МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
специализированного высшего образования
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.

Основными задачами дисциплины являются:

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

ПК-6 - Способность выбирать и применять технические средства защиты информации и обеспечивать их функционирование.

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	Основы передачи данных: понятие физической среды и классификация линий связи — Определение физической среды передачи данных. — Основные типы сред передачи: проводные (кабельные), беспроводные (радио-, оптические), смешанные. — Классификация линий связи по физической природе (электрические, оптические, акустические и др.), назначению и характеру эксплуатации. — Ключевые параметры линий связи: пропускная способность, затухание, помехозащищённость, дальность передачи.
2	Проводные линии связи: виды, характеристики и особенности защиты — Воздушные линии, симметричные и коаксиальные кабели: сравнительный анализ. — Вторичные параметры линий: волновое сопротивление, коэффициент затухания, коэффициент распространения. — Уязвимости проводных линий для несанкционированного доступа. — Методы защиты: экранирование, заземление, контроль целостности линий.
3	Волоконно?оптические линии связи (ВОЛС): принципы работы и защита от утечек — Физические основы передачи данных по оптическим волокнам. — Преимущества ВОЛС: высокая скорость, защищённость, устойчивость к помехам. — Каналы утечки через оптические линии: боковое излучение, несанкционированное подключение. — Методы обнаружения и предотвращения утечек: мониторинг рефлектограммами (OTDR), криптографическая защита.
4	Беспроводные каналы связи: классификация и риски утечки информации — Типы беспроводных каналов: радиочастотные (Wi?Fi, Bluetooth, сотовая связь), спутниковые,

№ п/п	Тематика лекционных занятий / краткое содержание
	инфракрасные, лазерные. — Особенности распространения сигналов в различных диапазонах (УКВ, СВЧ и др.). — Потенциальные каналы утечки: перехват радиосигналов, атаки типа MITM (Man?in?the?Middle). — Способы защиты: шифрование (WPA3, VPN), контроль зоны покрытия, использование направленных антенн.
5	Технические каналы утечки информации: классификация и механизмы возникновения — Понятие технического канала утечки информации (ТКУИ). — Классификация ТКУИ по физической природе: электромагнитные, акустические, вибрационные, оптические. — Источники и носители информации в каждом типе канала. — Факторы, влияющие на вероятность утечки: мощность сигнала, расстояние, среда распространения.
6	Электромагнитные каналы утечки: анализ и методы противодействия — Источники побочных электромагнитных излучений (ПЭМИН): кабели, оргтехника, сетевое оборудование. — Методы измерения уровня излучений: спектроанализаторы, селективные вольтметры. — Способы снижения риска утечки: экранирование помещений, фильтрация сигналов, использование защищённых компонентов. — Нормативные требования к уровню ПЭМИН (ГОСТ, ФСТЭК).
7	Акустические и виброакустические каналы утечки: особенности и защита — Механизмы возникновения акустических каналов: прямое прослушивание, съём информации через строительные конструкции. — Технические средства съёма: направленные микрофоны, лазерные системы, акселерометры. — Методы защиты: звукоизоляция помещений, генераторы акустических помех, виброзащита коммуникаций. — Практические примеры защиты переговорных комнат и режимных зон.
8	Комплексный подход к защите каналов передачи данных — Интеграция технических и организационных мер защиты. — Этапы оценки защищённости объекта: аудит линий связи, моделирование угроз, тестирование на проникновение. — Использование систем мониторинга и IDS/IPS для выявления аномалий в трафике. — Нормативная база РФ в области защиты информации (ФЗ?149, ФЗ?152, приказы ФСТЭК).

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Предварительная оценка и классификация технических каналов утечки информации. При выполнении лабораторной работы студент получает навыки определять для заданного преподавателем канала передачи данных основные каналы утечки информации, классифицировать их по физическим характеристикам и оценивать потенциальную опасность.

№ п/п	Наименование лабораторных работ / краткое содержание
2	Анализ электромагнитных каналов утечки информации в офисных помещениях. Студент научится выявлять источники побочных электромагнитных излучений (ПЭМИН), измерять их уровень с помощью специализированного оборудования, строить карты электромагнитной обстановки и предлагать меры по снижению рисков утечки данных через электромагнитные каналы.
3	Исследование акустических каналов утечки информации и методов их блокирования. В ходе работы студент освоит методы обнаружения акустических каналов (включая виброакустические), научится использовать шумомеры и генераторы акустических помех, оценит эффективность звукоизоляции и активного зашумления для защиты речевой информации.
4	Оценка защищённости проводных линий передачи данных от несанкционированного подключения. Студент приобретёт навыки выявления потенциальных точек несанкционированного подключения к кабельным линиям, освоит методы контроля целостности линий, научится использовать рефлектометры и другие приборы для обнаружения несанкционированных отводов, а также оценит эффективность экранированных кабелей.
5	Практическое исследование методов защиты беспроводных сетей Wi?Fi от перехвата данных. Работа направлена на освоение навыков анализа беспроводных сетей с помощью анализаторов спектра, выявления уязвимостей в настройках шифрования (WEP, WPA, WPA2, WPA3), тестирования стойкости паролей и настройки механизмов аутентификации. Студент также оценит эффективность изоляции гостевых сетей и сегментации трафика.
6	Моделирование атак на волоконно?оптические линии связи и методы их обнаружения. Студент изучит физические принципы утечки информации через оптические каналы, научится моделировать атаки типа «подключение к волокну» и «анализ боковых излучений», освоит использование оптических рефлектометров (OTDR) для выявления несанкционированных подключений и оценит эффективность криптографической защиты трафика.
7	Тестирование эффективности экранирующих конструкций и материалов для защиты помещений. В рамках лабораторной работы студент проведёт измерения уровня электромагнитного излучения до и после установки экранирующих материалов (металлических сеток, специальных красок, штор), оценит коэффициент экранирования на различных частотах и подберёт оптимальные решения для конкретных условий эксплуатации.
8	Комплексная оценка защищённости канала передачи данных с использованием средств мониторинга и IDS/IPS. Студент освоит работу с системами обнаружения и предотвращения вторжений (IDS/IPS), научится настраивать правила мониторинга сетевого трафика, анализировать логи событий безопасности, выявлять признаки сканирования, атак типа MITM (Man?in?the?Middle) и DDoS, а также формировать рекомендации по настройке межсетевых экранов и политик безопасности.

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 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.)	URL: http://library.miit.ru/bookscatalog/metod/03-42764.pdf (дата обращения 03.02.2026) Текст : непосредственный.004 Г60
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. Иванов, Н.Н. Пуцко; Ред. В.П. Соловьев. - М.: МИИТ, 2007. - 121 с. : ил. - Библиогр.: с. 120 (7 назв.).	URL: http://library.miit.ru/miitpublishing/04-35015.pdf (miit.ru). (дата обращения 03.02.2026) Текст : непосредственный.681.3

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 и
квантовые коммуникации» Я.М. Голдовский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова