

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

УТВЕРЖДАЮ
Зам. директора по УВР
Н.А. Андреева
«22» / 04 2024 г.

**Защита информации в беспроводных высокоскоростных
системах передачи данных
Б1.В.ДВ.04.02
рабочая программа дисциплины**

Кафедра: Инфокоммуникационные технологии и системы связи

Направление подготовки:

11.03.02 Инфокоммуникационные технологии и системы связи

Профиль: Защищенные инфокоммуникационные системы

Формы обучения: очная, заочная

**Распределение часов дисциплины по семестрам (для очной формы
обучения (ОФО), курсам (для заочной формы обучения (ЗФО))**

Вид учебной работы	ОФО		ЗФО	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	4	144/7	4	36/4 108/5
Контактная работа, в том числе (по семестрам, курсам):		72/7		2/4 8/5
Лекции		36/7		2/4 2/5
Практических занятий		36/7		6/5
Семинаров				
Самостоятельная работа		72/7		34/4 100/5
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с оценкой с разбивкой по семестрам (курсам)		1/7		1/5
Число экзаменов с разбивкой по семестрам (курсам)				

Программу составил:

Доцент кафедры ИТСС к.т.н., доцент Руденко Н.В.

Рабочая программа дисциплины **«Защита информации в беспроводных высокоскоростных системах передачи данных»**

Разработана в соответствии с ФГОС ВО:

направления подготовки

11.03.02 ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ,
утвержденным приказом Министерства образования и науки Российской Федерации
от 19 сентября 2017 г. № 930.

Составлена на основании учебных планов

направления 11.03.02 Инфокоммуникационные технологии и системы связи

профиля «Защищенные инфокоммуникационные системы», одобренных Учёным советом СКФ МТУСИ, протокол № 9 от 22.04.2024 г., и утвержденного директором СКФ МТУСИ 22.04.2024 г.

Одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от 22.04 2024 г. № 9

Зав. кафедрой  В.И. Юхнов

1. Цели изучения дисциплины

Целью освоения дисциплины «Защита информации в беспроводных высокоскоростных системах передачи данных» для студентов является приобретение знаний и умений использовать принципы в современных системах и сетях радиосвязи, их назначении, принципах построения и функционирования, а также об основных стандартах криптографической защиты, методах организации защищенной связи и протоколах обмена защищенной информацией.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у обучающегося способности решать профессиональные задачи в соответствии с *технологическим видом деятельности*.

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

Компетенции обучающегося, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)	
ПК-1: Способен обеспечить защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи	
Знать	
Основные математические методы и алгоритмы шифрования, расшифрования и дешифрования сообщений. Электронной (цифровой) подписи в телекоммуникационных системах. Принципы работы, структурные схемы, протоколы и способы программирования криптосистем и систем электронной подписи. Основные аспекты информационной безопасности; опасности и угрозы, возникающие в развитии современного информационного общества; требования информационной безопасности Методы защиты объектов от несанкционированного доступа физических лиц и основные направления противодействия техническим средствам разведки.	
Уметь:	
Определять опасности и угрозы, возникающие в развитии современного информационного общества. Реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации. Применять на практике технические методы защиты информации, пользоваться стандартной терминологией и определениями. Составлять протоколы шифрования и расшифрования сообщений.	
Владеть :	
Языком предметной области: основными терминами, понятиями, определениями в области информационной безопасности Способностью сознать опасности и угрозы, возникающие в развитии современного информационного общества Способностью сознать опасности и угрозы, возникающие в развитии современного информационного общества, соблюдать основные требования информационной безопасности Способностью применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств электросвязи и информатики; организовывать и проводить их испытания с целью оценки соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов Методы и средства инженерной защиты и технической охраны объектов Навыками о типовых разработанных средствах защиты информации и возможностями их использования в реальных задачах создания и внедрения инфокоммуникационных систем	

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.23 «Схемотехника»
2	Б1.В.08 «Сети электросвязи и методы их защиты»
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б2.О.03(Пд) «Производственная практика (преддипломная)»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часа, 72 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
1	2	3	4	5	6
Курс 4, Семестр 7					
Модуль 1 Основные сведения о беспроводных системах – 36 (18 Лек+18 ПЗ) часов контактной работы, 36 часов СР					
1.1	Лекция 1. Основные определения и понятия. Принципы построения систем и сетей радиосвязи	Лек.	2	ПК-1	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. Общие свойства радиоволн. Особенности распространения в атмосфере радиоволн различных диапазонов	Лек.	4	ПК-1	Л1.1 Л1.2 Л1.3
1.3	Практическое занятие 1 Расчет рабочих частот для радиосвязи в диапазоне коротких волн	ПЗ	4	ПК-1	Л3.1 Л3.2
1.4	Лекция 3. Структура передающих и приемных устройств. Модель цифровой системы связи.	Лек.	4	ПК-1	Л1.1
1.5	Практическое занятие 2 Расчет зоны уверенного приёма	ПЗ	4	ПК-1	Л3.1 Л3.2
1.6	Распространение сигнала в свободном пространстве.	СР	4	ПК-1	Л1.1
1.7	Понятие радиопомех	СР	4	ПК-1	Л1.1
1.8	Принципы построения и перспективы развития сети электросвязи.	СР	4	ПК-1	Л1.1
1.9	Лекция 4. Стандарты мобильной связи. История, развитие, перспективы	Лек	4	ПК-1	Л1.1
1.10	Практическое занятие 3 Изучение работы сетей связи с использованием программного продукта CiscoPacketTracer.	ПЗ	4	ПК-1	Л3.1 Л3.2
1.11	Практическое занятие 4 Исследование формирования сигнала в стандарте GSM	ПЗ	6	ПК-1	Л3.1 Л3.2
1.12	Лекция 5. Стандарты широкополосных сетей. Стандарт Wi-Fi и Wi-MAX. Особенности стандарта	Лек.	4	ПК-1	Л1.1

