

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 УР

Н.А. Андреева

«28» 04 2026 г.

Технические средства и методы защиты информации

Б1.В.ДВ.04.01

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),
курсам (для заочной формы обучения)**

Вид учебной работы	ОФ		ЗФ	
	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 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

Технические средства и методы защиты информации

Разработана в соответствии с ФГОС ВО:

направления подготовки

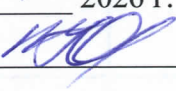
11.03.02 ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ СВЯЗИ,
утвержденным приказом Министерства образования и науки Российской Федерации от
19 сентября 2017 г. № 930.

Составлена на основании учебных планов

направления **11.03.02 Инфокоммуникационные технологии и системы связи**
профилей «Защищенные инфокоммуникационные системы», «Мобильная связь и
интернет вещей», «Инфокоммуникационные системы и сети», одобренных Учёным
советом СКФ МТУСИ, протокол № 8 от 31.03 2026 г., и утвержденного
директором СКФ МТУСИ 31.03 2026г.

Одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от 28.04 2026 г. № 9

Зав. кафедрой  В.И. Юхнов

1. Цели изучения дисциплины

Целью преподавания дисциплины является формирование у обучающихся знаний в области методов и средств инженерной защиты информации, а также возможностями их использования в реальных задачах создания и внедрения инфокоммуникационных систем

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 сознавать опасности и угрозы, возникающие в развитии современного информационного общества Способностью сознавать 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	Б1.В.ДВ.04.02 «Защита информации в беспроводных высокоскоростных системах передачи данных»

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 Концепция инженерно-технической защиты информации – 36 (18 Лек+18 ПЗ) часов контактной работы, 36 часов СР					
1.1	Лекция 1. Основные определения и понятия. 1. Характеристика инженерно-технической защиты информации как области информационной безопасности. 2. Основные проблемы инженерно-технической защиты информации. 3. Представление сил и средств защиты информации в виде системы. 4. Основные параметры системы защиты информации	Лек.	6	ПК-1	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. Теоретические основы инженерно-технической защиты информации. Особенности информации как предмета защиты. 1. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. 2. Принципы защиты информации техническими средствами. 3. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.	Лек.	6	ПК-1	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. Характеристика технической разведки Основные задачи и органы технической разведки.	Лек.	6	ПК-1	Л1.1 Л1.2 Л1.3
1.4	Практическое занятие 1. Изучение законодательной и нормативной базы правового регулирования вопросов защиты информации	ПЗ	4	ПК-1	Л3.1

1.5	Практическое занятие 2. Изучение задач и функций органов по технической защите информации в РФ	ПЗ	4	ПК-1	ЛЗ.1
1.6	Практическое занятие 3. Изучение положений о государственном лицензировании деятельности в области защиты информации	ПЗ	6	ПК-1	ЛЗ.1
1.7	Практическое занятие 4. Организация аттестации выделенного помещения по требованиям безопасности информации	ПЗ	4	ПК-1	ЛЗ.2
1.8	Демаскирующие признаки объектов Параметрические технические каналы утечки речевой информации Акустоэлектрические каналы утечки речевой информации Демаскирующие признаки объектов в видимом диапазоне Демаскирующие признаки объектов в инфракрасном диапазоне Демаскирующие признаки радиоэлектронных средств Виброакустические технические каналы утечки речевой информации	СР	36	ПК-1	Л1.1 Л1.2 Л1.3
Модуль 2 – Технический контроль эффективности мер защиты информации - 36 (18 Лек+18 ПЗ) часов контактной работы, 36 часов СР					
2.1	Лекция 4. Общие вопросы организации противодействия технической разведке. 1. Основные организационные и технические мероприятия, используемые для противодействия технической разведке. 2. Методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам. 3. Физические основы образования побочных электромагнитных излучений от технических средств.	Лек.	4	ПК-1	Л1.1 Л1.2 Л2.1
2.2	Практическое занятие 5 «Исследование детектора электромагнитного поля ST111».	ПЗ	2	ПК-1	Л1.1 ЛЗ.1
2.3	Практическое занятие 6 Обнаружение сигналов линейных и сетевых закладок	ПЗ	4	ПК-1	Л1.1 ЛЗ.1
2.4	Лекция 5. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. 1. Основные этапы доступа к ресурсам вычислительной системы. 2. Использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания. 3. Способы разграничения доступа к	Лек.	4	ПК-1	Л1.3 Л2.1 Л2.2 Л2.3

