

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ

Директор Пятигорского института
(филиал) СКФУ

_____ Т.А. Шебзухова
«__» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы информационной безопасности

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Направление подготовки/специальность 10.03.01 Информационная безопасность

Квалификация выпускника: бакалавр

Форма обучения очная

Год начала обучения 2021

Изучается в 1 семестре

г. Пятигорск 20__ г.

1. Цель и задачи освоения дисциплины

Целью освоения дисциплины «Основы информационной безопасности» является формирование набора общекультурных и профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Задачами освоения дисциплины являются: формирование базовых понятий в области информационной безопасности и защиты информации, осознание места и роли информационной безопасности в системе национальной безопасности РФ и выработка первоначальных практических навыков по защите документов на персональном компьютере.

2. Место дисциплины в структуре основной образовательной программы

Дисциплина относится к дисциплинам базовой части (Б1.Б.28). Ее освоение происходит в 1 семестре.

3. Связь с предшествующими дисциплинами

Дисциплина реализуется в 1 семестре

4. Связь с последующими дисциплинами

Пререквизитами данной дисциплины являются предметы: «Теоретические основы защиты информации», «Информационная среда и информационная безопасность», «Персональная кибербезопасность», «Ознакомительная практика», «Подготовка к сдаче и сдача государственного экзамена»

5. Компетенции обучающегося, формируемые в результате изучения дисциплины

5.1 Наименование компетенции

Код	Формулировка:
ОК-5	способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-9	способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
ПК-10	способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

5.2 Знания, умения и навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций

Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: <ul style="list-style-type: none">социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты	ОК-5

<p>интересов личности, общества и государства, соблюдать нормы профессиональной этики;</p> <p>Уметь:</p> <ul style="list-style-type: none"> ▪ понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики <p>Владеть:</p> <ul style="list-style-type: none"> ▪ навыками понимания социальной значимости своей будущей профессии, обладания высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдения нормы профессиональной этики 	
<p>Знать:</p> <ul style="list-style-type: none"> ▪ значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации <p>Уметь:</p> <ul style="list-style-type: none"> ▪ понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации. <p>Владеть:</p> <ul style="list-style-type: none"> ▪ навыками понимания значения информации в развитии современного общества, применения информационных технологий для поиска и обработки информации 	ОПК-4
<p>Знать:</p> <ul style="list-style-type: none"> ▪ информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты <p>Уметь:</p> <ul style="list-style-type: none"> ▪ определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты <p>Владеть:</p> <ul style="list-style-type: none"> ▪ навыками определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания 	ОПК-7

информационных процессов и особенностей функционирования объекта защиты	
<p>Знать:</p> <ul style="list-style-type: none"> ▪ современные методы осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности <p>Уметь:</p> <ul style="list-style-type: none"> ▪ осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности <p>Владеть:</p> <ul style="list-style-type: none"> ▪ основными принципами, методами осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности 	ПК-9
<p>Знать:</p> <ul style="list-style-type: none"> ▪ современные методы анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности <p>Уметь:</p> <ul style="list-style-type: none"> ▪ проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности <p>Владеть:</p> <ul style="list-style-type: none"> ▪ основными принципами, методами осуществления анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности 	ПК-10

6. Объем учебной дисциплины/модуля

Объем занятий: Итого	135ч.	5з.е.
В т.ч. аудиторных	21 ч.	
Из них:		
Лекций	7,5 ч.	
Лабораторных работ	13,5 ч.	
Практических занятий	– ч.	

Самостоятельной работы
Зачет с оценкой

114 ч.
1 семестр

7. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества астрономических часов и видов занятий

7.1 Тематический план дисциплины

№	Раздел (тема) дисциплины	Реализуемые компетенции	Контактная работа обучающихся с преподавателем, часов				Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	
1 семестр							
	Раздел 1. Модель информационной безопасности и правовое регулирование информационной безопасности в РФ.						
1	Тема 1. Терминологические основы информационной безопасности.	ОК-5, ОПК-4, ОПК-7, ПК-9, ПК-10			1,5	13	
	Раздел 2. Правовая защита информации и защита информации, отнесенной к государственной тайне.						
2	Тема 2. Характеристика правовых способов защиты информации.	ОК-5, ОПК-4, ОПК-7, ПК-9			1,5	13	
	Раздел 3. Защита персональных данных.						
3	Тема 3. Понятие персональных данных и основные категории в сфере их защиты.	ОК-5, ОПК-4, ОПК-7, ПК-9, ПК-10	1,5		1,5	13	
	Раздел 4. Угрозы в сфере защиты информации и способы противодействия им.						
4	Тема 4. Классификация угроз в сфере защиты информации.	ОК-5, ОПК-4, ОПК-7, ПК-9, ПК-10	1,5		1,5	13	