	LTE				
1.13	Персональные беспроводные сети.	СР	4	ПК-1	Л1.1 Л1.3 Л2.1
1.14	Беспроводные сенсорные сети.	СР	4	ПК-1	Л1.1 Л1.3 Л2.1
1.15	Малые локальные беспроводные сети.	СР	4	ПК-1	Л1.1 Л1.3 Л2.1
1.16	Большие локальные беспроводные сети.	СР	6	ПК-1	Л1.1 Л1.3 Л2.1
1.17	Глобальные беспроводные сети.	СР	6	ПК-1	Л1.1 Л1.3 Л2.1
Модуль 2 – Защита информации в беспроводных высокоскоростных системах - 36 (18 Лек+18 ПЗ) часов контактной работы, 36 часов СР					
2.1	Лекция 6. Транкинговая связь: стандарт TETRA.	Лек.	4	ПК-1	Л1.1
2.2	Практическое занятие 5. Принципы построения и типы транкинговых систем	ПЗ	4	ПК-1	Л3.1 Л3.2
2.2	Лекция 7. Цели и задачи мер защиты информации в беспроводных высокоскоростных системах	Лек.	4	ПК-1	Л1.2 Л1.3
2.3	Практическое занятие 6. Изучение работы маршрутизатора с использованием CiscoPacketTracer	ПЗ	4	ПК-1	Л2.1 Л3.1 Л3.2
2.4	Практическое занятие 7. Изучение возможностей работы протокола NAT.	ПЗ	4	ПК-1	Л2.1 Л3.1
2.5	Лекция 8. Защита информации в беспроводных высокоскоростных системах. Программные средства	Лек.	4	ПК-1	Л1.2 Л1.3 Л2.1
2.6	Лекция 9. Защита информации в беспроводных высокоскоростных системах. Технические средства	Лек.	4	ПК-1	Л1.2 Л1.3 Л2.1
2.6	Практическое занятие 8. Конфигурирование списков управления доступом ACL.	ПЗ	4	ПК-1	Л2.1 Л3.1 Л3.2
2.7	Лекция 10. Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок	Лек.	2	ПК-1	Л1.2 Л1.3 Л2.1
2.8	Практическое занятие 9. Конфигурирование виртуальной локальной сети VLAN	ПЗ	2	ПК-1	Л1.4 Л3.1 Л3.2
2.9	Способы предотвращения утечки информации через ПЭМИН	СР	4	ПК-1	Л1.2 Л1.3 Л2.1
2.10	Методы средства ограничения доступа к компонентам ЭВМ	СР	4	ПК-1	Л1.2 Л1.3 Л2.1

2.11	Надёжность средств защиты компонент в беспроводных высокоскоростных системах	СР	4	ПК-1	Л1.2 Л1.3 Л2.1
2.12	Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям	СР	6	ПК-1	Л1.2 Л1.3 Л2.1
2.14	Безопасность оптоволоконных кабельных систем.	СР	6	ПК-1	Л1.2 Л1.3 Л2.1
2.16	Расчёт характеристик локальной вычислительной сети Ethernet	СР	6	ПК-1	Л2.1 Л3.1
2.17	Подавление информационных сигналов в цепях заземления	СР	6	ПК-1	Л2.1 Л3.1
Зачет					
Итого – 144 часа					

4.2 Заочная форма обучения, 5 лет (всего 144 часа, аудиторных 10 часов)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, сессия 2					
Модуль 1 Основные сведения о беспроводных системах – - 36 (2 Лек) часов контактной работы, 34 часов СР					
1.1	Лекция 1. Основные определения и понятия. Принципы построения систем и сетей радиосвязи	Лек.	2	ПК-1	Л1.1 Л1.2 Л1.3
1.2	Общие свойства радиоволн. Особенности распространения в атмосфере радиоволн различных диапазонов	СР	2	ПК-1	Л1.1 Л1.2 Л1.3
1.3	Расчет рабочих частот для радиосвязи в диапазоне коротких волн	СР	2	ПК-1	Л3.1
1.4	Структура передающих и приемных устройств. Модель цифровой системы связи.	СР	2	ПК-1	Л1.1 Л1.2 Л1.3
1.5	Расчет зоны уверенного приёма	СР	2	ПК-1	Л3.1
1.6	Распространение сигнала в свободном пространстве.	СР	2	ПК-1	Л1.1 Л1.2 Л1.3
1.7	Понятие радиопомех	СР	2	ПК-1	Л1.1 Л1.2 Л1.3
1.8	Принципы построения и перспективы развития сети электросвязи.	СР	2	ПК-1	Л1.1 Л1.2 Л1.3
1.9	Стандарты мобильной связи. История, развитие, перспективы	СР	2	ПК-1	Л1.1 Л1.2 Л1.3
1.10	Изучение работы сетей связи с использованием программного продукта CiscoPacketTracer.	СР	2	ПК-1	Л3.1

1.11	Исследование формирования сигнала в стандарте GSM	СР	2	ПК-1	ЛЗ.1
1.12	Стандарты широкополосных сетей. Стандарт Wi-Fi и Wi-MAX. Особенности стандарта LTE	СР	4	ПК-1	Л1.1 Л1.2 Л1.3
1.13	Персональные беспроводные сети.	СР	2	ПК-1	Л1.1 Л1.2 Л2.1
1.14	Беспроводные сенсорные сети.	СР	2	ПК-1	Л1.1 Л1.2 Л2.1
1.15	Малые локальные беспроводные сети.	СР	2	ПК-1	Л1.1 Л1.2 Л2.1
1.16	Большие локальные беспроводные сети.	СР	2	ПК-1	Л1.1 Л1.2 Л2.1
1.17	Глобальные беспроводные сети.	СР	2	ПК-1	Л1.1 Л1.2 Л2.1
Курс 5, сессия 2					
Модуль 2 – Защита информации в беспроводных высокоскоростных системах –8 (2 Лек+6 ПЗ) часов контактной работы, 100 часов СР					
2.1	Транкинговая связь: стандарт TETRA.	СР	6	ПК-1	Л1.1 Л1.2 Л1.3
2.2	Принципы построения и типы транкинговых систем	СР	6	ПК-1	ЛЗ.1
2.3	Лекция №2. Цели и задачи мер защиты информации в беспроводных высокоскоростных системах	Лек.	2	ПК-1	Л1.2 Л1.3
2.4	Практическое занятие 1. Изучение работы маршрутизатора с использованием CiscoPacketTracer	ПЗ	2	ПК-1	Л2.1 ЛЗ.1 ЛЗ.2
2.5	Изучение возможностей работы протокола NAT	СР	8	ПК-1	Л2.1 ЛЗ.1
2.6	Защита информации в беспроводных высокоскоростных системах. Программные средства	СР	8	ПК-1	Л1.2 Л1.3
2.7	Защита информации в беспроводных высокоскоростных системах. Технические средства	СР	8	ПК-1	Л1.2 Л1.3
2.8	Практическое занятие 2. Конфигурирование списков управления доступом ACL.	ПЗ	2	ПК-1	Л2.1 ЛЗ.1 ЛЗ.2
2.9	Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок	СР	8	ПК-1	Л1.2 Л1.3 Л2.1
2.10	Практическое занятие 3. Конфигурирование виртуальной локальной сети VLAN	ПЗ	2	ПК-1	Л1.4 ЛЗ.1 ЛЗ.2
2.11	Способы предотвращения утечки информации через ПЭМИН	СР	8	ПК-1	Л1.2 Л1.3

