

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение  
высшего образования**

**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»  
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске**

**УТВЕРЖДАЮ**

Зам. директора по учебной работе  
Институт сервиса, туризма и дизайна  
(филиал) СКФУ в г. Пятигорске

\_\_\_\_\_ М.В. Мартыненко  
"\_\_" \_\_\_\_\_ 20\_\_ г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Сети и системы радиосвязи и средства их информационной защиты**

Направление подготовки  
Направленность (профиль)

10.03.01 Информационная безопасность  
Комплексная защита объектов информатизации

Квалификация выпускника  
Форма обучения

Бакалавр  
Очная

Год начала обучения

2020 г.

Реализуется

в 6 семестре

**СОГЛАСОВАНО:**

Зав. выпускающей кафедрой систем управления и информационных технологий

\_\_\_\_\_ И.М Першин  
"\_\_" \_\_\_\_\_ 20\_\_ г.

**РАЗРАБОТАНО:**

Зав. кафедрой систем управления и информационных технологий

\_\_\_\_\_ И.М Першин  
"\_\_" \_\_\_\_\_ 20\_\_ г.

Рассмотрено УМК

Протокол №\_\_ от «\_\_» \_\_\_\_\_ 20\_\_ г.

"\_\_" \_\_\_\_\_ 20\_\_ г.

Председатель УМК института

\_\_\_\_\_ А.Б. Нарыжная

старший преподаватель кафедры систем управления и информационных технологий

\_\_\_\_\_ И.В. Калиберда

"\_\_" \_\_\_\_\_ 20\_\_ г.

Пятигорск, 2020

### **1. Цель и задачи освоения дисциплины**

Целью освоения дисциплины «Сети и системы радиосвязи и средства их информационной защиты» является формирование набора профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Задачи освоения дисциплины:

- сетях радиосвязи;
- системах радиосвязи;
- средствах информационной защиты систем радиосвязи.

### **2. Место дисциплины в структуре образовательной программы**

Дисциплина «Сети и системы радиосвязи и средства их информационной защиты» входит в вариативную часть блока Б1 ОП ВО подготовки бакалавра направления 10.03.01 Информационная безопасность и является дисциплиной по выбору. Ее освоение происходит в 6 семестре.

### **3. Связь с предшествующими дисциплинами**

Пререквизитами являются: «Сети и системы передачи информации»

### **4. Связь с последующими дисциплинами**

Кореквизитами являются: «Имитаторы сигналов радиотехнических средств»

### **5. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы**

#### **5.1 Наименование компетенций**

Код	Формулировка:
ОПК-1	способность использовать основы философских знаний для формирования мировоззренческой позиции
ОПК-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
ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты
ПК-7	способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПСК-1	способность формировать предложения по оптимизации комплекса технических средств, применяемых в процессе защищаемого объекта и его информационных составляющих, с целью совершенствования информационной безопасности объектов информатизации
ПСК-2	способность применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и ис-

	пользования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем
ПСК-5	способность разобрать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение

## 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
<p><b>Знать:</b> основы философских знаний для формирования мировоззренческой позиции</p> <p><b>Уметь:</b> использовать основы философских знаний для формирования мировоззренческой позиции</p> <p><b>Владеть:</b> способностью использовать основы философских знаний для формирования мировоззренческой позиции</p>	ОПК-1
<p><b>Знать:</b> 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><b>Уметь:</b> 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><b>Владеть:</b> способностью 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>	ОПК-5
<p><b>Знать:</b> программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p> <p><b>Уметь:</b> применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p> <p><b>Владеть:</b> способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p>	ПК-2
<p><b>Знать:</b> информационную безопасность объекта защиты</p> <p><b>Уметь:</b> администрировать подсистемы информационной безопасности объекта защиты</p> <p><b>Владеть:</b> способностью администрировать подсистемы информационной безопасности объекта защиты</p>	ПК-3
<p><b>Знать:</b> анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений</p> <p><b>Уметь:</b> проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений</p> <p><b>Владеть:</b> способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и</p>	ПК-7

