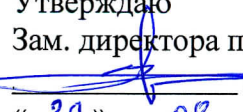


МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УВР
 А.Ф. Жуковский
« 29 » 08 2022 г.

Защита информации от утечки по техническим каналам Б1.О.34
рабочая программа дисциплины

Кафедра: Инфокоммуникационные технологии и системы связи
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем.**
Формы обучения: **очная**

**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):	3	108/7сем		
Контактная работа, в том числе (по семестрам, курсам):		54/7сем		
Лекции		22/7сем		
Лабораторных работ				
Практических занятий		32/7сем		
Семинаров				
Самостоятельная работа		54/7сем		
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам (курсам)		1/7сем		
Число экзаменов с разбивкой по семестрам (курсам)				

Программу составил:

Доцент кафедры ИТСС, к.т.н., доцент Борисов Б.П.

Рецензент:

Ведущий сотрудник ФГУП «РНИИРС, д.т.н., доцент Елисеев А.В.

Рабочая программа дисциплины

«Защита информации от утечки по техническим каналам»

разработана в соответствии с ФГОС ВО:

направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г. №1427.

Составлена на основании учебного плана

направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 25.04.2022, и утвержденного директором СКФ МТУСИ 25.04.2022 г.

Рассмотрена и одобрена на заседании кафедры

«Инфокоммуникационные технологии и системы связи»

Протокол от «29» 08 2022 г. № 1

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

«Инфокоммуникационные технологии и системы связи»

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

«Инфокоммуникационные технологии и системы связи»

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

«Инфокоммуникационные технологии и системы связи»

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

«Инфокоммуникационные технологии и системы связи»

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

Зав. кафедрой _____

1. Цели изучения дисциплины

Целью преподавания дисциплины «Защита информации от утечки по техническим каналам» является формирование у обучаемых знаний в области защиты информации, умений и навыков практического обеспечения защиты информации передаваемой по техническим каналам при использовании комплексного подхода к защите информации.

2. Планируемые результаты обучения

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

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)	
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	
Знать:	
<ul style="list-style-type: none">- технические каналы утечки информации;- методы и средствами технической защиты информации от утечки информации по техническим каналам;- демаскирующие признаки объектов;- средства выявления каналов утечки информации;- способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;- методы криптографического преобразования информации.	
Уметь:	
<ul style="list-style-type: none">- применять средства криптографической и технической защиты информации.	
Владеть:	
<ul style="list-style-type: none">- навыками анализа и оценки угроз информационной безопасности объекта защиты;- методами и средствами технической защиты информации;- навыками работы по применению средств криптографической и технической защиты информации.	

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Дисциплина «Защита информации от утечки по техническим каналам» является логическим продолжением дисциплины Б1.О.29 «Основы управления информационной безопасностью», знание которой в объеме требований образовательной программы является необходимым.
2	Успешное освоение дисциплины «Защита информации от утечки по техническим каналам» базируется также на знаниях, приобретенных из дисциплин: Б1.О.06 «Физика», Б1.О.20 «Электроника», Б1.О.28 «Сети и системы передачи информации».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Дисциплина является базовой для успешного освоения дисциплины: Б1.О.37 «Комплексное обеспечение защиты информации»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 54 аудиторных часов, 54 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 1					
Модуль 1. Технические каналы утечки информации (28+27) часов					
1.1	Лекция 1. Источники и носители защищаемой информации 1. Основные термины и определения 2. Возможности видов технической разведки 3. Задачи систем защиты информации	Лк 1	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.2	Лекция 2. Технические каналы утечки информации 1. Структура, классификация и основные характеристики 2. Технические каналы утечки информации в ТСПИ 3. Технические каналы утечки информации при передачи ее по каналам связи	Лк 2	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. Технические каналы утечки речевой информации 1. Краткие сведения по акустике 2. Характеристики речевой информации 3. Акустические каналы утечки речевой информации	Лк 3	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.4	Практическое занятие №1 Исследование акустоэлектрического канала утечки информации с использованием закладного устройства «Телефонное ухо»	Пз 1	4	ОПК-9	Л1.1 Л1.2
1.5	Практическое занятие №2 Исследование акустоэлектрического канала утечки информации в среде Multisim с использованием закладного устройства в сети электропитания	Пз 2	4	ОПК-9	
1.6	Лекция 4. Технические каналы утечки видовой информации 1. Способы скрытого видеонаблюдения и съемки 2. Характеристики оборудования	Лк 4	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.7	Лекция 5. Демаскирующие признаки объектов 1. Общая характеристика 2. Демаскирующие признаки объектов в диапазонах электромагнитного спектра	Лк 5	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.8	Лекция 6. Средства выявления каналов утечки информации 1. Общие сведения 2. Индикаторы электромагнитного поля и сканирующие радиоприемники 3. Многофункциональные комплекты для выявления каналов утечки информации	Лк 6	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.9	Практическое занятие №3 Изучение перехвата ПЭМИ, создаваемого монитором ВТ	Пз 3	4	ОПК-9	Л1.1 Л1.2
1.10	Практическое занятие №4 Проведение радио мониторинга на информационном	Пз 4	4	ОПК-9	