					Л2.1
2.12	Методы средства ограничения доступа к компонентам ЭВМ	СР	8	ПК-1	Л1.2 Л1.3 Л2.1
2.13	Надёжность средств защиты компонент в беспроводных высокоскоростных системах	СР	8	ПК-1	Л1.2 Л1.3 Л2.1 Л2.3
2.14	Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям	СР	8	ПК-1	Л1.2 Л1.3 Л2.1 Л2.3
2.15	Безопасность оптоволоконных кабельных систем.	СР	8	ПК-1	Л1.2 Л1.3 Л2.1
2.16	Расчёт и исследование характеристик локальной вычислительной сети Ethernet	СР	8	ПК-1	Л2.1 Л3.1
2.17	Подавление информационных сигналов в цепях заземления	СР	8	ПК-1	Л2.1 Л3.1 Л2.2
Зачет					
Итого – 144 часа					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1.Рекомендуемая литература				
5.1.1.Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	Захаркин С.В., Иванов В.А., Конышев М.Ю., Шишкин Н.В	Мобильные системы связи	М.: Горячая линия-Телеком, 2025	Э1
Л1.2	Лохвицкий, М.С., Сорокин А.С., Шорин О.А.	Мобильная связь: стандарты, структуры, алгоритмы, планирование	М.: Горячая линия-Телеком, 2025	Э2
Л1.3	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации	М.: РИОР, 2025	Э3
5.1.2.Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин.	Защита информации	М.: ИЦ РИОР: НИЦ ИНФРА-М, 2024	Э4
Л2.2	Ерохин С.Д., Петухов А.Н., Пилюгин П.Л.	Управление безопасностью критических информационных инфраструктур	М.: Горячая линия-Телеком, 2024	Э5
Л2.3	Баранова Е.К., Бабаш А.В.	Основы информационной безопасности	М.: РИОР, 2025	Э6

5.1.3.Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
ЛЗ.1	. Решетникова И.В., Панков Г.К., Карпенко Е.А.	Сети электросвязи и методы их защиты. Методические указания для проведения лабораторных работ	РнД: СКФ МТУСИ, 2024	Э7
ЛЗ.2	Решетникова И.В..	Программно-аппаратные средства защиты информации	РнД: СКФ МТУСИ, 2024	Э8
5.2.Электронные образовательные ресурсы				
Э1	https://elib.mtuci.ru/view.php?book_id=34654			
Э2	https://elib.mtuci.ru/view.php?book_id=3542			
Э3	https://znanium.ru/read?id=465001			
Э4	https://znanium.ru/read?id=443251			
Э5	https://elib.mtuci.ru/view.php?book_id=4161			
Э6	https://znanium.ru/read?id=472922			
Э7	https://elib.mtuci.ru/view.php?book_id=169993			
Э8	https://elib.mtuci.ru/view.php?book_id=170086			
5.3.Программное обеспечение				
П.1	MS Excel – с лицензией			
П.2	MS Word – с лицензией			
П.3	MS Power Point – с лицензией			

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционные аудитории, оснащенные проектором, ПК (ноутбуком), экраном.
6.2 МТО лабораторных работ и практических занятий	
1	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.3 МТО рубежных контролей, зачета	
1	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.4 МТО самостоятельной работы обучающихся	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы

Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

8. Методические рекомендации по освоению дисциплины

Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочесть задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины Б1.В.ДВ.04.02 «Защита информации в беспроводных высокоскоростных системах передачи данных» для использования в 20__/20__ учебном году

Утверждаю

Зам. директора по УР _____
«__» _____ 20__ г.

Направление: 11.03.02 Инфокоммуникационные технологии и системы связи

Профиль: Защищенные инфокоммуникационные системы

Форма обучения: очная, заочная.

(Возможны следующие варианты):

а) Рабочая программа действует без изменений.

б) В рабочую программу вносятся следующие изменения:

- 1)
- 2)
- 3)

Разработчик (и): _____
(ФИО, ученая степень, ученое звание)

«__» _____ 20__ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры _____

Протокол № _____ от «__» _____ 20__ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; Может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по

		соответствующей дисциплине.
--	--	-----------------------------

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
ПК-1		
Знать:		
Основные математические методы и алгоритмы шифрования, расшифрования и дешифрования сообщений. Электронной (цифровой) подписи в телекоммуникационных системах. Принципы работы, структурные схемы, протоколы и способы программирования криптосистем и систем электронной подписи.	Контрольная работа 1	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 6-8 «Отлично» - 8-10
Основные аспекты информационной безопасности; опасности и угрозы, возникающие в развитии современного информационного общества; требования информационной безопасности Методы защиты объектов от несанкционированного доступа физических лиц и основные направления противодействия техническим средствам разведки.	Контрольная работа 2	Модуль 1 0÷25 «Неудовлетворительно» - 0-10 «Удовлетворительно» - 11-15 «Хорошо» - 16-20 «Отлично» - 21-25
Уметь:		
Определять опасности и угрозы, возникающие в развитии современного информационного общества.	Практическое занятие 1 Практическое занятие 2	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 6-8 «Отлично» - 8-10
Реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации. Применять на практике технические методы защиты информации, пользоваться стандартной терминологией и определениями. Составлять протоколы шифрования и расшифрования сообщений.	Практическое занятие 5 Практическое занятие 6 Практическое занятие 7	Модуль 2 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
Владеть:		
Языком предметной области: основными терминами, понятиями, определениями в области информационной безопасности Способностью созавать опасности и угрозы, возникающие в развитии современного информационного общества Способностью созавать опасности и угрозы, возникающие в развитии	Практическое занятие 3 Практическое занятие 4	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 6-8 «Отлично» - 8-10