участвовать в проведении технико-экономического обоснования соответствующих проектных решений	
<p><b>Знать:</b> оптимизацию комплекса технических средств, применяемых в процессе защищаемого объекта и его информационных составляющих, с целью совершенствования информационной безопасности объектов информатизации</p> <p><b>Уметь:</b> формировать предложения по оптимизации комплекса технических средств, применяемых в процессе защищаемого объекта и его информационных составляющих, с целью совершенствования информационной безопасности объектов информатизации</p> <p><b>Владеть:</b> способностью формировать предложения по оптимизации комплекса технических средств, применяемых в процессе защищаемого объекта и его информационных составляющих, с целью совершенствования информационной безопасности объектов информатизации</p>	ПСК-1
<p><b>Знать:</b> современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем</p> <p><b>Уметь:</b> применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем</p> <p><b>Владеть:</b> способностью применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем</p>	ПСК-2
<p><b>Знать:</b> комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение</p> <p><b>Уметь:</b> разобрать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение</p> <p><b>Владеть:</b> способностью разобрать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение</p>	ПСК-5

## 6. Объем учебной дисциплины/модуля

	Астр. часов	
Объем занятий: Итого	81 ч.	3 з.е.
В том числе аудиторных	48 ч.	
Из них:		
Лекций	12 ч.	
Лабораторных работ	24 ч.	
Практических занятий	12 ч.	
Самостоятельной работы	6 ч.	
Экзамен	6 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.	Тема 1. Общие принципы построения систем радиосвязи. Классификация. Диапазоны частот.	ОПК-1, ОПК-5, ПК-2, ПК-3, ПК-7, ПСК-1, ПСК-2, ПСК-5	1,5	1,5			3
2.	Тема 2. Наземные системы: Системы подвижной радиосвязи. Радиорелейные линии. Принципы построения.	ОПК-1, ОПК-5, ПК-2, ПК-3, ПК-7, ПСК-1, ПСК-2, ПСК-5	1,5	1,5	6		
3.	Тема 3. Соединительные ЦРРЛ для сетей подвижной радиосвязи.	ОПК-1, ОПК-5, ПК-2, ПК-3, ПК-7, ПСК-1, ПСК-2, ПСК-5	1,5	1,5			3
4.	Тема 4. Транкинговые сети, сети персонального радиовызова, беспроводные телефоны.	ОПК-1, ОПК-5, ПК-2, ПК-3, ПК-7, ПСК-1, ПСК-2, ПСК-5	1,5	1,5			
5.	Тема 5. Сети и системы радиодоступа.	ОПК-1, ОПК-5, ПК-2, ПК-3, ПК-7, ПСК-1, ПСК-2, ПСК-5	1,5	1,5			
6.	Тема 6. Спутниковые системы. Основные принципы построения. Роль спутниковых систем в сетях 3-го поколения.	ОПК-1, ОПК-5, ПК-2, ПК-3, ПК-7, ПСК-1, ПСК-2, ПСК-5	1,5	1,5	12		
7.	Тема 7. Полосы частот. Технологии.	ОПК-1, ОПК-5, ПК-2, ПК-	1,5	1,5			

		3, ПК-7, ПСК-1, ПСК-2, ПСК-5					
8.	Тема 8. Средства информационной защиты сетей и систем радиосвязи	ОПК-1, ОПК-5, ПК-2, ПК-3, ПК-7, ПСК-1, ПСК-2, ПСК-5	1,5	1,5	6		
	Итого		12	12	24		6