	компьютерным ресурсам; разграничение доступа по спискам.				
2.5	Лекция 6. Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок	Лек.	4	ПК-1	Л1.1 Л1.2
2.6	Лекция №7. Цели и задачи технического контроля эффективности мер защиты информации 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	Лек.	6	ПК-1	Л1.1 Л1.2
2.7	Практическое занятие 7 Изучение положений о сертификации средств защиты информации по требованиям безопасности информации	ПЗ	4	ПК-1	Л1.1 Л3.1
2.8	Практическое занятие 8 Изучение положения о сертификации средств вычислительной техники и связи	ПЗ	4	ПК-1	Л3.1
2.9	Практическое занятие 9 Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации	ПЗ	4	ПК-1	Л3.1
2.10	Способы предотвращения утечки информации через ПЭМИН ПК Методы средства ограничения доступа к компонентам ЭВМ Надёжность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям Безопасность оптоволоконных кабельных систем. Заземление технических средств и подавление информационных сигналов в цепях заземления	СР	36	ПК-1	Л1.1 Л1.2 Л1.3
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 Концепция инженерно-технической защиты информации - 36 (2 Лек+34 ПЗ) часов контактной работы, 36 часов СР					
1.1	Лекция 1. Основные определения и понятия. 1. Характеристика инженерно-технической защиты информации как области информационной безопасности. 2. Основные проблемы инженерно-технической	Лек.	2	ПК-1	Л1.1 Л1.2 Л1.3

	защиты информации. 3. Представление сил и средств защиты информации в виде системы. 4. Основные параметры системы защиты информации				
1.2	Изучение законодательной и нормативной базы правового регулирования вопросов защиты информации	СР	4	ПК-1	ЛЗ.1 Л1.3
1.3	Методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам; физические основы образования побочных электромагнитных излучений от технических средств; каналы утечки информации Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля; взаимная проверка подлинности и другие случаи опознания; способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам	СР	14	ПК-1	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3
1.4	Демаскирующие признаки объектов Параметрические технические каналы утечки речевой информации Акустоэлектрические каналы утечки речевой информации Демаскирующие признаки объектов в видимом диапазоне Демаскирующие признаки объектов в инфракрасном диапазоне Демаскирующие признаки радиоэлектронных средств Виброакустические технические каналы утечки речевой информации	СР	16	ПК-1	Л1.1 Л1.2 Л1.3 Л2.1
Курс 5, сессия 2					
Модуль 2 – Технический контроль эффективности мер защиты информации –8 (2 Лек+6 ПЗ) часов контактной работы, 100 часов СР					
2.1	Лекция 2. Общие вопросы организации противодействия технической разведке. 1. Основные организационные и технические мероприятия, используемые для противодействия технической разведке. 2. Методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам. 3. Физические основы образования побочных электромагнитных излучений от технических средств.	Лек	2	ПК-1	Л1.1 Л1.2 Л2.1 Л2.3
2.2	Практическое занятие №2 Изучение положений о сертификации средств защиты информации по требованиям безопасности	ПЗ	6	ПК-1	ЛЗ.1

	информации				
2.3	Способы предотвращения утечки информации через ПЭМИН ПК Методы средства ограничения доступа к компонентам ЭВМ Надёжность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям Безопасность оптоволоконных кабельных систем. Заземление технических средств и подавление информационных сигналов в цепях заземления	СР	100	ПК-1	Л1.1 Л1.2 Л2.1 Л3.1
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	Зайцев А.П., Мещеряков Р.В., Шелупанов А.А.	Технические средства и методы защиты информации	М.: Горячая линия-Телеком, 2025	Э1
Л1.2	Бузов Г.А.	Защита информации ограниченного доступа от утечки по техническим каналам	М.: Горячая линия-Телеком, 2024	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.
Л3.1	Решетникова И.В.,	Методические указания к практическим занятиям по дисциплине «Технические средства	РнД: СКФ МТУСИ, 2022	Э7

