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)

Основы информационной безопасности

Направление подготовки: 11.03.02 Инфокоммуникационные технологии и системы связи

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

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 170737
Подписал: заместитель директора академии Паринов Денис Владимирович
Дата: 26.12.2023

1. Общие сведения о дисциплине (модуле).

Целью освоения дисциплины «Основы информационной безопасности» является формирование у обучающихся компетенций в соответствии с требованиями самостоятельно утвержденного образовательного стандарта высшего образования (СУОС) по направлению подготовки балакавриата «Инфокоммуникационные технологии и системы связи».

Задачами освоения дисциплины «Основы информационной безопасности» являются:

- 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;
- приобретение навыков расследования компьютерных преступлений.
- освоение базовых приемов решения практических задач по темам дисциплины.

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 организационно-правовые положения в области защиты информации, основные методы и средства защиты информации, основы управления инцидентами информационной безопасности;

Уметь:

производить обоснование и оценку эффективности применения различных методов и средств защиты информации, обеспечения информационной безопасности при передаче и хранении информации;

Владеть:

методами управления инцидентами информационной безопасности; методами и примерами использования математического аппарата для решения задач обеспечения информационной безопасности.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 2 з.е. (72 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	Сем. №6
Контактная работа при проведении учебных занятий (всего):	32	32
В том числе:		
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 40 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.

Не предусмотрено учебным планом

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Оценка уязвимостей информационных технологий Оценка уязвимостей информационных технологий с использованием единой системы определения величины уязвимостей CVSS V2 и V3.
2	Основы проведения аудита информационной безопасности. Основы проведения аудита информационной безопасности. Пассивный поиск информации
3	Активный поиск информации. Активный поиск информации. Построение частной модели угроз безопасности информации и модели нарушителя в информационной системе организации.
4	Управление доступом в компьютероной системе Методы управления доступом в компьютерной системе.
5	Парольная аутентификация. Оценка стойкости парольной защиты. Генераторы паролей.
6	Простые шифровальные системы. Построение и применение простых шифровальных систем.
7	Атака на зашифрованный текст Атака на зашифрованный текст с использованием анализа частотности текста.
8	Симметричное и асимметричное шифрование. Стандарты симметричного и асимметричного шифрования.
9	Электронная подпись. Электронная подпись. Система Gpg4Win. Изучение инфраструктуры открытых ключей (PKI).
10	Стеганография. Применение стенографии
11	Анализ кадров Ethernet. Использование программы Wireshark для анализа кадров Ethernet.
12	DLP-система DLP-система STAFFCOP ENTERPRISE.
13	Сканирование уязвимостей веб-приложений, серверов и компьютеров. Инструменты для сканирования уязвимостей веб-приложений, серверов и компьютеров.
14	Практика тестирования безопасности Практика тестирования безопасности с использованием Web Security Dojo.
15	Обеспечение безопасности Обеспечение безопасности в Linux-системе.
16	Настройка идентификации и аутентификации Настройка идентификации и аутентификации в Astra Linux
17	Реверс-инжиниринг программного кода 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 "Основы информационной безопасности" - 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 – простое число, то М=№ последней цифры номера зачетной книжки{mod 11} (если М=0, то М=9, если М=1, то М=8), иначе М=№ последней цифры 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	Информационная безопасность. Практические аспекты: учебник для вузов ISBN 978-5-4383-0205-6 240 с. Сафиуллина Л. Х., Касимова А. Р., Рябов Я. С., Садыков А. М., Богомолов В. А. Учебник ИЦ Интермедия , 2021	https://e.lanbook.com/book/161340

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 сети INTERNET.
2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.
3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сети INTERNET
4. Для проведения практических занятий: компьютерный класс; компьютеры с минимальными требованиями.

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:

заведующий кафедрой, профессор,
д.н. кафедры «Системы управления
транспортной инфраструктурой» А.В. Горелик

Согласовано:

Заместитель директора академии Д.В. Паринов

Председатель учебно-методической
комиссии Д.В. Паринов