## 7.2 Наименование и содержание лекций

№ темы	Наименование тем дисциплины, их краткое содержание	Объем часов	Интерактивная форма проведения
1.	<p><b>Тема</b> Общие принципы построения систем радиосвязи. Классификация. Диапазоны частот.</p> <p><i>Содержание принципов построения систем радиосвязи. Классификация. Диапазоны частот. Регламент радиосвязи РФ. Стандарты аналоговых и цифровых систем радиосвязи.</i></p>	1,5	
2.	<p><b>Тема</b> Наземные системы: Системы подвижной радиосвязи. Радиорелейные линии. Принципы построения.</p> <p><i>Системы цифровой радиорелейной связи. Автоматизация проектирования цифровых радиорелейных линий.</i></p>	1,5	
3.	<p><b>Тема</b> Соединительные ЦРРЛ для сетей подвижной радиосвязи.</p> <p><i>Передача информации в цифровой форме по телефонным или телевизионным стволам аналоговых РРЛ одновременно с аналоговым телевизионным или многоканальным телефонным сообщением. Организация передачи только цифрового потока в стволе аналоговой РРЛ. Организация цифровых радиорелейных систем, по которым передается только цифровая информация; по таким системам могут передаваться цифровые потоки от ЦСП любой ступени иерархии; в этом случае используются различные способы модуляции: амплитудная, частотная, фазовая (в том числе многопозиционная).</i></p>	1,5	
4.	<p><b>Тема</b> Транкинговые сети, сети персонального радиовызова, беспроводные телефоны.</p> <p><i>Транкинговые системы радиосвязи. Стандарты аналоговой и цифровой транкинговой радиосвязи. Системы сотовой связи стандарта GSM. Системы по-</i></p>	1,5	

	<i>движной связи в стандартах IS-95 (CDMA) и DECT. Стандарты кодирования в пейджинговой связи.</i>		
5.	<b>Тема</b> Сети и системы радиодоступа.  <i>Физический и канальный уровни модели открытых информационных систем. Теоретические сведения о процессах функционирования систем радиодоступа, в частности, основные модели распространения радиоволн для разных классов систем, виды используемых сигналов, способы разделения каналов и т.д. Тенденции развития оборудования систем радиодоступа.</i>	1,5	
6.	<b>Тема</b> Спутниковые системы. Основные принципы построения. Роль спутниковых систем в сетях 3-го поколения.  <i>Современные спутниковые системы связи. Спутниковые системы персональной радиосвязи.</i>	1,5	
7.	<b>Тема</b> Полосы частот. Технологии.  <i>Методы и технические средства радиоразведки. Методы обнаружения сигналов. Методы ускоренного поиска частоты излучения и задержки импульсных потоков.</i>	1,5	
8.	<b>Тема</b> Средства информационной защиты сетей и систем радиосвязи  <i>Стандарты кодирования информации в пейджинговых сетях, перспективные спутниковые системы связи, включая спутниковые системы персональной радиосвязи, стандарты беспроводных локальных сетей IEEE 802.11, персональные сети радиодоступа стандартов IEEE 802.15, стандарты городских сетей широкополосного радиодоступа IEEE 802.16 (WiMAX), а также средства информационной защиты сетей и систем радиосвязи, предусмотренные соответствующими стандартами.</i>	1,5	
	<b>Итого</b>	<b>12</b>	

### 7.3 Наименование лабораторных работ

<b>№ Темы</b>	<b>Наименование тем дисциплины, их краткое содержание</b>	<b>Объем часов</b>	<b>Интерактивная форма проведения</b>
2	Лабораторная работа № 1. Создание системы «Стрелц-интеграл» на базе контроллера "РРОП-И" в ПО "WirelEx".  <i>изучение технологии конфигурирования интегриро-</i>	3	

	<i>ванной системы «Стрелец», уровни доступа для системы охранно-пожарной сигнализации.</i>		
2	Лабораторная работа № 2. Конфигурирование системы пожарной сигнализации в ПО "WireEx".  <i>научиться настраивать параметры и тактику работы интегрированной системы «Стрелец» для системы пожарной сигнализации и системы оповещения людей о пожаре.</i>	3	
6	Лабораторная работа № 3. Конфигурирование системы охранной сигнализации в ПО "WireEx".  <i>научиться настраивать параметры и тактику работы интегрированной системы «Стрелец» для системы охранной сигнализации.</i>	3	
6	Лабораторная работа № 4. Конфигурирование системы контроля и управления доступом в ПО "WireEx".  <i>научиться настраивать уровни доступа интегрированной системы «Стрелец» для системы охранно-пожарной сигнализации.</i>	3	Работа на тренажере
6	Лабораторная работа № 5. Конфигурирование топологии проводных устройств системы в ПО "Стрелец-Мастер".  <i>научиться конфигурировать топологию проводных устройств системы в ПО "Стрелец-Мастер"</i>	3	Работа на тренажере
6	Лабораторная работа № 6. Конфигурирование топологии системы охраны в ПО "Стрелец-Мастер".  <i>научиться конфигурировать топологию системы охраны в ПО "Стрелец-Мастер"</i>	3	Работа на тренажере
8	Лабораторная работа № 7. Конфигурирование топологии системы контроля и управления доступом в ПО "Стрелец-Мастер".  <i>научиться конфигурировать топологию системы контроля и управления доступом в ПО "Стрелец-Мастер".</i>	3	Работа на тренажере
8	Лабораторная работа № 8. Программирование индикации состояния разделов, групп разделов в ПО "Стрелец-Мастер".  <i>научиться программировать индикацию состояния разделов, групп разделов в ПО "Стрелец-Мастер"</i>	3	
	<b>Итого</b>	<b>24</b>	<b>12</b>



#### 7.4 Наименование практических занятий

№ Темы	Наименование работы	Объем часов	Форма проведения
1	Тема 1. 1. Содержание функции администрирования. 2. Содержание процедур администрирования. 3. Содержание службы администрирования.	1,5	
2	Тема 2. 1. Категории администраторов. 2. Инфраструктура ИТ. 3. Централизованная модель администрирования.	1,5	
3	Тема 3. 1. Распределенная (децентрализованная) модель администрирования. 2. Смешанная модель администрирования. 3. Планирование инсталляционных работ.	1,5	
4	Тема 4. 1. Выбор аппаратно-программных средств. 2. Инсталляция информационной системы (на примере FreeBSD); 3. Настройка информационной системы.	1,5	
5	Тема 5. 1. Методы выявления неполадок в работе информационной системы. 2. Оперативное управление и устранение неполадок в системе. 3. Средства администрирования ОС (FreeBSD).	1,5	
6	Тема 6. 1. Средства администрирования баз данных. 2. Средства администрирования ЛВС. 3. Средства администрирования глобальных информационных систем.	1,5	
7	Тема 7. 1. Сетевое администрирование. Установка, настройка и сопровождение DHCP сервера. 2. Службы каталогов. Установка, настройка и сопровождение Active Directory. 3. Удаленный доступ. Установка, настройка и управление службами удаленного доступа..	1,5	
8	Тема 8. 1. Многопользовательская вычислительная среда. Службы терминалов. Установка, настройка и управление службами терминалов. 2. Администрирование пользователей. Политики безопасности, их реализация в операционных системах. 3. Сетевое администрирование. Установка, настройка и сопровождение служб совместного доступа в Интернет.	1,5	

	<b>Итого</b>	<b>12</b>	
--	--------------	-----------	--

## 7.5 Технологическая карта самостоятельной работы обучающегося

### Технологическая карта

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
ОПК-1, ОПК-5, ПК-2, ПК-3, ПК-7, ПСК-1, ПСК-2, ПСК-5	Изучение литературы по темам 1-8	Конспект	■ беседа	68,58	7,62	76,2
ОПК-1, ОПК-5, ПК-2, ПК-3, ПК-7, ПСК-1, ПСК-2, ПСК-5	проработка лекционного материала	Конспект	■ беседа	1,08	0,12	1,2
ОПК-1, ОПК-5, ПК-2, ПК-3, ПК-7, ПСК-1, ПСК-2, ПСК-5	подготовка к лабораторным и практическим работам	Отчет	■ отчет письменный	3,24	0,36	3,6
Итого				72,9	8,1	81

## 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

Код оцениваемой компетенции	Этап формирования компетенции (№ темы)	Средства и технологии оценки	Тип контроля (текущий/промежуточный)	Вид контроля (текущий/промежуточный)	Наименование оценочного средства
ОПК-1, ОПК-5, ПК-2, ПК-3, ПК-7, ПСК-1, ПСК-2, ПСК-5	2,6,8	отчёт письменный	текущий	письменный	Темы индивидуальных заданий для лабораторных занятий
ОПК-1, ОПК-5, ПК-2, ПК-3, ПК-7, ПСК-1, ПСК-2, ПСК-5	1-8	Собеседование	текущий	письменный	Темы рефератов
ОПК-1, ОПК-5, ПК-2, ПК-3, ПК-7, ПСК-1, ПСК-2, ПСК-5	1-8	конспект	текущий	устный	Вопросы для собеседования