	Раздел 5. Виды защиты информации.					
5	Тема 5. Организационная защита информации.	ОК-5, ОПК-4, ОПК-7, ПК-9, ПК-10	1,5		1,5	13
	Раздел 6. Программные и криптографические средства защиты информации.					
6	Тема 6. Программные средства защиты информации.	ОК-5, ОПК-4, ОПК-7, ПК-9, ПК-10	1,5		1,5	13
	Раздел 7. Защита от утечки информации.					
	Тема 7. Пресечение разглашения конфиденциальной информации.	ОК-5, ОПК-4, ОПК-7, ПК-9, ПК-10			1,5	12
	Раздел 8. Обеспечение сохранности коммерческой тайны.					
	Тема 8. Основные категории в области коммерческой тайны.	ОК-5, ОПК-4, ОПК-7, ПК-9, ПК-10			1,5	12
	Раздел 9. Аудит информационной безопасности.					
	Тема 9. Понятие аудита информационной безопасности.	ОК-5, ОПК-4, ОПК-7, ПК-9, ПК-10	1,5		1,5	12
	Итого за 1 семестр		7,5		13,5	114
	Итого		7,5		13,5	114

7.2 Наименование и содержание лекций

№	Наименование разделов и тем дисциплины, их краткое содержание	Объем часов	Форма проведения
	1 семестр		
3	Тема 3. Понятие персональных данных и основные категории в сфере их защиты. Принципы обработки персональных данных.	1,5	
4	Тема 4. Классификация угроз в сфере защиты информации. Меры обеспечения информационной безопасности. Организационные, организационно-технические и технические мероприятия обеспечения информационной безопасности. Способы неправомерного овладения конфиденциальной информацией.	1,5	
5	Тема 5. Организационная защита информации. Инженерно-техническая защита информационной	1,5	

	безопасности. Аппаратные средства защиты информации.		
6	Тема 6. Программные средства защиты информации. Защита от несанкционированного доступа в информационную систему. Защита от копирования и разрушения. Вирусы и антивирусные программы. Криптографические средства защиты информации. Шифрование речи.	1,5	
9	Тема 9. Понятие аудита информационной безопасности. Система обнаружения компьютерных атак.	1,5	
	Итого за 1 семестр	7,5	-
	Итого	7,5	-

7.3 Наименование и содержание лабораторных работ

№	Наименование темы лабораторных занятий	Объем часов	Форма проведения
	1 семестр		
1	Лабораторная работа № 1. Защита баз данных на примере MS ACCESS.	1,5	
2	Лабораторная работа № 2. Введение в систему MathCad.	1,5	
3	Лабораторная работа № 3. Датчики случайных чисел.	1,5	
4	Лабораторная работа № 4. Шифр Цезаря.	1,5	
5	Лабораторная работа № 5. Алгоритм шифрования XOR.	1,5	
6	Лабораторная работа № 6. Изучение системы охранной сигнализации на базе оборудования «Болид». Настройка тактики работы системы охранной сигнализации при помощи программы «Pprog».	1,5	
7	Лабораторная работа № 7. Изучение системы Орион Про на базе оборудования «Болид». Настройка уровней доступа для охранно-пожарной системы при помощи программы «Pprog».	1,5	
8	Лабораторная работа № 8. Изучение системы Орион Про на базе оборудования «Болид». Настройка паролей для охранно-пожарной системы при помощи программы «Pprog».	1,5	
9	Лабораторная работа № 9. Изучение системы пожарной сигнализации на базе оборудования «Болид».	1,5	
	Итого за 1 семестр	13,5	-
	Итого	13,5	-

