ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
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
_____ А.Г. Жуковский
«22» 08 2019 г.

Технические средства и методы защиты информации
Б1.В.ДВ.05.01
рабочая программа дисциплины

Кафедра: Инфокоммуникационные технологии и системы связи
Направление подготовки: **11.03.02 Инфокоммуникационные технологии и системы связи**
Профиль: Защищенные системы и сети связи
Формы обучения: **очная, заочная**

Распределение часов дисциплины по семестрам (ОФ), курсам (ЗФ)

Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	6	216/7	6	216/4
Контактная работа, в том числе (по семестрам, курсам):		62		10/4
Лекции		26/7		4/4
Лабораторных работ		10/7		
Практических занятий		26/7		6/4
Семинаров				
Самостоятельная работа		154/7		206/4
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		1/4
Число экзаменов с разбивкой по семестрам (курсам)				

Программу составили:

Профессор кафедры ИТСС д.т.н., профессор Шевчук П.С.

Рецензенты:
Заведующий кафедрой ИВТ д.т.н., профессор Соколов С.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, профиля «Защищенные системы и сети связи», одобренных Учёным советом СКФ МТУСИ, Протокол № 5 от 24.12.2018, и утвержденных директором СКФ МТУСИ 15.01.2019 г.

Одобрена на заседании кафедры «Инфокоммуникационные технологии и системы связи»

Протокол от 26.08.2019 г. № 1
Зав. кафедрой _____ В.И. Юхнов

Визирование для использования в 201__/201__ уч. году

Утверждаю
Зам. директора по УВР
__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры ИТСС

Протокол от __ __ 20__ г. № _

Зав. кафедрой _____ В.И. Юхнов

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры ИТСС

Протокол от _ _____ 20__ г. № _

Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры ИТСС

Протокол от _ _____ 20__ г. № _

Зав. кафедрой _____

---

1. Цели изучения дисциплины

Целью преподавания дисциплины является формирование у обучаемых знаний в области криптографических методов защиты информации и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях и системах связи.

2. Планируемые результаты обучения

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

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ПК-10: Способен обеспечить защиту от несанкционированного доступа сооружений и средств связи сетей электросвязи
Знать (Необходимые знания):
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 (Необходимые умения):
Определять опасности и угрозы, возникающие в развитии современного информационного общества. 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 (Трудовые действия):
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.25 «Основы информационной безопасности сетей и систем»
2	Б1.О.07 «Информатика»
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.В.14 «Методы и средства защиты компьютерной информации»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 216 часа, 62 часов контактной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 3, Семестр 6					
Модуль 1 Концепция инженерно-технической защиты информации – 108 (30+78) часов					
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 1.	4	ПК-10	Л1.1 Л1.3
1.2	Лекция 2. Теоретические основы инженерно-технической защиты информации. Особенности информации как предмета защиты. 1. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. 2. Принципы защиты информации техническими средствами. 3. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.	Лек 2.	4	ПК-10	Л1.1 Л1.3
1.3	Лекция 3. Характеристика технической разведки Основные задачи и органы технической разведки.	Лек 3.	4	ПК-10	Л1.1 Л1.2 Л1.3
1.4	Практическое занятие №1 Демаскирующие признаки объектов наблюдения, сигналов и веществ. Виды демаскирующих признаков и их характеристики. Понятие о текущей и эталонной признаковой структуре.	ПЗ1.	4	ПК-10	Л1.1
1.5	Практическое занятие №2. Принципы технической разведки. Основные этапы и процессы добывания информации технической раз-	ПЗ2	4	ПК-10	Л1.1

	ведкой Шпионаж, сбор служебной информации, сканирование эфира, обработка неучтенных источников.				
1.6	Практическое занятие №3. Базовые этапы построения системы комплексной защиты вычислительных систем; анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация	ПЗ3	6	ПК-10	Л1.1
1.7	Лабораторная работа №1. Организация аттестации выделенного помещения по требованиям безопасности информации	ЛР 1	4		
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	78	ПК-10	Л1.1 Л1.3
Модуль 2 ТЕХНИЧЕСКИЙ КОНТРОЛЬ ЭФФЕКТИВНОСТИ МЕР ЗАЩИТЫ ИНФОРМАЦИИ – 98 (32+76) часов					
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.	4	ПК-10	Л1.2 Л2.1
2.2	Лабораторная работа № 2 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	ЛР2	2	ПК-10	Л1.1 Л1.3
2.3	Лабораторная работа № 3 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	ЛР3	4	ПК-10	Л1.1 Л1.3

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 компьютерным ресурсам; разграничение доступа по спискам.	Лек 5.	4	ПК-10	Л1.2 Л2.1
2.5	Лекция 6. Специальные исследования технических средств и систем на возможность утечки информации за счет побочных электромагнитных излучений и наводок	Лек 6.	4	ПК-10	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	Лек7 .	4	ПК-10	Л1.2
2.7	Практическое занятие №4. «Исследование детектора электромагнитного поля ST107».	ПЗ №4	4	ПК-10	Л1.1 Л1.3
2.8	Практическое занятие № 5 «Многофункциональный поисковый прибор ST-031 «Пиранья»».	ПЗ №5	4	ПК-10	Л1.2
2.9	Практическое занятие № 6 «Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации».	ПЗ №6	4	ПК-10	Л2.1
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	76	ПК-10	Л1.1 Л1.3
Зачет					
Итого – 216 часа					

4.2 Заочная форма обучения 5 лет (всего 216 часа, аудиторных 10 часов)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
4 Курс, 8 семестр					
Модуль 1 Концепция инженерно-технической защиты информации – 108 (4+104) часов					

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 1.	2	ПК-10	Л1.1 Л1.3
1.2	Практическое занятие №1 Демаскирующие признаки объектов наблюдения, сигналов и веществ. Виды демаскирующих признаков и их характеристики. Понятие о текущей и эталонной признаковой структуре.	ПЗ	2	ПК-10	Л1.1 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	СРС	52	ПК-10	Л1.1 Л1.3
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	СРС	52	ПК-10	Л1.1 Л1.2 Л1.3
Модуль 2 ТЕХНИЧЕСКИЙ КОНТРОЛЬ ЭФФЕКТИВНОСТИ МЕР ЗАЩИТЫ ИНФОРМАЦИИ – 98 (6+92) часов					
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	Лек 2.	2	ПК-10	Л1.2 Л2.1

	средств.				
2.2	Практическое занятие № 2 «Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации».	ПЗ2	4	ПК-10	Л1.1
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	92	ПК-10	Л1.1 Л1.2 Л2.1 Л1.1
Зачет					
Итого – 216 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	Бабаш А. В.	1. Криптографические методы защиты информации: Учебное пособие для вузов. http://znanium.com/catalog/product/1022055	М.: ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 413 с.:	Э1
Л1.2	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации : учеб. пособие / — 3-е изд., перераб. и доп.	М.: РИОР : ИНФРА-М, 2017. — 322 с.	Э2
Л1.3	А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков;	Технические средства и методы защиты информации: Учебник для вузов / Под ред. А.П. Зайцева - 7 изд., исправ. -; 60x90 1/16 - (Уч. для вузов). http://znanium.com/catalog/product/390284	М.: Гор. линия-Телеком, 2012. - 442с.	Э3
Л1.4	Скрыль С. В.	Технические средства и методы защиты информации / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. -: ISBN 978-5-9912-0084-4 - Режим доступа: http://znanium.com/catalog/product/560580	М.:Гор. линия-Телеком, 2012. - 616 с	Э4
6.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	В.А. Ворона, В.А. Тихонов.	Инженерно-техническая и пожарная защита объектов -.: ил.; 60x90 1/16. - (Обеспечение безопасности объектов). ISBN 978-5-9912-0179-7, 1000 экз. - Режим доступа: http://znanium.com/catalog/product/344187	М.: Гор. линия-Телеком, 2012. - 512 с	Э5
Л2.2	А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин.	Защита информации: Учебное пособие - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6 - Режим доступа: http://znanium.com/catalog/product/474838	М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.:	Э6
6.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**