		Собеседование	промежуточный	устный	Вопросы к экзамену
					Вопросы для проверки уровня знаний
					Вопросы (задания) для проверки умений и навыков

## 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
(для каждой компетенции)	ОПК-1				
Базовый	<b>Знать:</b> основы философских знаний для формирования мировоззренческой позиции	Не знает: основы философских знаний для формирования мировоззренческой позиции	Недостаточно хорошо знает основы философских знаний для формирования мировоззренческой позиции	Знает основы философских знаний для формирования мировоззренческой позиции	
	<b>Уметь:</b> использовать основы философских знаний для формирования мировоззренческой позиции	Отсутствие умения использовать основы философских знаний для формирования мировоззренческой позиции	Частично умеет использовать основы философских знаний для формирования мировоззренческой позиции	Умеет использовать основы философских знаний для формирования мировоззренческой позиции	
	<b>Владеть</b> способностью использовать основы философских знаний для формирования мировоззренческой позиции	Не владеет способностью использовать основы философских знаний для формирования мировоззренческой позиции	Недостаточно хорошо владеет способностью использовать основы философских знаний для формирования мировоззренческой позиции	Владеет навыками способностью использовать основы философских знаний для формирования мировоззренческой позиции.	
	ОПК-5				
	<b>Знать:</b> социальную значимость своей будущей профессии, обладать	Отсутствуют знания социальной значимости своей будущей профессии,	Частичные знания социальной значимости своей будущей профессии,	Имеются знания социальной значимости своей будущей профессии, обладать высокой моти-	



	тельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	нальной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	
<b>ПК-2</b>					
	<b>Знать:</b> программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Отсутствуют знания программных средств системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Частичные знания программных средств системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Имеются знания программных средств системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
	<b>Уметь:</b> применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Отсутствие умения применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Частично умеет применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Умеет применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
	<b>Владеть:</b> способностью применять про-	Не владеет способностью применять программные	Частично владеет способностью применять про-	Владеет способностью применять программные средства	

	граммные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	граммные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
	<b>ПК-3</b>				
	<b>Знать:</b> информационную безопасность объекта защиты	Отсутствуют знания информационной безопасности объекта защиты	Частичные знания информационной безопасности объекта защиты	Имеются знания информационной безопасности объекта защиты	
	<b>Уметь:</b> администрировать подсистемы информационной безопасности объекта защиты	Отсутствие умения администрировать подсистемы информационной безопасности объекта защиты	Частично умеет администрировать подсистемы информационной безопасности объекта защиты	Умеет администрировать подсистемы информационной безопасности объекта защиты	
	<b>Владеть:</b> способностью администрировать подсистемы информационной безопасности объекта защиты	Не владеет способностью администрировать подсистемы информационной безопасности объекта защиты	Частично владеет способностью администрировать подсистемы информационной безопасности объекта защиты	Владеет способностью администрировать подсистемы информационной безопасности объекта защиты	
	<b>ПК-7</b>				
	<b>Знать:</b> анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования со-	Отсутствуют знания анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-	Частичные знания анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-	Имеются знания анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования со-	

	ответствующих проектных решений	экономического обоснования соответствующих проектных решений	экономического обоснования соответствующих проектных решений	проектных решений	
	<b>Уметь:</b> проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Отсутствие умения проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Частично умеет проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Умеет проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	
	<b>Владеть:</b> способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Не владеет способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Частично владеет способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Владеет способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	
<b>ПСК-1</b>					
	<b>Знать:</b>	Отсутствуют знания опти-	Частичные знания опти-	Имеются знания оптимизации	