	объекте				
1.11	Концептуальная модель информационной безопасности. Направления обеспечения информационной безопасности. Электрические линии связи. Методы и средства инженерной защиты и технической охраны Мероприятия по выявлению и оценке свойств каналов утечки информации	СР	27	ОПК-9	Л1.1 Л1.2 Л1.3 Л2.1
Модуль 2 Скрытие и защита информации от утечки по техническим каналам (26+27)					
2.1	Лекция 7 Концепция и методы инженерно-технической защиты информации 1. Экранирование электромагнитных волн 2. Безопасность оптоволоконных кабельных систем 3. Заземление технических средств и подавление информационных сигналов в цепях заземления	Лк 7	2	ОПК-9	Л1.1 Л1.2 Л1.3
2.2	Лекция 8. Фильтрация информационных сигналов 1. Основные сведения о помехоподавляющих фильтрах 2. Выбор типа фильтра	Лк 8	2	ОПК-9	Л1.1 Л1.2 Л1.3
2.3	Практическое занятие №5 Исследование электрических параметров помехоподавляющих фильтров в среде Multisim	Пз 5		ОПК-9	Л1.1 Л1.2
2.4	Лекция 9. Устройства контроля и защиты слаботочных линий и сети 1. Особенности слаботочных линий и сетей как каналов утечки информации 2. Схемы подключения анализаторов к к электросиловым и телефонным линиям в здании 3. Устройства контроля и защиты проводных линий от утечки информации	Лк 9	2	ОПК-9	Л1.1 Л1.2 Л1.3
2.5	Практическое занятие №6 Исследование информационного скрывания речевого сообщения в тональном канале связи методом частотного скремблирования в среде Multisim	Пз 6	4	ОПК-9	Л1.1 Л1.2
2.6	Лекция 10. Скрытие и защита от утечки информации в низкочастотном диапазоне 1. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам 2. Скрытие речевой информации в телефонных системах с использованием криптографических методов	Лк 10	2	ОПК-9	Л3.1
2.7	Практическое занятие №7 Исследование электрических параметров СЗИ «Гранит-8» в среде Multisim	Пз 7	4	ОПК-9	Л1.1 Л1.2
2.8	Лекция 11. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах 1. Программно-аппаратные комплексы	Лк 11	2	ОПК-9	Л3.1

	2. Программные продукты				
2.9	Практическое занятие №8 Изучение активной защиты от перехвата ПЭМИ	Пз 8	4	ОПК-9	
2.10	Технический контроль эффективности мер защиты информации. Цели и задачи. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ. Методы испытаний ПЭВМ Методы контроля побочных электромагнитных излучений генераторов технических средств. Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации.	СР	27	ОПК-9	Л1.1 Л1.2 Л1.3 Л2.1
2.11	Зачет			ОПК-9	Л1.1 Л1.2 Л1.3 Л2.1
Итого – 108 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
ЛП.1	Зайцев А. П., Мещеряков Р.В., Шелупанов А. А.	Технические средства и методы защиты информации	М.: Гор. линия-Телеком, 2014. – 442 с.	5
ЛП.2	А.М. Голиков	Защита информации от утечки по техническим каналам	Томский Государственный университет Систем управления и радиоэлектроники, 2015	Э1
ЛП.3	Бузов Г.А.	Защита информации ограниченного доступа от утечки по техническим каналам	М.: Гор. линия-Телеком, 2015. - 586 с.: 60x90 1/16 (Обложка) ISBN 978-5-9912-0424-8	Э2
5.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
ЛП.1	Е. Б. Белов, В.П. Лось, Р. В. Мещеряков, Д. А. Шелупанов	Основы информационной безопасности	М.: Гор. линия-Телеком, 2011. - 558 с.: ил.; 60x88 1/16. - (Специальность; Учебное пособие для высших учебных заведений.	Э3
5.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/72090.html			
Э2	http://znanium.com/catalog/product/895240			
Э3	http://znanium.com/catalog/product/405159			
5.3. Ресурс информационно-телекоммуникационной сети «Интернет»				
1.	http://www.securitylab.ru			
2.	http://www.intuit.ru			

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерная аудитория с выходом в интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерная аудитория

7. Методические указания для обучающихся по освоению дисциплины

7.1 Указания по самостоятельной работе студента

Достижение целей эффективной подготовки студентов в вузах невозможно без их целеустремленной самостоятельной работы. При этом, безусловно, нельзя обойтись без живого общения и консультирования со стороны профессорско-преподавательского состава. 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. Обязательным компонентом самостоятельной работы студентов является внеаудиторный практикум по иностранному языку.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов, выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий, учебно-методических материалов, образцов техники
- содержать материал, углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Проведению самостоятельной работы (как и любого другого вида занятий) должна предшествовать подготовка как преподавателя, так и обучаемых.

Постановку задачи обучаемым на проведение самостоятельного занятия преподаватель осуществляет на одном из занятия, предшествующему данному. Он разъясняет смысл занятия и указывает, что к нему студенты должны приготовить. Задание на самостоятельную работу должно быть выдано заблаговременно с тем, чтобы слушатели имели время на информационный поиск в библиотеке необходимых пособий.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу студентов по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную базу учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков:
 - способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
 - облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
 - приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной работы по освоению учебного материала необходимо использовать в соответствии с указаниями методических разработок раздела 5 настоящей Рабочей программы.

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта <http://www.intuit.ru/>.

Таблица 7.1 – 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: 54	Неделя
Модуль 1 – 27 часа			
1	Концептуальная модель информационной безопасности.	4	1
2	Направления обеспечения информационной безопасности.	3	2
3	Электрические линии связи.	4	3
4	Оптические линии связи.	4	4
5	Доктрина информационной безопасности Российской Федерации;	4	5
6	Методы и средства инженерной защиты и технической охраны	4	6
7	Мероприятия по выявлению и оценке свойств каналов утечки информации	4	7-8
Модуль 2 – 27 часа			
8	Технический контроль эффективности мер защиты информации. Цели и задачи.	4	9
9	Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ.	4	10
10	Методы испытаний ПЭВМ	5	11-12
11	Методы контроля побочных электромагнитных излучений генераторов технических средств.	5	13-14
12	Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации.	5	15-16
13	Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация.	4	17

Дополнения и изменения в рабочей программе