7.4 Наименование практических занятий

Практические работы учебным планом не предусмотрены

7.5 Технологическая карта самостоятельной работы обучающегося

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ОК-5, ОПК-4, ОПК-7, ПК-9, ПК-10	Подготовка к лекциям	Конспект	Собеседование	0,68	0,07	0,75
ОК-5, ОПК-4, ОПК-7, ПК-9, ПК-10	Самостоятельное изучение литературы по темам 1-9	Конспект	Собеседование	98,28	10,92	109,2
ОК-5, ОПК-4, ОПК-7, ПК-9, ПК-10	Подготовка к лабораторным занятиям	Индивидуальное задание	Отчет письменный	3,65	0,40	4,05
Итого				102,6	11,4	114

8. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

8.1 Перечень компетенций с указанием этапов их формирования в процессе освоения ОП ВО. Паспорт фонда оценочных средств

Фонд оценочных средств, позволяющий оценить уровень сформированности компетенций, размещен в УМК дисциплины «Основы управленческой деятельности» на кафедре информационной безопасности, систем и технологий и представлен следующими компонентами:

Код оцениваемой компетенции	Этап формирования компетенции (№ темы)	Средства и технологии оценки	Тип контроля (текущий /промежуточный)	Вид контроля (текущий/промежуточный)	Наименование оценочного средства
ОК-5, ОПК-4, ОПК-7, ПК-9, ПК-10	Темы 1-6	собеседование	текущий	устный	Вопросы для собеседования
ОК-5, ОПК-4, ОПК-7, ПК-9, ПК-10	Темы 1-9	отчет письменный	текущий	письменный, с помощью технических средств	Темы индивидуальных заданий для письменного отчета

8.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Уровни сформированности компетенций	Индикаторы	Дескрипторы			
		2 балла	3 балла	4 балла	5 баллов
Базовый	ОК-5				
	Знать социальную значимость	Не уверен в знаниях	Не достаточно хорошо знает:	Знать социальную значимость своей	

<p>области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдения нормы профессиональной этики</p>	<p>деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдения нормы профессиональной этики</p>	<p>деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдения нормы профессиональной этики, однако не достаточно хорошо применяет их на практике</p>	<p>профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдения нормы профессиональной этики</p>	
ОПК-4				
<p>Знать ■ значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации</p>	<p>Не уверен в знаниях ■ значения информации в развитии современного общества, применять информационные технологии для поиска и обработки информации</p>	<p>Не достаточно хорошо знает: значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации</p>	<p>Знает ■ значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации</p>	
<p>Уметь ■ понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.</p>	<p>Не умеет понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.</p>	<p>Не достаточно хорошо умеет понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.</p>	<p>Умеет понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.</p>	
<p>Владеть навыками понимания значения информации в развитии современного общества,</p>	<p>Не владеет навыками понимания значения информации в развитии современного общества,</p>	<p>Владеет навыками понимания значения информации в развитии современного общества,</p>	<p>Владеет на достаточно хорошем уровне навыками понимания значения информации в развитии</p>	

применения информационных технологий для поиска и обработки информации	применения информационных технологий для поиска и обработки информации	применения информационных технологий для поиска и обработки информации	современного общества, применения информационных технологий для поиска и обработки информации	
ОПК-7				
Знать информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Не уверен в знаниях информационных ресурсов, подлежащих защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Не достаточно хорошо знает: информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знает <ul style="list-style-type: none"> ■ информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты 	
Уметь определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Не умеет определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Не достаточно хорошо умеет определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Умеет определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
Владеть навыками определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на	Не владеет навыками определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных	Владеет навыками определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных	Владеет на достаточно хорошем уровне навыками определения информационных ресурсов, подлежащих защите, угроз безопасности	

<p>основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>	<p>путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>	<p>путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты, однако не достаточно хорошо применяет их на практике</p>	<p>информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>	
ПК-9				
<p>Знать современные методы осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности</p>	<p>Не знает современные методы осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности</p>	<p>▪ Не достаточно хорошо знает современные методы осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности</p>	<p>Знать современные методы осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности</p>	
<p>Уметь: ▪ осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов,</p>	<p>Не умеет осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических</p>	<p>Не достаточно хорошо умеет осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов,</p>	<p>Умеет осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам</p>	

составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	обеспечения информационной безопасности по профилю своей профессиональной деятельности	
Владеть основными принципами, методами осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Не владеет основными принципами, методами осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Владеет основными принципами, методами осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Достаточно хорошо владеет основными принципами, методами осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	
ПК-10				
Знать современные методы анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Не знает современные методы анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Не достаточно знает современные методы анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знает на достаточно хорошем уровне современные методы анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	
Уметь: проводить анализ	Не умеет проводить	Не достаточно хорошо умеет	Достаточно хорошо умеет	

	информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	анализ информационн ой безопасности объектов и систем на соответствие требованиям стандартов в области информационн ой безопасности	проводить анализ информационн ой безопасности объектов и систем на соответствие требованиям стандартов в области информационн ой безопасности	проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	
	Владеет основными принципами, методами осуществления анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Владеет основными принципами, методами осуществления анализа информационн ой безопасности объектов и систем на соответствие требованиям стандартов в области информационн ой безопасности, но не применяет возможные пути противодейств ия им	Не достаточно хорошо владеет основными принципами, методами осуществления анализа информационн ой безопасности объектов и систем на соответствие требованиям стандартов в области информационн ой безопасности	На хорошем уровне владеет основными принципами, методами осуществления анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	
Повышенный	ОК-5				
	Знать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональн ой деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональн ой этики;				Знает социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональн ой деятельности в области обеспечения информационн ой безопасности и защиты интересов личности, общества и государства, соблюдать

					нормы профессиональной этики;
	<p>Уметь понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики</p>				<p>Умеет понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики</p>
	<p>Владеть навыками понимания социальной значимости своей будущей профессии, обладания высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдения нормы профессиональной этики</p>				<p>Отлично владеет навыками понимания социальной значимости своей будущей профессии, обладания высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдения нормы профессиональной этики</p>
ОПК -4					
	<p>Знать значение информации в</p>				<p>Знает значение информации в</p>

	развитии современного общества, применять информационные технологии для поиска и обработки информации				развитии современного общества, применять информационные технологии для поиска и обработки информации
	Уметь понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.				Умеет понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.
	Владеть навыками понимания значения информации в развитии современного общества, применения информационных технологий для поиска и обработки информации				Отлично владеет навыками понимания значения информации в развитии современного общества, применения информационных технологий для поиска и обработки информации
ОПК-7					
	Знать информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты				Абсолютно знает информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
	Уметь: определять информационные ресурсы, подлежащие защите, угрозы				Умеет определять информационные ресурсы,

<p>безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>				<p>подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>
<p>Владеть навыками навыками определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>				<p>Уверенно владеет навыками определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>
ПК-9				
<p>Знать современные методы осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности</p>				<p>Абсолютно знает современные методы осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности</p>

					ной деятельности
<ul style="list-style-type: none"> ■ Уметь: осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности 					<ul style="list-style-type: none"> ■ Умеет осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
<p>Владеть основными принципами, методами осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности</p>					<p>Уверенно владеет основными принципами, методами осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности</p>
ПК-10					
Знать современные методы анализа информационной					Абсолютно знает современные методы анализа

	безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности				информационн ой безопасности объектов и систем на соответствие требованиям стандартов в области информационн ой безопасности
	Уметь: проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности				Умеет проводить анализ информационн ой безопасности объектов и систем на соответствие требованиям стандартов в области информационн ой безопасности
	Владеть основными принципами, методами осуществления анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности				Уверенно владеет основными принципами, методами осуществления анализа информационн ой безопасности объектов и систем на соответствие требованиям стандартов в области информационн ой безопасности

8.2 Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по дисциплине оцениваются знания, умения навыки в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

Рейтинговая оценка знаний студента

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
1.	Выполнение лабораторных работ 1-4	8 неделя	25
2.	Выполнение лабораторных работ 4-9	16 неделя	30

	Итого	55
--	--------------	-----------

Максимально возможный балл за весь текущий контроль устанавливается равным **55**. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

Промежуточная аттестация

Промежуточная аттестация в 1 семестре проводится в форме дифференцированного зачета.

Процедура зачета как отдельное контрольное мероприятие не проводится, оценивание знаний обучающегося происходит по результатам текущего контроля.