	онных составляющих, с целью совершенствования информационной безопасности объектов информатизации	онных составляющих, с целью совершенствования информационной безопасности объектов информатизации	информационных составляющих, с целью совершенствования информационной безопасности объектов информатизации	совершенствования информационной безопасности объектов информатизации	
<b>ПСК-2</b>					
	<b>Знать:</b> современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	Отсутствуют знания современных информационных технологий и методов цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	Частичные знания современных информационных технологий и методов цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	Имеются знания современных информационных технологий и методов цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	
	<b>Уметь:</b> применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	Отсутствие умения применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	Частично умеет применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	Умеет применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	
	<b>Владеть:</b> способностью применять современные информационные техноло-	Не владеет способностью применять современные информационные технологии и	Частично владеет способностью применять современные информационные техно-	Владеет способностью применять современные информационные технологии и методы цифровой	

	гии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	нологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем	
<b>ПСК-5</b>					
	<b>Знать:</b> комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	Отсутствуют знания комплекса организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	Частичные знания комплекса организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	Имеются знания комплекса организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	
	<b>Уметь:</b> разобрать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	Отсутствие умения разобрать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	Частично умеет разобрать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	Умеет разобрать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	
	<b>Владеть:</b> способностью	Не владеет способностью разобрать ком-	Частично владеет способностью разобрать	Владеет способностью разобрать комплекс органи-	

	разобрать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	закономерностей и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение	
Повышенный	<b>ОПК-1</b>				
	<b>Знать:</b> основы философских знаний для формирования мировоззренческой позиции				Знает основы философских знаний для формирования мировоззренческой позиции
	<b>Уметь:</b> использовать основы философских знаний для формирования мировоззренческой позиции				Показывает умение использовать основы философских знаний для формирования мировоззренческой позиции
	<b>Владеть:</b> способностью использовать основы философских знаний для формирования мировоззренческой позиции				Владеет способностью использовать основы философских знаний для формирования мировоззренческой позиции
	<b>ОПК-5</b>				
<b>Знать:</b> социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспече-				Знает социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в	

	<p>ния информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики</p>				<p>области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики</p>
	<p><b>Уметь:</b></p> <p>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><b>Владеть:</b></p> <p>способностью 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>Владеет способностью 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>

ПК-2					
	<p><b>Знать:</b></p> <p>программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p>				<p>Знает программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p>
	<p><b>Уметь:</b></p> <p>применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p>				<p>Умеет применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p>
	<p><b>Владеть:</b></p> <p>способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p>				<p>Владеет способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач</p>
ПК-3					
	<p><b>Знать:</b></p> <p>информационную безопасность объекта защиты</p>				<p>Знает информационную безопасность объекта защиты</p>
	<p><b>Уметь:</b></p>				<p>Умеет администрировать</p>

	администрировать подсистемы информационной безопасности объекта защиты				подсистемы информационной безопасности объекта защиты
	<b>Владеть:</b> способностью администрировать подсистемы информационной безопасности объекта защиты				Владеет способностью администрировать подсистемы информационной безопасности объекта защиты
	ПК-7				
	<b>Знать:</b> анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений				Знает анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
	<b>Уметь:</b> проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений				Умеет проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
	<b>Владеть:</b> способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информаци-				Владеет способностью проводить анализ исходных данных для проектирования подсистем и средств

	онной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений				обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
	ПСК-1				
	<p><b>Знать:</b></p> <p>оптимизацию комплекса технических средств, применяемых в процессе защищаемого объекта и его информационных составляющих, с целью совершенствования информационной безопасности объектов информатизации</p>				Знает оптимизацию комплекса технических средств, применяемых в процессе защищаемого объекта и его информационных составляющих, с целью совершенствования информационной безопасности объектов информатизации
	<p><b>Уметь:</b></p> <p>формировать предложения по оптимизации комплекса технических средств, применяемых в процессе защищаемого объекта и его информационных составляющих, с целью совершенствования информационной безопасности объектов информатизации</p>				Умеет формировать предложения по оптимизации комплекса технических средств, применяемых в процессе защищаемого объекта и его информационных составляющих, с целью совершенствования информационной безопасности объектов информатизации
	<p><b>Владеть:</b></p> <p>способностью формировать предложения по оптимизации комплекса технических средств, применяемых в процессе защища-</p>				Владеет способностью формировать предложения по оптимизации комплекса технических средств, применяемых в процессе за-