современного информационного общества, соблюдать основные требования информационной безопасности		
Способностью применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств электросвязи и информатики; организовывать и проводить их испытания с целью оценки соответствия требованиям технических регламентов, международных и национальных стандартов и иных нормативных документов Методы и средства инженерной защиты и технической охраны объектов Навыками о типовых разработанных средствах защиты информации и возможностями их использования в реальных задачах создания и внедрения инфокоммуникационных систем	Практическое занятие 8 Практическое занятие 9	Модуль 2 0÷5 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-3 «Хорошо» - 3-4 «Отлично» - 4-5
	Зачет	0-100 «Неудовлетворительно» - 0-40 «Удовлетворительно» - 41-60 «Хорошо» - 61-80 «Отлично» - 81-100

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные материалы для очной формы обучения

Модуль 1 (50 баллов):

Модуль содержит 5 лекционных занятия и 4 практических занятий. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненное и защищенное практическое занятие студент получает максимум 10 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ПК-1):

1. Перечислить и дать краткую характеристику систем наземной радиосвязи.
2. Типы и спутниковых систем радиосвязи. Достоинства и недостатки.
3. Виды орбит и особенности применения спутниковых систем на этих орбитах.
4. Транковые системы.
5. Принцип построения систем сотовой связи.
6. Типы систем сотовой связи.
7. Особенности поколений сотовой связи 1,2,3, 4 и 5G.
8. Сети телевизионного вещания
9. Распространение сигнала в свободном пространстве.
10. Влияние многолучевости на распространение сигнала.
11. Моделирование потерь распространения.

12. Общие свойства радиоволн.
13. Поляризация электромагнитного поля и диапазоны волн радиосигналов.
14. Особенности распространения в атмосфере радиоволн различных диапазонов.
15. Виды модуляции и ширина спектра радиосигналов.
16. Зона уверенного приема радиосигналов.
17. Структура передающих и приемных устройств.
18. Модель цифровой системы связи.
19. Классификация систем связи с подвижными объектами.
20. Основные характеристики систем связи с подвижными объектами.
21. Обобщённая структурная схема СМС.
22. Состав оборудования СМС: абонентские станции, базовые станции, сетевая подсистема.
23. Диапазоны частот, выделенные для систем подвижной радиосвязи. Планы частот.
24. Нормы на параметры излучения передатчиков систем подвижной радиосвязи. Классы излучения.
25. Концепция повторного использования частот. Кластер. Модели повторного использования частот.
26. Методы формирования и передачи сигналов в ССМС.

Практическое занятие №1

Расчет рабочих частот для радиосвязи в диапазоне коротких волн (ПК1)

Контрольные вопросы

1. Как получается дальнейшее распространение коротких волн?
2. От чего зависит радиус действия поверхностных волн КВ диапазона и чему он может быть равен?
3. Почему образуется зона молчания на КВ?
4. Как определяют практически критические частоты слоев?
5. Как получаются замирания на КВ и как с ними борются в системах радиосвязи?
6. Как устраняют прямое кругосветное эхо на КВ?

Практическое занятие №2

Расчет зоны уверенного приёма (ПК1)

Контрольные вопросы

1. Какие стандартные диапазоны радиочастот используются для теле- вещания?
2. Какие стандартные диапазоны радиочастот используются в радио- вещании на метровых радиоволнах?
3. От чего зависит расстояние прямой видимости?
4. Как влияет нормальная рефракция в тропосфере на дальность распространения радиоволн МВ и ДМВ?
5. Чем можно объяснить дальнейшее распространение УКВ и ДМВ над морской поверхностью?
6. Возможно ли отражение радиоволн МВ диапазона от ионосферы?

Практическое занятие №3

Изучение работы сетей связи с использованием программного продукта CiscoPacketTracer. (ПК1)

Контрольные вопросы

1. Пояснить алгоритм работы концентратора.
2. Что такое широковещательный пакетный шторм?
3. Ограничения на посторонние сети при использовании концентраторов?

4. Основные достоинства и недостатки концентраторов?
5. Поясните алгоритм работы коммутатора.
6. Поясните работу коммутатора в режиме самообучения.
7. Классификация коммутаторов.
8. Как решается вопрос борьбы с петлями на канальном уровне?
9. Что такое Vlan и для чего он может быть применён в сети?
10. Правила конфигурирования коммутатора при настройке Vlan.
11. Что такое магистральный порт и для чего он нужен?

Практическое занятие №4.

Исследование формирования сигнала в стандарте GSM

Организация аттестации выделенного помещения по требованиям безопасности информации (ПК1)

Контрольные вопросы

1. Принцип работы квадратурного модулятора
2. Временные интервалы в стандарте GSM.
3. Требования к спектру излучаемого сигнала
4. Принцип работы квадратурного демодулятора
5. Частотная манипуляция с минимальным частотным сдвигом
6. Эффект многолучевого распространения радиоволн
7. Способы борьбы с влиянием отраженных сигналов
8. Влияние скорости движения мобильной станции на работу канала связи

Модуль 2: (50 баллов):

Модуль содержит 5 лекционных занятий и 5 практических занятий. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 25. За выполненное и защищенное практическое занятие максимум 5 баллов. Общее максимальное количество баллов за модуль 2 составляет 50.