	Карпенко Е.А. и методы защиты информации»		
5.2.Электронные образовательные ресурсы			
Э1	https://elib.mtuci.ru/view.php?book_id=4112		
Э2	https://elib.mtuci.ru/view.php?book_id=3168		
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=170008		
5.3.Программное обеспечение			
П.1	MS Excel – с лицензией		
П.2	MS Word – с лицензией		
П.3	MS Power Point – с лицензией		
П.4	ПО «ST111 Analyzer»		
П.5	ПО «Металлоискатель ВМ-611 Вихрь»		

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 студентов	
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.04.01 «Технические средства и методы защиты информации» 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. 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. Определять опасности и угрозы, возникающие в развитии современного информационного общества.	Практическое занятие 1 Практическое занятие 2 Практическое занятие 3	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 4 Практическое занятие 5 Практическое занятие 6	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	Лабораторная работа 1	Модуль 1 0÷10 «Неудовлетворительно» - 0-3 «Удовлетворительно» - 4-6 «Хорошо» - 6-8 «Отлично» - 8-10

Способностью созавать опасности и угрозы, возникающие в развитии современного информационного общества, соблюдать основные требования информационной безопасности 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	Лабораторная работа 2 Лабораторная работа 3	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

Данная дисциплина формирует у обучающегося 1 компетенцию

Модуль 1 (50 баллов):

Модуль содержит 3 лекционных занятия, 3 практическое и 1 лабораторное занятия. 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; за лабораторную работу - максимум 10 баллов. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ПК-1):

Характеристика инженерно-технической защиты информации как области информационной безопасности.

Основные проблемы инженерно-технической защиты информации.

Представление сил и средств защиты информации в виде системы.

Основные параметры системы защиты информации

Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации.

Принципы защиты информации техническими средствами.

Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.

Кто является основным ответственным за определение уровня классификации информации?

Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

Что такое политика безопасности?

Практическое занятие №1 Изучение законодательной и нормативной базы правового регулирования вопросов защиты информации (ПК1)

Контрольные вопросы

- Назовите основные виды конфиденциальной информации.
- Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?
- Охарактеризуйте место правовых мер в системе комплексной защиты информации.
- Назовите интересы государства в области обеспечения информационной безопасности.
- Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.
- Какой закон определяет понятие «официальный документ»?
- Какой закон определяет понятие «электронный документ»?
- В каком законе приведена классификация средств защиты информации?
- Назовите основные положения Доктрины информационной безопасности РФ.
- Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?
- Дайте определение системы защиты государственной тайны и укажите ее составляющие.
- Что в соответствии с законодательством РФ представляет собой засекречивание информации.
- Перечислите основные принципы засекречивания информации.
- Что понимается под профессиональной тайной?
- Какие виды профессиональных тайн вам известны?
- Что представляет собой электронная подпись?

Практическое занятие №2

Изучение задач и функций органов по технической защите информации в РФ (ПК-1)

Контрольные вопросы

1. Перечислите органы государственного регулирования и контроля в области информационной безопасности РФ. Каковы основные направления их деятельности?
2. Какие организации в области технической защиты информации являются ключевыми органами?
3. Назовите документы, которым руководствуется ФСБ России в своей деятельности?
3. Перечислите основные задачи ФСБ в области технической защиты информации.
4. Перечислите основные функции ФСБ в области технической защиты информации.
5. В каком случае ФСБ России имеет право проводить плановые проверки?
6. Перечислите основные задачи ФСТЭК в области технической защиты информации.
7. Перечислите основные функции ФСТЭК в области технической защиты информации.
8. Каковы полномочия ФСТЭК?

