организационно-правовое обеспечение ИБ.

66. Организационная защита информации.

67. Сущность ОЗИ и ее место в комплексной системе защиты информации.

68. Виды ОЗИ. Лицензирование деятельности предприятия по проведению работ, связанных с использование сведений составляющих государственную тайну.

69. Комплексное обеспечение информационной безопасности.

70. Правовые основы защиты информации.

71. Законодательное регулирование информатизации в России и за рубежом.

72. Концепция правового обеспечения информационной безопасности РФ.

73. Стандарты и нормативно-методические документы в области обеспечения информационной безопасности.

74. Государственная система обеспечения информационной безопасности.

75. Международные правовые акты по защите информации.

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 - 10 баллов (на каждом занятии),
- участие на практических занятиях 70 - баллов (на каждом занятии),
- выполнение самостоятельной работы - 20 баллов.
- выполнение контрольных работ - 100 баллов (1 теоретический вопрос - 20 баллов, 15 тестов – 30 баллов, решение задачи – 50 баллов).

Промежуточный контроль по дисциплине включает:

- устный опрос - 50 баллов,
- решение задачи- 50 баллов

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

а) основная литература:

1. Горбенко А.О. Основы информационной безопасности (введение в профессию) [Электронный ресурс] : учебное пособие / А.О. Горбенко. — Электрон. текстовые данные. — СПб. : Интермедия, 2017. — 335 c. — 978-5-4383-0136-3. — Режим доступа: http://www.iprbookshop.ru/66797.html
2. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 c. — 978-5-94774-821-5. — Режим доступа: http://www.iprbookshop.ru/52209.html

б) дополнительная литература:

3. Основы информационной безопасности [Электронный ресурс] : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В.Ю. Рогозин [и др.]. — Электрон. текстовые данные. — М. : ЮНИТИ-ДАНА, 2017. — 287 c. — 978-5-238-02857-6. — Режим доступа: http://www.iprbookshop.ru/72444.html
4. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А.Е. Фаронов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52160.htmlЛихоносов А.Г. Защита и обработка конфиденциальных документов: учеб. пособие М.:Юридический институт МИИТа, 2011-36с.

5. Нестеров С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Нестеров С.А.. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 c. — 978-5-7422-4331-1. — Режим доступа: http://www.iprbookshop.ru/43960.html

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

1. Государственные программы Российской Федерации: Официальный портал госпрограмм РФ. [Электронный ресурс]. URL: http://programs.gov.ru/portal (дата обращения 12.03.2018).
2. Справочно-правовая система «КонсультантПлюс» [Электронный ресурс] – URL: http://www.consultant.ru (дата обращения 08.06.2018).
3. Информационно-правовой портал «Гарант.ру» [Электронный ресурс] – URL: http://www.garant.ru (дата обращения 05.06.2018).
4. 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).
5. eLIBRARY.RU[Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва. – URL: http://elibrary.ru/defaultx.asp (дата обращения 05.02.2018).

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 может быть 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.

Для проведения индивидуальных консультаций может использоваться также электронная почта.

Программное обеспечение:

1. Windows 10
2. Windows 8.1
3. Access 2016
4. Kaspersky System Center 10
5. ABBYY FineReader 10
6. Электронный словарь ABBYYLingvo
7. Интернет-версия системы ГАРАНТ
8. Справочная правовая система «КонсультантПлюс»
9. Microsoft Office
10. Windows 2008 serverrus
11. MS Office Standard 2010 Professional Russian

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

Учебная аудитория, мультимедиа проектор, ноутбук, доска, наглядные пособия, специализированная мебель: столы, стулья.