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 бакалавриата
по направлению подготовки
11.03.02 Инфокоммуникационные технологии и системы связи,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информации в мобильных системах

Направление подготовки: 11.03.02 Инфокоммуникационные технологии и системы связи

Направленность (профиль): Системы мобильной связи и сетевые технологии на транспорте

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения дисциплины «Защита информации в мобильных системах» являются

- приобретение знаний и умений в соответствии с образовательным стандартом РУТ (МИИТ);

- формирование умений работать с организационно-правовой документацией по защите информации, оценивать угрозы объектам защиты информации, выстраивать комплексную систему защиты информации на предприятии, выявлять и расследовать инциденты информационной безопасности;

- получение знаний и выработка компетенций в области определения политики информационной безопасности мобильных систем;

- освоение базовых приемов решения практических задач по темам дисциплины.

Задачи изучения дисциплины:

- получение необходимых знаний по общим подходам к построению систем мобильной связи и сетей передачи информации, методам решения проблем электромагнитной совместимости, а также распределения нагрузки в области инфокоммуникаций.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-3 - Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности.

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

Знать:

- основные причины и особенности современных информационных и мобильных угроз;

-основные методы и средства защиты информации в информационных системах;

-правовые основы обеспечения защиты информации в мобильных системах;

-требования к системе организации информационной безопасности мобильных систем.

Уметь:

- самостоятельно анализировать и оценивать угрозы информационной безопасности;
- классифицировать угрозы информационной безопасности с целью создания эффективной системы защиты от мобильных угроз;
- правильно применять современные средства информационной безопасности отечественных и зарубежных производителей.

Владеть:

- методами и примерами обеспечения информационной безопасности мобильных систем.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 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 №6
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	32	32

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 60 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	СИСТЕМЫ МОБИЛЬНОЙ СВЯЗИ Рассматриваемые вопросы: - системы подвижной радиосвязи; - системы фиксированной радиосвязи; - системы персонального радиовызова; - транкинговые системы.
2	МЕТОДИКИ ПРОГНОЗА ЗОН ПОКРЫТИЯ СЕТЕЙ Рассматриваемые вопросы: - статистическая модель напряженности поля; - детерминированная модель напряженности поля; - дифракционная аналитическая модель напряженности поля сигнала.
3	ЧАСТОТНО-ТЕРРИТОРИАЛЬНОЕ ПЛАНИРОВАНИЕ Рассматриваемые вопросы: - методы и алгоритмы частотно-территориального планирования; - особенности планирования различных сетей.
4	РЕКОМЕНДАЦИИ ПО ИСПОЛЬЛЗОВАНИЮ МЕТОДИК ЧАСТОТНО-ТЕРРИТОРИАЛНОГО ПЛАНИРОВАНИЯ Рассматриваемые вопросы: - сети стандарта GSM-1800, GSM-900, NMT-450, TETRA.
5	ПРОСТРАНСТВЕННОЕ И ЧАСТОТНО-ВРЕМЕННОЕ ПЛАНИРОВАНИЕ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ Рассматриваемые вопросы: - реализация пространственного планирования; - сотовый принцип построения систем мобильной связи; - особенности построения систем мобильной связи с макросотовой структурой; - особенности построения систем мобильной связи с микросотовой структурой; - реализация частотно-временного планирования; - применение многостанционного доступа; - частотные планы систем мобильной связи.
6	ПРОБЛЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ. АНАЛИЗ ОСНОВНЫХ УГРОЗ Рассматриваемые вопросы: - общие положения; - угрозы информационной безопасности; - классификация угроз информационной безопасности ТКС; - виды представления информации в ТКС и возможные каналы ее утечки; - модель вероятного нарушителя; - цели и возможные сценарии несанкционированного доступа к

№ п/п	Тематика лекционных занятий / краткое содержание
	ТКС; - обеспечение защиты информации в телекоммуникационных системах.
7	ПРАКТИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ СТАНДАРТА GSM Рассматриваемые вопросы: - особенности построения и функционирования систем мобильной связи стандарта GSM; - общая характеристика стандарта GSM; - структурная схема и состав оборудования систем связи; - сетевые интерфейсы и радиоинтерфейсы; - структура служб и передача данных; - терминальное оборудование и адаптеры мобильной станции; - структура TDMA-кадров и формирование сигналов; - организация физических и логических каналов; - модуляция радиосигнала; - особенности защиты информации от ошибок в системах мобильной связи стандарта GSM; - сверточное кодирование и перемежение в полноскоростном речевом канале; - кодирование и перемежение в каналах управления; - особенности обеспечения безопасности информации в системах мобильной связи стандарта GSM; - общая характеристика безопасности связи; - механизмы аутентификации; - конфиденциальность передачи данных; - обеспечение конфиденциальности абонента; - модуль подлинности абонента.
8	ПРАКТИЧЕСКИЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ СТАНДАРТА IS-95 Рассматриваемые вопросы: - особенности построения и функционирования систем мобильной связи с кодовым разделением; каналов стандарта IS-95; - общая характеристика систем мобильной связи CDMA; - особенности регистрации мобильных станций в системах CDMA; - особенности прохождения вызовов в системах CDMA; - особенности «эстафетной передачи» в системах CDMA; - особенности регулирования мощности в системах CDMA; - особенности защиты информации в системах мобильной связи стандарта IS-95; - аспекты безопасности в стандарте IS-95; - особенности защиты информации в прямом канале связи; - особенности защиты информации в обратном канале связи.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Цели и задачи информационной безопасности. Рассматриваемые вопросы:

№ п/п	Тематика практических занятий/краткое содержание
	- цели и задачи информационной безопасности; - место информационной безопасности в национальной безопасности РФ.
2	Основы проведения аудита информационной безопасности. Рассматриваемые вопросы: - пассивный и активный поиск информации.
3	Система защиты информации в организации. Рассматриваемые вопросы: - построение системы защиты информации в организации.
4	Методы управления доступом Рассматриваемые вопросы: - методы управления доступом в компьютерной системе.
5	Управление рисками на различных стадиях жизненного цикла информационной системы. Рассматриваемые вопросы: - трехмерная модель “куб безопасности”.
6	Анализ информационных рисков, угроз и уязвимостей системы. Рассматриваемые вопросы: - оценка рисков по двум факторам; - оценка рисков по трем факторам.
7	Анализ рисков информационной безопасности. Рассматриваемые вопросы: - программное обеспечение для анализа рисков информационной безопасности.
8	Оценка вероятности угроз от мобильных устройств по отдельным категориям Рассматриваемые вопросы: - оценка вероятности угроз от мобильных устройств по отдельным категориям: потеря или кража мобильного устройства; перехват данных, которые передаются по сетям Wi-Fi или 3G; захват данных через соединения Bluetooth; мобильные вирусы (включая вирусы электронной почты).
9	Политики безопасного использования мобильных устройств в различных областях Рассматриваемые вопросы: - защита паролем; - защита карт памяти; - шифрование файлов; - резервное копирование; - ограничения использования аппаратного и программного обеспечения.
10	Стандарты симметричного и асимметричного шифрования. Рассматриваемые вопросы: - электронная подпись; - система Gpg4Win; - изучение инфраструктуры открытых ключей (PKI). Стеганография.
11	«Консьюмеризация». Рассматриваемые вопросы: - обеспечение контроля за хаотичным подключением мобильных устройств к корпоративным ресурсам; - распределение мобильных устройств и привязка к пользователям; - обеспечение единообразия корпоративного программного обеспечения; - распространение корпоративных настроек и политик безопасности на устройства.
12	Защита данных в случае кражи. Рассматриваемые вопросы: - контроль утечки данных мобильных устройств;

№ п/п	Тематика практических занятий/краткое содержание
	- защита мобильных устройств от вредоносных программ; - защита мобильных устройств от фишинга; - защита мобильных устройств от телефонного спама; - единый инструментарий для разных мобильных платформ (iOS, Android, Symbian, Windows Mobile, BlackBerry, Windows Phone) и их защиты с помощью одной системы; - антивирусная защита мобильных устройств.
13	Инструменты для сканирования уязвимостей Рассматриваемые вопросы: - инструменты для сканирования уязвимостей веб-приложений, серверов и компьютеров.
14	Обеспечение безопасности Рассматриваемые вопросы: - обеспечение безопасности в Linux-системе.
15	Настройка идентификации и аутентификации Рассматриваемые вопросы: - настройка идентификации и аутентификации в Astra Linux.
16	Реверс-инжиниринг программного кода Рассматриваемые вопросы: - применение реверс-инжиниринга программного кода.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к практическим занятиям
2	Работа с лекционным материалом, литературой, самостоятельное изучение разделов (тем) дисциплины(модуля
3	Выполнение курсового проекта.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых проектов

Курсовой проект по дисциплине "Защита информации в мобильных системах" - это комплексная самостоятельная работа обучающегося. Темой курсового проекта является "Шифрование информации различными алгоритмами". Исходные данные выбираются согласно варианту:

Вариант 0

Исходное сообщение: Основными_каналами_телеграфной_связи_на_железнодорожном_транспорте_являются _каналы_частотного_телеграфирования

p=13 и g=3

Вариант 1

Исходное сообщение: Характеристика_узловой_системы_телеграфной_сети_железнодорожного_транспорта_и_классификация_видов_телеграфной_связи

p=11 и g=3

Вариант 2

Исходное сообщение: Скелетная_схема_организации_телеграфной_связи_управления_железной_дороги_составляется_по_атласу_железных дорог

p=13 и g=3

Вариант 3

Исходное сообщение: Анализ_систем_организации_телеграфной_связи_на_железнодорожном_транспорте_и_выбор_телеграфных_станций

p=19 и g=7

Вариант 4

Исходное сообщение: Выбор_каналообразующей_аппаратуры_производится_с_учетом_обеспечения_высокой_устойчивости_действия_телеграфной_связи

p=19 и g=5

Вариант 5

Исходное сообщение: Расчет_нагрузки_каналов_телеграфной_станции_производится_для_часа_наибольшего_значения_потоков_телеграфных_сообщений

p=7 и g=3

Вариант 6

Исходное сообщение: Техническое_задание_на_определение_среднесуточной_нагрузки_проектируемой_станции_абонентского_ телеграфирования

p=13 и g=7

Вариант 7

Исходное сообщение: Точный_расчет_и_выбор_оптимального_варианта_организации_телеграфной_связи_и_размещения _оборудования

p=17 и g=11

Вариант 8

Исходное сообщение: Характеристика_и_принципы_организации_телеграфной_связи_по_системе_ абонентского_телеграфирования_и_общего_пользования

p=19 и g=13

Вариант 9

Исходное сообщение: Расчет_телеграфной_нагрузки_для_определения_числа_потребных_каналов_и_необходимого_количества_оборудования_для станции

p=17 и g=7

Ключи шифрования:

K1=Фамилия

K2=ddmm (день и месяц рождения, 4 цифры, цифру 0, если она есть в дате, заменить на 9)

Число M:

Если последняя цифра номера зачетной книжки – ...

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

№ п/п	Библиографическое описание	Место доступа
1	Основы информационной безопасности ISBN 978-5-8114-6738-9 324 с. Нестеров С. А. Учебник Издательство "Лань" , 2021	https://e.lanbook.com/book/165837
2	Системы и сети мобильной связи ISBN 978-5-7782-3833-6 96 с. Райфельд М. А., Спектор А. А. Учебное пособие Новосибирский государственный технический университет , 2019	https://e.lanbook.com/book/152245

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

Информационный портал Научная электронная библиотека eLIBRARY.RU (www.elibrary.ru);

Единая коллекция цифровых образовательных ресурсов (http://window, edu.ru);

Научно-техническая библиотека РУТ (МИИТ) (http/library.miit.ru);

Поисковые системы «Яндекс», «Google» для доступа к тематическим информационным ресурсам;

Электронно-библиотечная система издательства «Лань» – http://e.lanbook.com/;

Электронно-библиотечная система ibooks.ru – http://ibooks.ru/;

Электронно-библиотечная система «УМЦ» – http://www.umczdt.ru/;

Электронно-библиотечная система «Intermedia» – http://www .intermediapublishing.ru/;

Электронно-библиотечная система «BOOK.ru» – http://www.book.ru/;

Электронно-библиотечная система «ZNANIUM.COM» – http://www.znanium.com/

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

Программное обеспечение для выполнения практических заданий включает в себя программные продукты общего применения: операционную систему Windows, Microsoft Office 2003 и выше, Браузер Internet Explorer 8.0 и выше с установленным Adobe Flash Player версии 10.3 и выше, Adobe Acrobat.

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

Для проведения аудиторных занятий и самостоятельной работы требуется:

1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET;

2. Специализированная лекционная аудитория с мультимедиа аппаратурой интерактивной доской.

3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET

Для проведения практических занятий требуется:

компьютерный класс; компьютеры.

Технические требования к оборудованию для осуществления учебного процесса с использованием дистанционных образовательных технологий:

колонки, наушники или встроенный динамик (для участия в аудиоконференции); микрофон или гарнитура (для участия в аудиоконференции); веб-камеры (для участия в видеоконференции);

для ведущего: компьютер с процессором Intel Core 2 Duo от 2 ГГц (или аналог) и выше, от 2 Гб свободной оперативной памяти.

9. Форма промежуточной аттестации:

Зачет в 6 семестре.
Курсовой проект в 6 семестре.

10. Оценочные материалы.

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

Авторы:

директор академии	А.В. Горелик

Согласовано:

Директор	Б.В. Игольников
Руководитель образовательной программы	А.С. Веселова
Председатель учебно-методической комиссии	Д.В. Паринов