	<p>емого объекта и его информационных составляющих, с целью совершенствования информационной безопасности объектов информатизации</p>				<p>щищаемого объекта и его информационных составляющих, с целью совершенствования информационной безопасности объектов информатизации</p>
ПСК-2					
	<p><b>Знать:</b></p> <p>современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем</p>				<p>Знает современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем</p>
	<p><b>Уметь:</b></p> <p>применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем</p>				<p>Умеет применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизи-</p>



					рованных систем
	<p><b>Владеть:</b></p> <p>способностью применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем</p>				Владеет способностью применять современные информационные технологии и методы цифровой обработки сигналов для эффективного анализа и использования массивов информации при решении задач обеспечения информационной безопасности автоматизированных систем
	ПСК-5				
	<p><b>Знать:</b></p> <p>комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение</p>				Знает комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение
	<p><b>Уметь:</b></p> <p>разобрать комплекс организационных и технических мер по обеспечению инфор-</p>				Умеет разобрать комплекс организационных и технических мер по обеспечению инфор-

	мационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение				ной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение
	<b>Владеть:</b> способностью разобрать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение				Владеет способностью разобрать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации, провести выбор необходимых технологий и технических средств, организовать его внедрение и последующее сопровождение

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 1-3	6 неделя	25
2.	Выполнение лабораторных работ 4-8	12 неделя	30
<b>Итого за семестр</b>			<b>55</b>

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	<b>100</b>
Хороший	<b>80</b>
Удовлетворительный	<b>60</b>
Неудовлетворительный	<b>0</b>

Промежуточная аттестация в форме экзамена предусматривает проведение обязательной экзаменационной процедуры и оценивается 40 баллами из 100. В случае если рейтинговый балл студента по дисциплине по итогам семестра равен 60, то программой автоматически добавляется 32 премиальных балла и выставляется оценка «отлично». Положительный ответ студента на экзамене оценивается рейтинговыми баллами в диапазоне от 20 до 40 ( $20 \leq S_{\text{ЭКЗ}} \leq 40$ ), оценка меньше 20 баллов считается неудовлетворительной.

*Шкала соответствия рейтингового балла экзамена 5-балльной системе*

Рейтинговый балл по дисциплине	Оценка по 5-балльной системе
35 – 40	Отлично
28 – 34	Хорошо
20 – 27	Удовлетворительно

Итоговая оценка по дисциплине, изучаемой в семестре, определяется по сумме баллов, набранных за работу в течение семестра, и баллов, полученных при сдаче экзамена:

*Шкала пересчета рейтингового балла по дисциплине в оценку по 5-балльной системе*

Рейтинговый балл по дисциплине	Оценка по 5-балльной системе
88 – 100	Отлично
72 – 87	Хорошо
53 – 71	Удовлетворительно
<53	Неудовлетворительно

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

Результатом итоговой проверки знаний студентов по дисциплине учебным планом предусмотрен экзамен.

**Вопросы к экзамену**

Вопросы для проверки уровня обученности:

**Знать:**

1. Системы цифровой радиорелейной связи
2. Транкинговые системы радиосвязи
3. Системы сотовой связи стандарта GSM
4. Системы подвижной связи в стандартах IS-95 (CDMA) и DECT
5. Стандарты кодирования в пейджинговой связи
6. Перспективные спутниковые системы связи
7. Беспроводные локальные сети на основе стандартов IEEE 802.11
8. Персональные сети радиодоступа. Стандарты IEEE 802.15, Bluetooth
9. Стандарты городских сетей широкополосного радиодоступа IEEE 802.16 (WiMAX)
10. Виды радиосвязи.
11. Структура сетей WiMAX.
12. Стандарт IEEE 802.16. Физический уровень безопасности.
13. Стандарт IEEE 802.16. Сообщения управления ключами конфиденциальности.
14. Стандарт IEEE 802.16. Сообщение отклика регистрации.
15. Применение оборудования для стандарта IEEE 802.16

**Уметь, владеть:**

1. Процесс эксплуатации радиоканальных информационных систем.
2. Сопровождение радиоканальных информационных систем.
3. Жизненный цикл создания и использования ИС.