Практическое занятие №3 Изучение положений о государственном лицензировании деятельности в области защиты информации (ПК1)

Контрольные вопросы

- Сформулируйте основные понятия, принятые в сфере государственного лицензирования в области защиты информации.
- Организационная структура системы государственного лицензирования в области защиты информации.
- Функции государственных органов по лицензированию в области защиты информации.
- Функции лицензионных центров по лицензированию в области защиты информации.
- Права и обязанности лицензиатов.

Порядок проведения лицензирования и контроля за деятельностью лицензиатов.
Назовите случаи приостановления или прекращения действия лицензии.
В каких случаях предприятию отказывают в выдаче лицензии?
Какие документы предоставляются для получения лицензии?
Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
Какие средства относятся к шифровальным?
Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?
Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.
Назовите лицензионные требования и условия при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
Назовите лицензионные требования и условия при предоставлении услуг в области шифрования информации.
Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.

Практическое занятие №4. Организация аттестации выделенного помещения по требованиям безопасности информации (ПК1)

Порядок проведения занятия

Составить самостоятельно (или получить у преподавателя) документацию на контролируемое помещение, изучить ее, определить возможные разведопасные направления и возможные виды разведки.

Изобразить план-схему исследуемого помещения.

На основании нижеприведенной методики, составить план проведения визуального осмотра помещения и выявить объекты, требующие при обследовании использования имеющихся средств видеонаблюдения и металлодетектора.

Сделать выводы по результатам проделанной работы и подготовить отчет.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

Придерживаться рекомендаций, указанных в Лабораторном практикуме

Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.

Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.

Предъявить отчет преподавателю для подтверждения факта выполнения практического занятия.

Контрольные вопросы (ПК-1):

1. Средства акустического контроля.
2. Аппаратура для съема информации с окон.
3. Специальная звукозаписывающая аппаратура.
4. Микрофоны различного назначения и исполнения.
5. Электросетевые подслушивающие устройства.
6. Приборы для съема информации с телефонной линии связи и сотовых телефонов.
7. Специальные системы наблюдения и передачи видеоизображений.
8. Специальные фотоаппараты.
9. Приборы наблюдения в дневное время и приборы ночного видения.
10. Специальные средства радиоперехвата и приема ПЭМИН и др

Модуль 2: (50 баллов):

Модуль содержит 4 лекционных занятия, 3 практического и 2 лабораторных 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. За выполненную и защищенную лабораторную работу студент получает максимум 5 баллов. Общее максимальное количество баллов за модуль 2 составляет 50.

Вопросы для контрольной работы (ПК-1):

1. Основные организационные и технические мероприятия, используемые для противодействия технической разведке.
2. Методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам;
3. Физические основы образования побочных электромагнитных излучений от технических средств.
4. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах.
5. Базовые этапы построения системы комплексной защиты вычислительных систем.
6. Анализ моделей нарушителя; угрозы информационно-программному обеспечению.
7. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.
8. Основные этапы доступа к ресурсам вычислительной системы; использование простого пароля; использование динамически изменяющегося пароля.
9. Взаимная проверка подлинности и другие случаи опознавания.
10. Способы разграничения доступа к компьютерным ресурсам; разграничение доступа по спискам.
11. Виды информации с точки зрения информационной безопасности.
12. Виды защищаемой информации.
13. Интересы личности (общества, государства) в информационной сфере.
14. Проблемы региональной информационной безопасности.
15. Основные нормативно-правовые акты в области информационной безопасности.
16. Исторические этапы развития системы защиты информации в России.

Практическое занятие №5

Исследование детектора электромагнитного поля ST111 (ПК1)

Порядок проведения занятия

По техническому описанию прибора и настоящему пособию изучить устройство, технические характеристики, инструкцию по эксплуатации детектора электромагнитного поля ST111 и меры безопасности при работе с ним.

Руководствуясь инструкцией по эксплуатации, подготовить прибор к работе, произвести проверку его работоспособности, настройку и юстировку.

3. Обеспечить удаление из зоны действия прибора мощных помеховых объектов.