Л3.1	Шевчук П.С.	Методические указания по проведению практических занятий по дисциплине «Основы криптографии»/ П.С. Шевчук. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2015. – 53 с.: ил.	РнД: СКФ МТУСИ, 2016	Э7
Л3.2	Шевчук П.С..	Методические указания по проведению лабораторных работ по дисциплине « Основы криптографии»/ П.С. Шевчук. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2015. – 59 с.: ил.	РнД: СКФ МТУСИ, 2016	Э8
Л3.3	Шевчук П.С.	Методические указания по выполнению курсовой работы по дисциплине «Основы криптографии»/ П.С. Шевчук. – Ростов-на -Дону: Изд-во СКФ МТУСИ, 2015. – 53 с.: ил.	РнД: СКФ МТУСИ, 2016	Э9

6.2. Электронные образовательные ресурсы	
Э1	http://znanium.com/catalog/product/1022055
Э2	http://znanium.com/catalog/product/763644
Э3	http://znanium.com/catalog/product/390284
Э4	http://znanium.com/catalog/product/560580
Э5	http://znanium.com/catalog/product/344187
Э6	http://znanium.com/catalog/product/474838
Э7	http://www.skf-mtusi.ru/?page_id=659
Э8	http://www.skf-mtusi.ru/?page_id=659
Э9	http://www.skf-mtusi.ru/?page_id=659
6.3. Программное обеспечение	
П.1	Python
П.2	Scilab
П.3	Word processor Microsoft Word or LibreOffice Writer.

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий, ауд. 305	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 Аудитория 305 МТО лабораторных работ и практических занятий	
1	Компьютерная аудитория 305.
6.3 МТО рубежных контролей, экзамена	
1	Компьютерная аудитория 305

7. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа студентов 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.

Постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятии, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально. Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта http://www.intuit.ru/ .

Для подготовки к рубежной аттестации и к экзамену целесообразно использовать

материалы сайта http://i-exam.ru/ в режимах: «Тестирование обучение» и «Тестирование-самоконтроль». Студентам, успешно решающим тестовые задания целесообразно проверить свои силы, решая олимпиадные задания по информатике по адресу http://test.i-exam.ru/training/olymp/index.html .

Студентам очной формы обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе 4.1, рекомендуется соблюдать последовательность их изучения, представленную в таблице 3.

Таблица 3 – Учебный материал, выносимый на самостоятельное изучение студентам очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 154	Неделя
	Модуль 1		
1	Демаскирующие признаки объектов Параметрические технические каналы утечки речевой информации	25	1-2
2	Акустоэлектрические каналы утечки речевой информации	25	3-4
3	Демаскирующие признаки объектов в видимом диапазоне	26	5-7
	Модуль 2		
4	Способы предотвращения утечки информации через ПЭМИН ПК	13	7-8
5	Методы средства ограничения доступа к компонентам ЭВМ	13	8-10
6	Надёжность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям	13	10-138
7	Безопасность оптоволоконных кабельных систем.	13	14
8	Заземление технических средств и подавление информационных сигналов в цепях заземления	13	15
9	Виброакустические технические каналы утечки речевой информации	13	16-17

Студенты заочной формы обучения могут осваивать вопросы для самостоятельного изучения, представленные в подразделе 4.2 в произвольной последовательности, в удобное для них время. Однако к началу сессии они должны ориентироваться в материале, представленном в строках 1.2, 1.3, 1.6, 1.8, 2.2, 2.3, 2.5-2.7, 2.9, 2.10, 3.1 таблицы подраздела 4.2.

Дополнения и изменения