Вопросы для контрольной работы (ПК-1):

1. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ
2. Порядок проведения контроля защищенности АС от НСД
3. Методы контроля побочных электромагнитных излучений генераторов технических средств
4. Мероприятия по выявлению и оценке свойств каналов утечки информации
5. Специальные проверки
6. Специальные обследования
7. Специальные исследования.
8. Основные способы защиты от потери информации и нарушений работоспособности сетей и систем
9. Внесение функциональной и информационной избыточности.
10. Способы резервирования информации; правила обновления резервных данных.
11. Методы сжатия информации.
12. Архивация файловых данных.
13. Резервирование системных данных; подготовка к программной среде.
14. Концептуальные вопросы построения уровней защиты систем управления базами данных (СУБД).
15. Основные требования к подсистеме безопасности СУБД.
16. Общие сведения о разграничении доступа к базам данных.
17. Обязанности администратора по защите баз данных от несанкционированного

доступа.

18. Определение полномочий пользователей по доступу к базе данных
19. Методы формирования и передачи сигналов в ССМС.
20. Виды модуляции в системах связи с подвижными объектами. Непрерывные виды модуляции. Дискретные виды модуляции.
21. Методы многостанционного доступа в системах подвижной связи.
22. Принципы кодового разделения каналов.
23. Прямое расширение спектра частот. 1
24. Скачкообразное изменение частоты несущей.
25. OFDM модуляция. OFDMA многостанционный доступ.
26. Основные сведения о помехоустойчивом кодировании в СМС.
27. Основные сведения о сжатии речи в СМС.

Практическое занятие №5

Принципы построения и типы транкинговых систем (ПК1)

Контрольные вопросы

1. Дайте характеристику общих требований к транкинговым системам.
2. Каковы принципы построения и функционирования транкинговых систем?
3. Дайте характеристику режимов работы транкинговых систем.
4. Какова классификация транкинговых систем?
5. Поясните принцип передачи речи в стандарте TETRA.
6. Поясните принцип передачи данных в стандарте TETRA.
7. Какова структура сети стандарта TETRA?

Практическое занятие №6

Изучение работы маршрутизатора с использованием CiscoPacketTracer (ПК1)

Контрольные вопросы

1. Каковы правила составления статического маршрута?
2. Каковы принципы динамической маршрутизации?
3. Как выполнять конфигурирование оборудования при настройке маршрутизаторов и коммутаторов третьего уровня?
4. Как построить сеть на базе маршрутизаторов?
5. Как определить адресацию в сети?
6. Как выполняется формирование таблиц маршрутизации.
7. Как произвести настройку статического конфигурирования?
8. Как произвести настройку протокола RIP?
9. Как произвести настройку протокола OSPF?

Практическое занятие №7

Изучение возможностей работы протокола NAT (ПК1)

Контрольные вопросы

1. Опишите все возможные схемы работы службы NAT.
2. Какие частные IP адреса используются службой NAT в каждом классе адресов?
3. Перечислите преимущества и недостатки службы NAT.
4. Перечислите этапы настройки службы NAT.
5. Опишите схему проверки работы службы NAT.
6. Опишите основные проблемы в работе сервера NAT.
7. Что обеспечивает служба NAT?

Практическое занятие №8

Конфигурирование списков управления доступом ACL (ПК1)

Контрольные вопросы

1. Какие параметры контролирует расширенные списки доступа?
2. Приведите пример команды, разрешающей передачу пакетов от хоста на все веб-сервера.
3. Перечислите основные типы списков доступа.
4. Что такое шаблон маски подсети и приведите примеры его использования в списках доступа.
5. Какое правило обработки сетевого трафика задает следующий список доступа:
Ipaccess-list 111 deny tcp any any eq 80.
6. Локальная сеть соединена с роутером по интерфейсу Fa0/0, а внешняя сеть соединена по интерфейсу Fa0/1. Из локальной сети запрещен вход во внешнюю сеть, а из внешней сети запрещено входить на FTP сервер, расположенный во внутренней сети. Для реализации этих правил был создан список доступа. Назовите интерфейс и в каком направлении (на вход или на выход), к которому следует применить созданный список доступа.
7. Для какого варианта не может быть проведено сравнение на основе расширенного списка доступа IP?
 - протокол;
 - IP адрес отправителя;
 - IP адрес получателя;
 - имя файла для передачи по протоколу FTP.
8. Назовите, какой шаблон маски соответствует сети 10.16.0.0./12?
9. В списке доступа содержится следующее правило: Permit any host 192/168/1/1/it 25. Какие номера портов оно обрабатывает?
10. Напишите правило доступа для входа в любую сеть вашей схемы.

Практическое занятие №9

Конфигурирование виртуальной локальной сети VLAN (ПК1)

Контрольные вопросы

1. Для чего создаются виртуальные локальные сети и каковы их достоинства?
2. Как связываются между собой VLAN и порты коммутатора?
3. Как обеспечивается общение между узлами разных виртуальных сетей?
4. Как обеспечивается управление виртуальными локальными сетями?
5. Можно ли построить VLAN на нескольких коммутаторах и как это сделать?
6. Для чего служит идентификатор кадра (tag) и где он размещается?
7. Что такое транковый порт и зачем он создаётся?
8. Как он создается транковый порт на коммутаторе и маршрутизаторе?
9. Какие команды используются для назначения VLAN на интерфейсы?
10. Какие команды используются для создания транковых соединений?
11. Какие команды используются для верификации VLAN?

1.3.2 Вопросы, выносимые на зачет по дисциплине «Защита информации в беспроводных высокоскоростных системах передачи данных»

1. Перечислить и дать краткую характеристику систем наземной радиосвязи. (ПК-1).
2. Типы и спутниковых систем радиосвязи. Достоинства и недостатки. (ПК-1).
3. Виды орбит и особенности применения спутниковых систем на этих орбитах. (ПК-1).
4. Транковые системы. (ПК-1).
5. Принцип построения систем сотовой связи. (ПК-1).
6. Типы систем сотовой связи. (ПК-1).
7. Особенности поколений сотовой связи 1,2,3, 4 и 5 G. (ПК-1).
8. Сети телевизионного вещания (ПК-1).