Провести обследование помещения лаборатории. Выявить и тщательно зафиксировать все источники ЭМС, и определить их характеристики, пользуясь всеми возможностями детектора электромагнитного поля ST111.

Провести обследование контрольных образцов имитаторов ЗУ и провести их идентификацию с использованием и без использования частотомера.

Составить отчет о проделанной работе, который должен включать:

описание индикатора, принципа его действия, характеристик и основных приемы работы; данные, полученные при исследовании ЭМО в лаборатории;

результаты идентификации контрольных образцов с подробным обоснованием принято решения.

Отчет составляется персонально каждым учащимся, и полученные в нем результаты подлежат защите у преподавателя.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

Придерживаться рекомендаций, указанных в Лабораторном практикуме.

Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.

Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.

Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

Практическое занятие №6

Обнаружение сигналов линейных и сетевых закладок (ПК1)

Порядок проведения занятия

Составить самостоятельно (или получить у преподавателя) документацию на контролируемое помещение, изучить ее, определить возможные разведопасные направления и возможные виды разведки.

Изобразить план-схему исследуемого помещения.

На основании нижеприведенной методики, составить план проведения визуального осмотра помещения и выявить объекты, требующие при обследовании использования имеющихся средств видеонаблюдения и металлодетектора.

Сделать выводы по результатам проделанной работы и подготовить отчет.

Подготовка отчета

При подготовке отчета по лабораторной работе необходимо:

Придерживаться рекомендаций, указанных в Лабораторном практикуме

Выполнить требования стандартов по оформлению отчетов (ЕСКД, ЕСПД) в соответствии с образцами типовых форм отчетных документов, приведенными в приложении.

Использовать рабочие материалы, подготовленные на этапе, предшествующем выполнению лабораторной работы.

Предъявить отчет преподавателю для подтверждения факта выполнения лабораторной работы.

Контрольные вопросы (ПК-1):

1. Специальные исследования акустических и виброакустических каналов (ПК-1).
2. Специальные исследования акустоэлектрических преобразований (ПК-1).
3. Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок (ПК-1).
4. Объекты защиты информации (ПК-1).
5. Охраняемые сведения и демаскирующие признаки (ПК-1).
6. Технические каналы утечки информации (ПК-1).
7. Причины образования технических каналов утечки информации (ПК-1).
8. Прямой перехват сигналов (ПК-1).

Практическое занятие №7

Изучение положений о сертификации средств защиты информации по требованиям безопасности информации (ПК1)

Контрольные вопросы

1. Сформулируйте цели системы сертификации средств защиты информации по требованиям безопасности информации.
2. Какова организационная структура системы сертификации средств защиты информации по требованиям безопасности информации?
3. Назовите виды и схемы сертификации средств защиты информации.
4. Каковы функции ФСТЭК в области сертификации средств защиты информации?
5. Каковы функции органов сертификации средств защиты информации?
6. Каковы функции испытательных лабораторий (центров)?
7. Каковы функции заявителей?
8. Каков общий порядок проведения сертификации средств защиты информации.
9. Перечислите виды контроля в области сертификации средств защиты информации?
10. Чем определяются сроки проведения сертификационных испытаний?
11. На какой срок выдается сертификат?
12. Назовите причины приостановления или аннулирования действия сертификата.

Практическое занятие №8.

Изучение положения о сертификации средств вычислительной техники и связи (ПК1)

Контрольные вопросы

1. Какова организационная структура системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации?
2. Назовите виды и схемы сертификации средств вычислительной техники и связи по требованиям безопасности информации.
3. Каковы функции органов сертификации, испытательных лабораторий и заявителей в системе сертификации средств вычислительной техники и связи по требованиям безопасности информации?
4. Каковы особенности порядка подготовки и проведения сертификации средств вычислительной техники и связи по требованиям безопасности информации.
5. Перечислите виды контроля в области сертификации средств вычислительной техники и связи по требованиям безопасности информации.
6. На какой срок выдается сертификат?
7. Назовите причины приостановления или аннулирования действия сертификата.

