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.Г. Жуковский
«_29_» _____08_____ 2022 г.

Программно-аппаратные средства защиты информации Б1.О.33
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	144/7сем		
Контактная работа, в том числе (по семестрам, курсам):		72/7сем		
Лекции		24/7сем		
Лабораторных работ		24/7сем		
Практических занятий		24/7сем		
Семинаров				
Самостоятельная работа		72/7сем		
Контроль				
Число контрольных работ (по курсам)				
Число КР (по семестрам, курсам)				
Число КП (по семестрам, курсам)				
Число зачетов с разбивкой по семестрам (курсам)				
Число экзаменов с разбивкой по семестрам (курсам)		1/7сем		

Программу составил:
Доцент кафедры ИТСС, к.т.н., доцент Решетникова И.В.

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

Рабочая программа дисциплины
«Программно-аппаратные средства защиты информации»

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. N 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 2022г. № 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 «Программно-аппаратные средства защиты информации» является формирование у обучаемых 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 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:
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.
Уметь:
Определять опасности и угрозы, возникающие в развитии современного информационного общества. Реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации.
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
ОПК-12:Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений
Знать:
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:
Применять на практике технические методы защиты информации, пользоваться стандартной терминологией и определениями. Составлять протоколы шифрования и расшифрования сообщений.
Владеть:

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	Дисциплина «Программно-аппаратные средства защиты информации» является логическим продолжением дисциплины Б1.В.05 «Разработка безопасного программного обеспечения (Проектирование защищенных информационных систем)», знание которой в объеме требований образовательной программы является необходимым.
2	Успешное освоение дисциплины «Программно-аппаратные средства защиты информации» базируется также на знаниях, приобретенных из дисциплин: Б1.В.01 «Введение в профессию», Б1.О.29 «Основы управления информационной безопасностью».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Дисциплина является базовой для успешного освоения дисциплин: Б1.О.40 «Администрирование средств защиты информации в компьютерных системах и сетях», Б2.В.03(Пд) «Производственная (преддипломная) практика»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часов, 72 аудиторных часов, 72 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 7					
Модуль 1. Концепция инженерно-технической защиты информации. (12+12+12+36) часов					
1.1	Лекция 1. Основные определения и понятия. 1. Характеристика инженерно-технической за-щиты информации как области информационной безопасности. 2. Основные проблемы инженерно-технической защиты информации. 3. Представление сил и средств защиты инфор-мации в виде системы. 4. Основные параметры системы защиты ин-формации	Л1.	4	ОПК-9	Л1.1 Л1.2 Л2.1 Л2.2
1.2	Лекция 2. Теоретические основы инженерно-технической защиты информации. Особенности ин-формации как предмета защиты.	Л2.	4	ОПК-9	Л1.1 Л1.2 Л2.1

	1. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. 2. Принципы защиты информации техни-ческими средствами. 3. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.				Л2.2
1.3	Лекция 3. Характеристика технической разведки Основные задачи и органы технической разведки. Демаскирующие признаки радиоэлектронных средств Виброакустические технические каналы утечки речевой информации	Л3.	4	ОПК-9	Л1.1 Л1.2 Л2.1 Л2.2
1.4	Практическая работа 1. Изучение законодательной и нормативной базы правового регулирования вопросов защиты информации	ПЗ1.	4	ОПК-9	Л3.1
1.5	Практическая работа 2. Изучение задач и функций органов по технической защите информации в РФ	ПЗ2	4	ОПК-9	Л3.1
1.6	Практическая работа 3. Изучение положений о государственном лицензировании деятельности в области защиты информации	ПЗ3	4	ОПК-9	Л3.1
1.7	Лабораторная работа №1. Организация аттестации выделенного помещения по требованиям безопасности информации	ЛР 1	6	ОПК-9	Л3.1
1.8	Лабораторная работа №2. Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении	ЛР 2	6	ОПК-9	Л3.1
1.9	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	СРС	36	ОПК-9	Л1.1 Л1.2 Л2.1 Л2.2
Модуль 2 Технический контроль эффективности мер защиты информации (12+12+12+36)					
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 объек-тов от утечки конфиденциальной информации по техническим каналам. 3. Физические основы образования побочных электромагнитных излучений от технических средств.	Л4	4	ОПК-13	Л1.1 Л1.2 Л2.1 Л2.2
2.2	Лекция 5. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. 1. Основные этапы доступа к ресурсам	Л5	4	ОПК-13	Л1.1 Л1.2 Л2.1

	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.				Л2.2
2.3	Лекция 6. 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 электромагнит-ных излучений генераторов технических средств	Л5	4	ОПК-13	Л1.1 Л1.2 Л2.1 Л2.2
2.4	Практическое занятие №4 Изучение положений о сертификации средств защиты информации по требованиям безопасности информации	ПЗ4	4	ОПК-13	Л3.1
2.5	Практическое занятие № 5 Изучение положения о сертификации средств вычислительной техники и связи	ПЗ5	4	ОПК-13	Л3.1
2.6	Практическое занятие № 6 Изучение типовой методики испытаний объектов информатики по требованиям безопасности информации	ПЗ6	4	ОПК-13	Л3.1
2.7	Лабораторная работа № 3 «Исследование детектора электромагнитного поля ST107».	ЛРЗ	6	ОПК-13	Л3.1
2.8	Лабораторная работа № 4 Обнаружение сигналов линейных и сетевых закладок	ЛР4	6	ОПК-13	Л3.1
2.9	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	СРС	26	ОПК-13	Л1.1 Л1.2 Л2.1 Л2.2
	Экзамен			ОПК-9, ОПК-1.3	Л1.1 Л1.2 Л2.1 Л2.2
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.	Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В.Мещеряков; Под ред. А.П.Зайцева - 7 изд., исправ. -	Москва : Гор. линия-Телеком, 2012. - 442с.; - (Уч. для вузов). ISBN 978-5-9912-0233-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/390284 . – Режим доступа: по подписке.	Э1
Л1.2	Душкин А.В., Барсуков О.М., Кравцов Е.В.	Программно-аппаратные средства обеспечения информационной безопасности:	Учебное пособие для вузов / Душкин А.В., Барсуков О.М., Кравцов Е.В. - Москва :Гор. линия-Телеком, 2016. - 248 с. (Специальность) ISBN 978-5-9912-0470-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/973806 . – Режим доступа: по подписке.	Э2
5.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1	Новиков, С.Н.	Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи / С.Н. Новиков ; под ред. В.П. Шувалова. --	Москва : Горячая линия -Телеком, 2018. - 128 с. - ISBN 978-5-9912-0410-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1040260 – Режим доступа: по подписке..	Э3
Л2.2	Новиков, В. К.	Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области ...:	Уч. пос./НовиковВ.К. - Москва : Гор. линия-Телеком, 2015.- 176с. (О)ISBN 978-5-9912-0525-2, 500 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/536932 . – Режим доступа: по	Э4

			подписке.	
5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л3.1	Решетникова И.В	ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИСЕТЕЙ И СИСТЕМ. Учебное пособие. – Ростов-на-Дону: СКФ МТУСИ, 2022. – 52 с.	РнД: СКФ МТУСИ, 2022	Э5

5.2. Электронные образовательные ресурсы	
Э1	https://znanium.com/catalog/document?pid=390284
Э2	https://znanium.com/catalog/document?id=329375
Э3	https://znanium.com/catalog/document?id=343949
Э4	https://znanium.com/catalog/document?id=67242
Э5	http://www.skf-mtusi.ru/?page_id=659

5.3. Программное обеспечение		
ЛР 1-4	MS Word – с лицензией	Программно-аппаратный комплекс "ЛЕГЕНДА"
ПЗ 1-4	MS Word – с лицензией	

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
	Мобильный комплекс RS turbo Mobile L
	Программно-аппаратный комплекс "ЛЕГЕНДА"
	Детектор электромагнитного поля ST107
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 баз) 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: 28	Неделя
Модуль 1 – 36 часов			
1	Параметрические технические каналы и акустоэлектрические каналы	6	1
2	Параметрические технические каналы утечки речевой информации	6	2
3	Акустоэлектрические каналы утечки речевой информации	6	3
4	Демаскирующие признаки объектов	6	4
5	Демаскирующие признаки объектов в видимом диапазоне	6	5-6
6	Демаскирующие признаки объектов в инфракрасном диапазоне	6	7-8
Модуль 2 – 36 часов			
7	Способы предотвращения утечки информации через ПЭМИН ПК	6	9
8	Методы средства ограничения доступа к компонентам ЭВМ	6	10
9	Надёжность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям	6	11
10	Безопасность оптоволоконных кабельных систем.	6	12-13
11	Заземление технических средств и подавление информационных сигналов в цепях заземления	6	14-15
12	Подготовка к экзамену	6	16

Дополнения и изменения в рабочей программе