Зачет выставляется по результатам работы в семестре, при сдаче всех контрольных точек, предусмотренных текущим контролем успеваемости. Если по итогам семестра обучающийся имеет от 33 до 60 баллов, ему ставится отметка «зачтено». Обучающемуся, имеющему по итогам семестра менее 33 баллов, ставится отметка «не зачтено».

Количество баллов за зачет ($S_{зач}$) при различных рейтинговых баллах по дисциплине по результатам работы в семестре

Рейтинговый балл по дисциплине по результатам работы в семестре ($R_{сем}$)	Количество баллов за зачет ($S_{зач}$)
$50 \leq R_{сем} \leq 60$	40
$39 \leq R_{сем} < 50$	35
$33 \leq R_{сем} < 39$	27
$R_{сем} < 33$	0

8.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этап формирования компетенций

Экзамен не предусмотрен учебным планом

9. Методические рекомендации для студентов по изучению дисциплины

9.1 Использование материала учебно-методического комплекса дисциплины

На первом этапе необходимо ознакомиться с рабочей программой дисциплины, в которой рассмотрено содержание тем лекционного курса, взаимосвязь тем лекций с лабораторными занятиями, темы и виды самостоятельной работы. По каждому виду самостоятельной работы предусмотрены определённые формы отчетности.

8.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

Текущая аттестация студентов проводится преподавателями, ведущими лабораторные занятия по дисциплине, в следующих формах: отчет письменный, собеседование.

Допуск к лабораторным работам происходит при наличии у студентов печатного

варианта отчета. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя.

Максимальное количество баллов студент получает, если оформление отчета соответствует установленным требованиям, а отчет полностью раскрывает суть работы. Основанием для снижения оценки являются:

- частично не соответствует установленным требованиям;
- в отчете непольностью раскрывает суть работы.

Отчет может быть отправлен на доработку в следующих случаях:

- полностью не соответствует установленным требованиям;
- не раскрыта суть работы.

Критерии оценивания ответов на вопросы собеседования, отчёта письменного приведены в Фонде оценочных средств по дисциплине «Основы информационной безопасности».

9 Методические указания для обучающихся по освоению дисциплины

На первом этапе необходимо ознакомиться с рабочей программой дисциплины, в которой рассмотрено содержание тем дисциплины лекционного курса, взаимосвязь тем лекций с практическими занятиями, темы и виды самостоятельной работы. По каждому виду самостоятельной работы предусмотрены определённые формы отчетности.

Для успешного освоения дисциплины, необходимо выполнить следующие виды самостоятельной работы, используя рекомендуемые источники информации

№ п/п	Виды самостоятельной работы	1. Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая литература	Интернет-ресурсы
1.	изучение литературы по темам 1-9	1,2	1,2	1,2	1-4
2.	проработка лекционного материала	1,2	1,2	1,2	1-4
3.	подготовка к лабораторным занятиям	1,2	1,2	1,2	1-4

10. Учебно-методическое и информационное обеспечение дисциплины

10.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины.

10.1.1. Перечень основной литературы:

1. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 424 с.— Режим доступа: <http://www.iprbookshop.ru/52161>.— ЭБС «IPRbooks», по паролю

10.1.2. Перечень дополнительной литературы:

1. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: <http://www.iprbookshop.ru/43183>.— ЭБС «IPRbooks», по паролю

10.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине:

1. Методические указания по выполнению лабораторных работ по дисциплине

"Теоретические основы защиты информации".

2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине "Теоретические основы защиты информации".

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

1. Университетская библиотека online. <http://www.biblioclub.ru>.
2. ЭБС «IPRbooks». <http://www.iprbookshop.ru>.
3. Электронная библиотека СКФУ.. <http://catalog.ncstu.ru>.
4. Государственная публичная научно-техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

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

Информационные технологии:

- Персональные компьютеры, объединенные в локальную сеть и имеющие выход в Интернет;

Информационные справочные системы:

- www.consultant.ru
- www.garant.ru

Перечень программного обеспечения и информационно-справочных систем:

Стандартные приложения Windows

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

2. Лекционная аудитория, оснащенная мультимедийным проектором.
3. Компьютерная лаборатория, оснащенная персональными компьютерами Pentium в количестве 10 шт., объединенными в локальную сеть и имеющими выход в Интернет.
4. Системы для разработки программных приложений, оборудование: ПО ERwin Process Modeler r7.