9. Распространение сигнала в свободном пространстве. (ПК-1).
10. Влияние многолучевости на распространение сигнала. (ПК-1).
11. Моделирование потерь распространения. (ПК-1).
12. Общие свойства радиоволн. (ПК-1).
13. Поляризация электромагнитного поля и диапазоны волн радиосигналов. (ПК-1).
14. Особенности распространения в атмосфере радиоволн различных диапазонов. (ПК-1).
15. Виды модуляции и ширина спектра радиосигналов. (ПК-1).
16. Зона уверенного приема радиосигналов. (ПК-1).
17. Структура передающих и приемных устройств. (ПК-1).
18. Модель цифровой системы связи. (ПК-1).
19. Классификация систем связи с подвижными объектами. (ПК-1).
20. Основные характеристики систем связи с подвижными объектами. (ПК-1).
21. Обобщённая структурная схема СМС. (ПК-1).
22. Состав оборудования СМС: абонентские станции, базовые станции, сетевая подсистема. (ПК-1).
23. Диапазоны частот, выделенные для систем подвижной радиосвязи. Планы частот. (ПК-1).
24. Нормы на параметры излучения передатчиков систем подвижной радиосвязи. Классы излучения. (ПК-1).
25. Концепция повторного использования частот. Кластер. Модели повторного использования частот. (ПК-1).
26. Методы формирования и передачи сигналов в ССМС. (ПК-1).
27. Виды модуляции в системах связи с подвижными объектами. Непрерывные виды модуляции. Дискретные виды модуляции. (ПК-1).
28. Методы многостанционного доступа в системах подвижной связи. (ПК-1).
29. Принципы кодового разделения каналов. (ПК-1).
30. Прямое расширение спектра частот. (ПК-1).
31. Скачкообразное изменение частоты несущей. (ПК-1).
32. OFDM модуляция. OFDMA многостанционный доступ. (ПК-1).
33. Основные сведения о помехоустойчивом кодировании в СМС. (ПК-1).
34. Основные сведения о сжатии речи в СМС. (ПК-1).
35. Виброакустические технические каналы утечки речевой информации (ПК-1).
36. Оптико-электронный технический канал утечки речевой информации (ПК-1).
37. Технические каналы утечки видовой информации. Способы скрытого видеонаблюдения и съемки (ПК-1).
38. Технические каналы утечки видовой информации (ПК-1).
39. Способы скрытого видеонаблюдения и съемки (ПК-1).
40. Демаскирующие признаки объектов (ПК-1).
41. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра (ПК-1).
42. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра (ПК-1).
43. Демаскирующие признаки радиоэлектронных средств (ПК-1).
44. Индикаторы электромагнитного поля (ПК-1).
45. Сканирующие радиоприемники (ПК-1).
46. Анализаторы спектра, радиочастотомеры (ПК-1).
47. Многофункциональные комплекты для выявления каналов утечки информации (ПК-1).
48. Скрытие речевой информации в телефонных системах с использованием криптографических методов (ПК-1).
49. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах (ПК-1).
50. Специальные исследования акустических и виброакустических каналов (ПК-1).

51. Специальные исследования акустоэлектрических преобразований (ПК-1).
52. Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок (ПК-1).
53. Излучатели электромагнитных полей (ПК-1).
54. Утечка информации по цепям заземления (ПК-1).
55. Утечка информации по цепям питания (ПК-1).
56. Высокочастотное навязывание (ПК-1).
57. Утечка информации по акустическим каналам (ПК-1).
58. Прямой акустический канал (ПК-1).
59. Виброакустический канал (ПК-1).
60. Оптико-акустический канал (ПК-1).
61. Электроакустический канал (ПК-1).

1.4 Оценочные средства для заочной формы обучения

Практическое занятие №1

Изучение работы маршрутизатора с использованием CiscoPacketTracer (ПК1)

Контрольные вопросы

1. Каковы правила составления статического маршрута?
2. Каковы принципы динамической маршрутизации?
3. Как выполнять конфигурирование оборудования при настройке маршрутизаторов и коммутаторов третьего уровня?
4. Как построить сеть на базе маршрутизаторов?
5. Как определить адресацию в сети?
6. Как выполняется формирование таблиц маршрутизации.
7. Как произвести настройку статического конфигурирования?
8. Как произвести настройку протокола RIP?
9. Как произвести настройку протокола OSPF?

Практическое занятие №2

Конфигурирование списков управления доступом ACL (ПК1)

Контрольные вопросы

1. Какие параметры контролирует расширенные списки доступа?
2. Приведите пример команды, разрешающей передачу пакетов от хоста на все веб-сервера.
3. Перечислите основные типы списков доступа.
4. Что такое шаблон маски подсети и приведите примеры его использования в списках доступа.
5. Какое правило обработки сетевого трафика задает следующий список доступа:
Ipaccess-list 111 deny tcp any any eq 80.
6. Локальная сеть соединена с роутером по интерфейсу Fa0/0, а внешняя сеть соединена по интерфейсу Fa0/1. Из локальной сети запрещен вход во внешнюю сеть, а из внешней сети запрещено входить на FTP сервер, расположенный во внутренней сети. Для реализации этих правил был создан список доступа. Назовите интерфейс и в каком направлении (на вход или на выход), к которому следует применить созданный список доступа.
7. Для какого варианта не может быть проведено сравнение на основе расширенного списка доступа IP?
 - протокол;
 - IP адрес отправителя;
 - IP адрес получателя;

- имя файла для передачи по протоколу FTP.

8. Назовите, какой шаблон маски соответствует сети 10.16.0.0/12?

9. В списке доступа содержится следующее правило: Permitanyhost 192/168/1/1/it 25. Какие номера портов оно обрабатывает?

10. Напишите правило доступа для входа в любую сеть вашей схемы.

Практическое занятие №3

Конфигурирование виртуальной локальной сети VLAN (ПК1)

Контрольные вопросы

1. Для чего создаются виртуальные локальные сети и каковы их достоинства?
2. Как связываются между собой VLAN и порты коммутатора?
3. Как обеспечивается общение между узлами разных виртуальных сетей?
4. Как обеспечивается управление виртуальными локальными сетями?
5. Можно ли построить VLAN на нескольких коммутаторах и как это сделать?
6. Для чего служит идентификатор кадра (tag) и где он размещается?
7. Что такое транковый порт и зачем он создаётся?
8. Как он создается транковый порт на коммутаторе и маршрутизаторе?
9. Какие команды используются для назначения VLAN на интерфейсы?
10. Какие команды используются для создания транковых соединений?
11. Какие команды используются для верификации VLAN?

Вопросы, выносимые на зачет такие же, как и для студентов очной формы обучения

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

2.1 Порядок и методика проведения текущего контроля и промежуточной аттестации

Предусмотрены следующие виды контроля:

- промежуточный контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- промежуточный контроль по каждому модулю – в форме отчетов по практическим занятиям для оценки практических навыков;
- итоговый контроль по дисциплине – в форме зачет с оценкой.

Текущий контроль успеваемости в форме защиты результатов практических занятий проводится в два этапа:

- 1-й этап: допуск к выполнению практического занятия – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний студентов теоретической части практического занятия и готовности к выполнению практических исследований;
- 2-й этап выполняется по окончании каждого практического занятия в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки студентом практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения студентов к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса,

снижения роли случайных и субъективных факторов при оценивании учебной деятельности студентов в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимся баллы могут быть переведены в оценку:

- «неудовлетворительно» - от 0% до 40% от максимального количества баллов;
- «удовлетворительно» - от 41% до 60% максимального количества баллов;
- «хорошо» - от 61% до 80% максимального количества баллов;
- «отлично» - от 81% до 100% максимального количества баллов.

Соотношения максимального количества баллов, полученных студентом по блокам модулей, показаны в Таблице

Таблица - Распределение баллов по блокам модулей дисциплины «Защита информации в беспроводных высокоскоростных системах передачи данных»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок (Распределение баллов по занятиям)
Модуль 1	50	10	40=10+10+10+10
Модуль 2	50	25	25=5+5+5+5+5
Модуль - зачет	100	100	

Как правило, теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения заданий на практических занятиях.

Результаты текущего контроля доводятся до сведения обучающихся на последнем занятии до проведения промежуточной аттестации.

На зачете с оценкой производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуются формировать вопросы в билетах к зачету таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

2.2 Методика проведения зачета в группах заочной формы обучения

Зачет по дисциплине «Защита информации в беспроводных высокоскоростных системах передачи данных» у студентов заочной формы обучения проводится письменно по классической методике. Вопросы сгруппированы в билетах. В каждом билете содержится по 2 теоретических вопроса. Количество билетов должно быть не менее числа студентов в группе. Студенты готовят письменные ответы на вопросы.

3 Промежуточная аттестация

Промежуточная аттестация проводится в форме зачета с оценкой. Зачет с оценкой проводится по расписанию экзаменационной сессии в письменном виде. Количество вопросов в экзаменационном билете – 2. Проверка ответов и объявление результатов производится в день зачета. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку обучающегося.

Образец экзаменационного билета к зачету с оценкой

	Федеральное агентство связи Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»	Утверждаю Зав. кафедрой «ИТСС» _____ Юхнов В.И. «___» _____ 20__ г.
Направление подготовки: 11.03.02 Инфокоммуникационные технологии и системы связи Курс: 4 Дисциплина: Защита информации в беспроводных высокоскоростных системах передачи данных		
Билет №10 1. Особенности поколений сотовой связи 1,2,3, 4 и 5 G. 2. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах. Доцент каф. «ИТСС» _____ Руденко Н.В. «___» _____ 20__ г.		

Один комплект отпечатанных экзаменационных билетов подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину

4 Тестовые задания для проведения оценки сформированности компетенции ПК-1

Тестовые задания позволяют оценить уровень сформированности компетенции ПК-1 - Способен обеспечить защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи.

На компетенцию ПК-1 сформировано 20 тестовых заданий. Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень содержит 50% тестовых заданий. Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень составляет 35 % заданий. В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень составляют – 15 % заданий. В заданиях используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	Как называется атака на систему, целью которой является довести её до отказа?

№ задания	Тексты заданий
	Выберите ответ: 1. Атака на уровне приложений 2. Подмена доверенного объекта в сети 3. Отказ в обслуживании 4. Отказ фильтрации трафика на уровне сети
2	Как называется атака, при которой злоумышленник получает доступ к системе от имени пользователя приложения? 1. Анализ сетевого трафика 2. Отказ в обслуживании 3. Атака на уровне сервера 4. Атака на уровне приложений
3	Какой диапазон акустических волн соответствует звуковому диапазону? 1 300-16000 Гц 2 1-300 Гц 3 16000-4 МГц 4 4-9МГц
4	Как называется устройство разведки, которое передает информацию злоумышленнику с помощью электромагнитных волн радиочастотного диапазона? 1 радиомаяк 2 анализатор спектра 3 радиозакладка 4 радиоприемник
5	Как называется основной орган внешней разведки Российской Федерации? 1 ФСТЭК России 2 СВР России 3 ФСБ России 4 ВКС России
6	Какое свойство информации нарушено, если в результате действий злоумышленников легитимный пользователь не может получить доступ к социальной сети? 1. Доступность 2. Целостность 3. Неотказуемость 4. Конфиденциальность
7	Подмена доверенного объекта в сети по-другому называется: 1. спуфинг 2. фишинг 3. шугаринг 4. скриминг
8	Установка аппаратного межсетевого экрана относится к: 1. Морально-этическим мерам обеспечения безопасности 2. Техническим мерам обеспечения безопасности 3. Физическим мерам обеспечения безопасности 4. Организационным мерам обеспечения безопасности
9	Какой орган исполнительной власти осуществляет контроль в области криптографической защиты информации? 1. Роскомнадзор 2. ФСТЭК России 3. МВД России

№ задания	Тексты заданий
	4. ФСБ России
10	В соответствии с каким документом производится аттестация объекта информатизации? 1. Указ Президента “Об аттестации объектов информатизации по требованиям безопасности информации” 2. Положение по аттестации объектов информатизации по требованиям безопасности информации 3. Федеральный Закон «Об аттестации» 4. Федеральный Закон «О государственной тайне»

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Установите соответствие указанным ниже понятиям своим определениям 1. Уязвимость 2. Потеря информации 3. Риск 4. Угроза безопасности информации А. Потенциально возможный ущерб Б. Слабое место в системе, которое может позволить злоумышленнику получить несанкционированный доступ, нарушить работу, украсть или изменить данные. В. Совокупность условий и факторов, создающих потенциальную или реальную опасность, связанную с утечкой информации. Г. Повреждение или утрата информации из-за различных факторов, случайных или намеренных действий.
12	Установите соответствие указанным ниже понятиям своим определениям 1. Доступность информации 2. Конфиденциальность 3. Целостность информации 4. Масштабируемость А. Необходимость предотвращения разглашения, утечки какой-либо информации. Б. Состояние информации, при котором отсутствует любое её изменение или изменение осуществляется только преднамеренно субъектами, имеющими на это право. В. Способность системы справляться с увеличивающейся нагрузкой без потери производительности Г. Состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно.
13	Установите соответствие характеристикам индикатора электромагнитного поля ST111 единицам измерения 1. Диапазон частот 2. Пороговая чувствительность 3. Потребляемый ток 4. Погрешность измерения частоты

№ задания	Тексты заданий
	А. % Б. мА В. МГц Г. Вт/см²
14	Установите соответствие указанным ниже понятиям своим определениям - IDS - Брандмауэр - Камкодер - RSA А. Система межсетевого экранирования Б. Криптографический алгоритм с открытым ключом В. видеокамера со встроенным портативным видеоманитофоном Г. система обнаружения вторжений

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности. *Инструкция: Прочитайте текст и установите правильную последовательность*

№ задания	Тексты заданий
15	Установите правильный порядок проведения технического контроля эффективности защиты информации: 1. Определение эффективности принятых мер защиты, предложение необходимых мер усиления защиты. Документальное оформление результатов. 2. Измерение нормируемых технических параметров защищаемого объекта по отдельным физическим полям на границе контролируемой зоны; 3. Определение возможных типов и средств технической разведки и предварительный расчет зон разведдоступности. 4. Определение состава и подготовки к работе контрольно-измерительной аппаратуры; 5. Сбор исходных данных, характеризующих уязвимости объекта информатизации по отношению к воздействиям технической разведки
16	Установите правильный порядок проведения инструментального контроля ПЭМИН: 1. Измерение параметров применяемых средств защиты (фильтров в отходящих линиях, систем активного зашумления и т.д.). 2. Оформление протоколов по результатам проведенных проверок. 3. Измерение уровней ПЭМИ и наводок информативных сигналов 4. Расчет выполнения норм и оценка защищенности.
17	Установите правильный порядок подготовки к работе, обнаружения и определения местоположения радиопередающих устройств (РПУ) с помощью детектора поля ST111 1. Установить порог индикации в одном из ближайших к проверяемому помещений. 2. Подключить ВЧ антенну к основному блоку. 3. При приближении изделия к РПУ наблюдать увеличение количество сегментов индикатора уровня. 4. Включить изделие. В случае появления надписи: «АККУМУЛЯТОР РАЗРЯЖЕН»

№ задания	Тексты заданий
	зарядить аккумулятор». 5. В случае, если местонахождение РПУ не выявлено, уменьшить чувствительность шкал индикации, установить новый нулевой порог относительно данного уровня сигнала и продолжать поиск.

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Добавить недостающие слова в определение электромеханических средств защиты информации: <i>Электромеханические средства защиты информации — это устройства, которые сочетают механические и электрические компоненты для предотвращения _____ доступа к _____, блокировки каналов утечки данных и обеспечения физической безопасности объектов.</i>
19	Добавить недостающие слова в содержание активных методов защиты информации Активные методы защиты информации содержат: - создание активных _____ для подавления вражеских РЭС; - использование генераторов _____ для маскировки информационных сигналов; - применение _____ целей и ловушек.
20	Определить особенности различных типов USB-ключей <i>Требуют физического подключения к компьютеру через USB-порт – это особенность _____</i> <i>Используют Bluetooth или RFID для связи с устройством – это особенность _____</i> <i>Требуют специального считывателя – это особенность _____</i>

Методика проведения тестирования

Максимальное время выполнения теста - 60 минут.

Количество тестовых заданий в тесте не менее 20. Для проведения контроля остаточных знаний компьютер формирует в случайном порядке 60 тестовых заданий.

При прохождении тестового контроля знаний обучающийся должен выбрать один или несколько правильных ответов в каждом тестовом задании.

В случае правильного ответа на **17** и более тестовых заданий (81-100% правильных ответов) обучающийся подтверждает освоение компетенций с уровнем «отлично». При ответе на **13** тестовых заданий (61-80% правильных ответов) обучающийся подтверждает освоение компетенций с уровнем «хорошо». При ответе на **9** тестовых заданий (41-60% правильных ответов) обучающийся подтверждает освоение компетенций с уровнем «удовлетворительно». При ответе менее чем на **8** тестовых заданий (0-40% правильных ответов) обучающийся не подтверждает необходимый уровень знаний и оценивается «неудовлетворительно».

Критерии оценивания ответов на тестовые задания (ПК-1)

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 3 баллами. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой; если допущена одна ошибка/неточность/ответ правильный, но не полный - 1 балл, если допущено более одной ошибки/ответ неправильный/ответ отсутствует- 0 баллов.

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Дисциплина «Защита информации в беспроводных высокоскоростных системах передачи данных» включает в себя для ОФО:

- лекционные занятия – 36 часов;
 - практические занятия – 36 часов;
 - промежуточную аттестацию – зачет с оценкой (7 семестр);
- для ЗФО:

- лекционные занятия – 2 часа;
- практические занятия – 6 часов;
- промежуточную аттестацию – зачет с оценкой 5 курс (2 сессия).

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

На практических занятиях следует обратить внимание на соответствие выбираемых обучающимися средств решаемым в работе задачам.

Во время выполнения заданий в учебной аудитории обучающийся может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, обучающийся может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего контроля и контроля знаний обучающихся при проведении промежуточной аттестации.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы обучающегося на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по подготовке к лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов,

научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности обучающихся.

2.2 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа обучающегося под управлением преподавателя. На них пополняются теоретические знания обучающихся, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение обучающихся к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия обучающийся обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к практическим занятиям;
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях;
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятий, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.