МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы магистратуры
по направлению подготовки
10.04.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Техническая защита каналов передачи данных

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью дисциплины «Техническая защита каналов передачи данных» является формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения применять специальные знания для решения конкретных научно-практических задач. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

Студенты должны научиться использовать сочетание различных технологий, протоколов и телекоммуникационного оборудования.

Дисциплина предназначена для получения знаний, необходимых для решения следующих профессиональных задач:

-изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;

-математическое моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований;

-составление отчета по выполненному заданию, участие во внедрении результатов исследований и разработок;

-изучение современных телекоммуникационных технологий, применяемых при построении телекоммуникационных сетей и систем.

-Организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;

-Разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности;

-Организация работы малых групп и коллективов исполнителей, сформированных для решения конкретных профессиональных задач.

-сбор и анализ исходных данных для обеспечения информационной безопасности с помощью средств технической защиты информации;

-разработка проектной и рабочей документации, оформление отчетов по законченным проектно-конструкторским работам;

-контроль соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности .

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области;
- технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.

Уметь:

- анализировать и оценивать угрозы информационной безопасности объекта;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- пользоваться нормативными документами по защите информации.

Владеть:

- навыками работы с нормативными правовыми актами;
- методами и средствами выявления угроз безопасности автоматизированным системам;
- методами технической защиты информации;
- методами формирования требований по защите информации;
- методами расчета и инструментального контроля показателей технической защиты информации;
- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
- профессиональной терминологией.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 6 з.е. (216 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №3
Контактная работа при проведении учебных занятий (всего):	32	32
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	16	16

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 184 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Правовые и организационные основы защиты информации ограниченного доступа Содержание учебного материала: - Основные понятия в области защиты информации. - Правовые основы обеспечения информационной безопасности. - Структура государственной системы защиты информации.

№ п/п	Тематика лекционных занятий / краткое содержание
2	Понятие об источниках и каналах утечки информации; основы технической защиты информации Содержание учебного материала: - Понятие и структура технического канала утечки информации. - Классификация технических каналов утечки информации. - Технические каналы утечки информации. - Модель и способы утечки. - Основные меры защиты информации от утечки по техническим каналам.
3	Технические каналы утечки информации. КЛАССИФИКАЦИЯ КАНАЛОВ Содержание учебного материала: - Технические каналы утечки информации. - Классификация каналов.
4	Технические каналы утечки информации - Нежелательные излучения технических средств обработки информации (ТСОИ). - Утечка информации по цепям заземления. - Утечка информации по цепям электропитания. - Утечка информации в волоконно-оптических линиях связи. - Высокочастотное навязывание.
5	Способы и средства защиты каналов утечки информации Содержание учебного материала: - Характеристика способов и средств защиты каналов утечки информации. - Пассивные способы и средства защиты акустической информации в защищаемых (выделенных) помещениях.
6	Способы и средства защиты каналов утечки информации. Содержание учебного материала: - Активные способы и средства защиты акустической информации в защищаемых помещениях. - Способы и средства защиты акустической информации от ее утечки по акустоэлектрическому каналу.
7	Источники и каналы утечки информации. Основы технической защиты информации Содержание учебного материала: - Излучатели электромагнитных полей. - Антенны. - Случайные излучатели. - Электрический диполь. - Магнитный диполь. - Сравнительный анализ полей электрического и магнитного диполя. - Краткая формулировка результатов сравнительного анализа.
8	Выбор методов и средства защиты в технических каналах Содержание учебного материала: - Проблемы перехвата информации. - Оборудование систем перехвата информации. - Радиоэлектронные каналы утечки информации. - Основные показатели.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Виды информации и основные методы ее защиты При выполнении лабораторной работы студент получает навыки анализа требований к информационной безопасности
2	Виды угроз информационной безопасности Российской Федераци. При выполнении лабораторной работы студент получает знания по основным видам угроз.
3	Программно-аппаратные средства обеспечения информационной безопасности При выполнении лабораторной работы студент получает навыки по функционированию программного обеспечения для информационной безопасности.
4	Испытания программных средств защиты При выполнении лабораторной работы студент получает навыки по функционированию программного обеспечения для информационной безопасности и в частности программного обеспечения VIPNET OFFICE FIREWALL, приобретение навыков по работе с данным продуктом.
5	Защита от утечек по каналу ПЭМИН, по акустическому и виброаккустическому каналам. При выполнении лабораторной работы студент получит практический опыт получения данных по каналу ПЭМИН, по акустическому и виброаккустическому каналам.
6	Создание зашифрованного канала передачи данных При выполнении лабораторной работы студент изучит основы программы PGP для шифрования данных.
7	Анализ трафика и сбор критичной информации программами пассивного анализа При выполнении лабораторной работы студент получит навыки применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.
8	Виды защищаемой информации на предприятии При выполнении лабораторной работы студент получит навыки в разработке классификации защищаемой информации по видам.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом Подготовка к лабораторным работам
2	Подготовка к промежуточной аттестации.
3	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Голдовский Я.М., Желенков Б.В., Сафонова И.Е.Криптографическая защита компьютерной информации : метод. указ. к лаб. раб. по дисц. "Теоретические	URL: http://library.miit.ru/bookscatalog/metod/03-42764.pdf (дата обращения 03.02.2026) Текст : непосредственный.004 Г60