Практическое занятие №9

Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации (ПК1)

Контрольные вопросы

1. Назовите цели и задачи испытаний и проверок.
2. Каковы условия проведения испытаний?
3. Перечислите общие методы испытаний.
4. В чем состоит суть испытаний объектов на соответствие организационно-техническим требованиям по защите информации?
5. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по каналам ПЭМИН?
6. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по цепям заземления и электропитания?
7. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по кабельным линиям передачи данных ЛВС и сетей связи?

8. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от НСД?
9. В чем состоит суть испытаний объектов на соответствие требованиям по защите информации от утечки по акустическим каналам?
10. В чем состоит суть проверки выполнения требований по защите информации от течи за счет встроенных технических средств?
11. В чем состоит суть проверки правильности применения криптографических средств защиты информации?
12. Каким образом осуществляется оценка результатов испытаний и оформление отчетных материалов?

1.3.2 Вопросы, выносимые на зачет по дисциплине «Технические средства и методы защиты информации»

1. Виды, источники и носители защищаемой информации (ПК-1).
2. Классификация иностранной технической разведки. Возможности видов технической разведки (ПК-1).
3. Основные этапы и процедуры добывания информации технической разведкой (ПК-1)
4. Задачи систем защиты информации (ПК-1)
5. Технические каналы утечки информации. Структура, классификация и основные характеристики (ПК-1)
6. Контроль и прослушивание телефонных каналов связи (ПК-1)
7. Технические каналы утечки речевой информации (ПК-1)
8. Акустические каналы утечки речевой информации Направленные микрофоны Виды направленных микрофонов (ПК-1).
9. Виброакустические технические каналы утечки речевой информации (ПК-1).
10. Оптико-электронный технический канал утечки речевой информации (ПК-1).
11. Технические каналы утечки видовой информации. Способы скрытого видеонаблюдения и съемки (ПК-1).
12. Технические каналы утечки видовой информации (ПК-1).
13. Способы скрытого видеонаблюдения и съемки (ПК-1).
14. Демаскирующие признаки объектов (ПК-1).
15. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра (ПК-1).
16. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра (ПК-1).
17. Демаскирующие признаки радиоэлектронных средств (ПК-1).
18. Индикаторы электромагнитного поля (ПК-1).
19. Сканирующие радиоприемники (ПК-1).
20. Анализаторы спектра, радиочастотомеры (ПК-1).
21. Многофункциональные комплекты для выявления каналов утечки информации (ПК-1).
22. Нелинейные локаторы (ПК-1).
22. Металлодетекторы (ПК-1).
23. Портативная рентгенотелевизионная установка (ПК-1).
24. Досмотровые эндоскопы (ПК-1).
25. Скрытие речевой информации в телефонных системах с использованием криптографических методов (ПК-1).
26. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах (ПК-1).
27. Методы и средства инженерной защиты и технической охраны объектов (ПК-1).
28. Категории объектов защиты (ПК-1).
29. Особенности задач охраны различных типов объектов (ПК-1).

30. Общие принципы обеспечения безопасности объектов (ПК-1).
31. Система охранно-тревожной сигнализации (ПК-1).
32. Система контроля и управления доступом (ПК-1).
33. Телевизионные системы (ПК-1).
34. Система пожарной сигнализации (ПК-1).
35. Периметровая охрана (ПК-1).
36. Аттестация объектов информатизации (ПК-1).
37. Мероприятия по выявлению и оценке свойств каналов утечки информации (ПК-1).
38. Специальные проверки (ПК-1).
39. Специальные обследования (ПК-1).
40. Специальные исследования (ПК-1).
41. Специальные исследования акустических и виброакустических каналов (ПК-1).
42. Специальные исследования акустоэлектрических преобразований (ПК-1).
43. Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок (ПК-1).
44. Объекты защиты информации (ПК-1).
45. Охраняемые сведения и демаскирующие признаки (ПК-1).
46. Технические каналы утечки информации (ПК-1).
47. Причины образования технических каналов утечки информации (ПК-1).
48. Прямой перехват сигналов (ПК-1).
49. Нежелательные излучения радиопередающих устройств систем связи и передачи информации (ПК-1).
50. Нежелательные излучения технических средств обработки информации (ПК-1).
51. Нежелательные электромагнитные связи (ПК-1).
52. Излучатели электромагнитных полей (ПК-1).
53. Утечка информации по цепям заземления (ПК-1).
54. Утечка информации по цепям питания (ПК-1).
55. Высокочастотное навязывание (ПК-1).
56. Утечка информации по акустическим каналам (ПК-1).
57. Прямой акустический канал (ПК-1).
58. Виброакустический канал (ПК-1).
59. Оптико-акустический канал (ПК-1).
60. Электроакустический канал (ПК-1).
61. Утечка информации в волоконно-оптических линиях связи (ПК-1).
62. Экранирование электромагнитных полей (ПК-1).
63. Экранирование электрических полей (ПК-1).
64. Экранирование магнитных полей (ПК-1).
65. Экранирование проводов и соединительных линий (ПК-1).
67. Материалы для экранов (ПК-1).
68. Фильтрация (ПК-1).
69. Заземление технических средств (ПК-1).

1.4 Оценочные средства для заочной формы обучения

Практическое занятие №1 Изучение законодательной и нормативной базы правового регулирования вопросов защиты информации (ПК1)

Контрольные вопросы

- Назовите основные виды конфиденциальной информации.
- Какие сведения, в соответствии с законодательством, не могут быть отнесены к информации с ограниченным доступом?
- Охарактеризуйте место правовых мер в системе комплексной защиты информации.

Назовите интересы государства в области обеспечения информационной безопасности.
 Перечислите основные нормативные акты РФ, связанные с правовой защитой информации.
 Какой закон определяет понятие «официальный документ»?
 Какой закон определяет понятие «электронный документ»?
 В каком законе приведена классификация средств защиты информации?
 Назовите основные положения Доктрины информационной безопасности РФ.
 Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?
 Дайте определение системы защиты государственной тайны и укажите ее составляющие.
 Что в соответствии с законодательством РФ представляет собой засекречивание информации.
 Перечислите основные принципы засекречивания информации.
 Что понимается под профессиональной тайной?
 Какие виды профессиональных тайн вам известны?
 Что представляет собой электронная подпись?

Практическое занятие №2. Изучение положений о сертификации средств защиты информации по требованиям безопасности информации (ПК1)

Контрольные вопросы

1. Сформулируйте цели системы сертификации средств защиты информации по требованиям безопасности информации.
 2. Какова организационная структура системы сертификации средств защиты информации по требованиям безопасности информации?
 3. Назовите виды и схемы сертификации средств защиты информации.
 4. Каковы функции ФСТЭК в области сертификации средств защиты информации?
 5. Каковы функции органов сертификации средств защиты информации?
 6. Каковы функции испытательных лабораторий (центров)?
 7. Каковы функции заявителей?
 8. Каков общий порядок проведения сертификации средств защиты информации.
 9. Перечислите виды контроля в области сертификации средств защиты информации?
 10. Чем определяются сроки проведения сертификационных испытаний?
 11. На какой срок выдается сертификат?
 12. Назовите причины приостановления или аннулирования действия сертификата.
- Вопросы 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 2.

Таблица 2 - Распределение баллов по блокам модулей дисциплины «Технические средства и методы защиты информации»

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. Рекомендуется 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 «Технические средства и методы защиты информации» 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: Технические средства и методы защиты информации		
Билет №10 1. Технические каналы утечки информации. Структура, классификация и основные характеристики. 2. Утечка информации по цепям питания. 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? 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

№ задания	Тексты заданий
	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 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.

№ задания	Тексты заданий
	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 А. % Б. мА В. МГц Г. Вт/см²
14	Установите соответствие указанным ниже понятиям своим определениям 1. IDS 2. Брандмауэр 3. Камкодер 4. 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

№ задания	Тексты заданий
	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» 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 содержании 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 по компетенции ПК-1, формируемой дисциплиной «Технические средства и методы защиты информации»

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 «Технические средства и методы защиты информации» 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.