4. Модели жизненного цикла информационных технологий.
5. Стандарты по сопровождению ИС.
6. Управление и обслуживание технических средств.
7. Особенности работы в многопользовательских средах: открытые системы; архитектура «клиент-сервер» и «клиент-серверные» технологии.
8. Построение многопользовательских информационных систем и управление ими.
9. Состав и структура информационной сетевой среды.
10. Сетевые информационные службы.
11. Службы безопасности.
12. Аппаратно-программные платформы администрирования операционных систем.
13. Аппаратно-программные платформы администрирования службы каталога.
14. Аппаратно-программные платформы администрирования служб радиоканальных информационных систем в глобальных сетях.
15. Управление доступом в Internet.

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

Процедура проведения экзамена осуществляется в соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования в СКФУ. В экзаменационный билет включаются 2 теоретических вопроса. Для подготовки по билету отводится 30 минут.

При подготовке к ответу студенту предоставляется право пользования справочными материалами.

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

Допуск к защите отчетов по 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 раскрывается суть работы.

Отчет может быть отправлен на доработку в следующих случаях:

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

Процедура проведения собеседования проводится в следующей форме: студенту выдается вопрос для собеседования, он готовит ответ (в письменной или устной форме) и отчитывается преподавателю по заданному вопросу. При подготовке к ответу студенту предоставляется право пользования справочными материалами. При проверке задания, оцениваются:

- последовательность и рациональность выполнения;
- точность вычислений;
- знание технологий, использованных при выполнении задания.

Критерии оценивания ответов на вопросы собеседования, отчёта приведены в Фонде оценочных средств по дисциплине «Сети и системы радиосвязи и средства их информационной защиты».

## 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 лабораторными 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	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая литература	Интернет-ресурсы
1.	изучение литературы по темам 1-8	1,2	1,2	1-2	1-2
2.	проработка лекционного материала	1,2	1,2	1-2	1-2
3.	подготовка к лабораторным и практическим работам	1,2	1,2	1-2	1-2

## 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. Гафнер В. В. Информационная безопасность : учеб.пособие /В.В. Гафнер. — Ростов н/Д : Феникс, 2010. — 324 с.
2. Программно-аппаратная защита информации: учеб.пособие/ П. Б. Хорев.- М.: Форум, 2012.- 352 с.

#### 10.1.2. Перечень дополнительной литературы:

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; Технические средства и методы защиты информации: Учебник для вузов / под ред. А.П. Зайцева и А.А. Шелупанова. - М.: ООО "Издательство Машиностроение", 2009. - 508 с.
2. Защита информации в операционных системах: учеб.пособие.- Ставрополь: Изд-во СГУ, 2008.- 318 с

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

1. Методические указания по организации и проведению самостоятельной работы по дисциплине Сети и системы радиосвязи и средства их информационной защиты.
2. Методические указания по выполнению лабораторных работ по дисциплине Сети и системы радиосвязи и средства их информационной защиты.
3. Методические указания по выполнению практических работ по дисциплине Сети и системы радиосвязи и средства их информационной защиты.

### 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](http://www.gpntb.ru).

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

Базовый пакет программ Microsoft Office Standard 2013. Бессрочная лицензия. Дата окончания срока поддержки (обновления) 11.04.2023г., Microsoft Windows Профессиональная. Бессрочная лицензия.

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

1. Учебная аудитория для групповых и индивидуальных консультаций: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: переносной ноутбук, проектор, доска магнитно-маркерная

2. Учебная аудитория для текущего контроля и промежуточной аттестации: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: переносной ноутбук, проектор, доска магнитно-маркерная

3. Учебная аудитория для проведения занятий семинарского типа (лабораторных работ): Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, переносной ноутбук, доска.

4. Учебная аудитория для проведения занятий семинарского типа (практических работ): Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, переносной ноутбук, проектор, доска магнитно-маркерная

5. Учебная аудитория для проведения занятий лекционного типа: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: переносной ноутбук, переносной проектор, доска. Учебно-наглядные пособия в виде тематических презентаций, соответствующих рабочим программам дисциплин