	основы компьютерной безопасности" для студ., обуч. по напр. "Информационная безопасность" / МИИТ. Каф. "Вычислительные системы и сети". - М. :МГУПС(МИИТ), 2013. - 36 с. : ил. - Библиогр.: с. 46. - 100 экз. - (в пер.)	
2	ГолдовскийЯ.М. ,Желенков Б.В., Цыганова Н.А. Маршрутизация в компьютерных сетях : [Электронный ресурс] : учеб. пособие по дисц. "Сети и телекоммуникации" для студ. напр. "Информатика и вычислительная техника" ; МИИТ. Каф. "Вычислительные системы и сети". - М. : РУТ(МИИТ), 2017. - 114 с. - 100 экз.	URL: http://library.miit.ru/bookscatalog/metod/DC-407.pdf (дата обращения 03.02.2026)Текст : непосредственный.004 Г60
3	Шифрование с открытым ключом: метод. указ. к лаб. раб. по дисц. Информационная безопасность и защита информации для студ. спец. Автоматизированные системы обработки информации и управления, Информационные системы и технологии / Э.И. Костюковская, А.М. Удалов; МИИТ. Каф. Автоматизированные системы управления. - М.: МИИТ, 2008. - 28 с. : ил. - Библиогр.: с. 26.	URL: http://library.miit.ru/bookscatalog/metod/DC-407.pdf (дата обращения 03.02.2026)Текст : непосредственный.004 Г60
4	Желенков Борис Владимирович. Канальный уровень модели OSI : метод. указ. к лаб. раб. по дисц. "Сети ЭВМ и телекоммуникации" для студ. 4 курса спец. "Вычислительные машины, комплексы, системы и сети", напр. "Информатика и вычислительная техника" / Б.В. Желенков ; МИИТ. Каф. "Вычислительные системы и сети". - М. : МИИТ, 2011. - 50 с. : ил. с. 49. - 100 экз. - (в пер.) : 42.60 р. - Текст : непосредственный.	URL: http://library.miit.ru/bookscatalog/metod/03-41547.pdf (miit.ru).(дата обращения 03.02.2026).Полочный шифр 004-Ж51
5	Защищенные беспроводные и мобильные коммуникации: Учеб. пособие для студ., обуч. по магистерской программе Безопасность и защита инф-ции напр. Информатика и выч. тех.; МИИТ. Центр компетентности Защита и безопасность информации / В.П. Соловьев, Д.В.	URL: http://library.miit.ru/miitpublishing/04-35015.pdf (miit.ru). (дата обращения 03.02.2026) Текст : непосредственный.681.3

	Иванов, Н.Н. Пуцко; Ред. В.П. Соловьев. - М.: МИИТ, 2007. - 121 с. : ил. - Библиогр.: с. 120 (7 назв.).	

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

- База данных стандартов: https://www.gost.ru/portal/gost/home/standarts
- База данных документов ФСТЭК: https://fstec.ru/dokumenty-filter

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой. Компьютер должен быть обеспечен лицензионными программными продуктами:

Microsoft Windows

Microsoft Office

Для проведения лабораторных работ необходимы персональные компьютеры с рабочими местами. Компьютер должен быть обеспечен лицензионными программными продуктами:

Microsoft Windows

Microsoft Office

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Для проведения аудиторных занятий и самостоятельной работы требуются:

-Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET

-Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

-Компьютерный класс с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET

Для проведения лабораторных работ:

-компьютерный класс; кондиционер; персональные компьютеры.

9. Форма промежуточной аттестации:

Зачет в 3 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, к.н. кафедры
«Вычислительные системы, сети и
информационная безопасность» Я.М. Голдовский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова