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 специалитета
по специальности
23.05.05 Системы обеспечения движения поездов,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность на железнодорожном транспорте

Специальность: 23.05.05 Системы обеспечения движения поездов

Специализация: Радиотехнические системы на железнодорожном транспорте

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Безопасность систем передачи данных на железнодорожном транспорте» является формирование у обучающихся компетенций в области:

принципов работы современных информационных технологий и использования их для решения задач профессиональной деятельности;

способности применять в практической деятельности пакеты прикладных программ для моделирования радиотехнических систем и беспроводных сетей связи.

Задачами дисциплины являются:

- приобретение учащимися знаний о системах передачи данных на железнодорожном транспорте;

- приобретение учащимися навыков применять в практической деятельности пакеты прикладных программ для безопасной передачи данных.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-2 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;

ПК-15 - Способен применять в практической деятельности пакеты прикладных программ для моделирования радиотехнических систем и беспроводных сетей связи.

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

Знать:

-принципы работы современных информационных технологий;

- пакеты прикладных программ для моделирования радиотехнических систем и беспроводных сетей связи.

Уметь:

- использовать современные информационные технологии;

- применять в практической деятельности пакеты прикладных программ для моделирования радиотехнических систем и беспроводных сетей связи.

Владеть:

-основными методами передачи данных в современных информационных технологиях;

-основными прикладными программами для моделирования радиотехнических систем и беспроводных сетей связи.

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 №9
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
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 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	Введение. Рассматриваемые вопросы: 1.1 Основные понятия и определения сетевых технологий (понятие сети, модель OSI, адресация в сетях и т.п.) 1.2. Краткая история появления и развития сетевых технологий.
2	Угрозы безопасности информации при ее передач. Рассматриваемые вопросы: 2.1 Понятие угроз безопасности информации. 2.2. Классификация угроз. 2.3. Модель нарушителя.
3	Профили защиты и системы обеспечения информационной безопасности корпоративных и телекоммуникационных сетей. Рассматриваемые вопросы: 3.1 Профиль защиты сети передачи данных ОАО “РЖД”. 3.2 Система обеспечения информационной безопасности единой магистральной цифровой сети связи. 3.3. Средства защиты информации в беспроводных широкополосных сетях доступа.
4	Профили защиты и системы обеспечения информационной безопасности автоматизированных и информационно-управляющих систем. Рассматриваемые вопросы: 4.1 Автоматизированная система ЭТРАН.
5	Архитектура открытых ключей. Рассматриваемые вопросы: 5.1 Понятие открытых ключей. 5.2.Инфраструктура открытых ключей.
6	Туннелирование и криптографические протоколы как технология защищенных виртуальных сетей. Рассматриваемые вопросы: 6.1. Понятие криптографических протоколов. 6.2. Туннелирование.
7	Способы предотвращения перехвата информации. Рассматриваемые вопросы: 7.1 Способы предотвращения перехвата информации через побочные электромагнитные излучения и наводки. 7.2. Способы предотвращения съема информации через излучения волоконно-оптических линий связи.
8	Архитектура и средства защиты информации в корпоративных вычислительных системах на основе мейнфреймов z-series. Рассматриваемые вопросы: 8.1 Архитектурные особенности z-series и операционных систем z/OS, z/VM 8.2. Средства обеспечения целостности и защиты данных. 8.3. Средства управления доступом. 8.4. Общая архитектура и средства криптографии. 8.5. Защита TCP/IP.
9	Системы обеспечения информационной безопасности корпоративного уровня. Рассматриваемые вопросы: 9.1. Системы управления доступом. 9.2. Защита электронной почты.

№ п/п	Тематика лекционных занятий / краткое содержание
10	Типовые программно-аппаратные средства защиты информации на железной дороге. Рассматриваемые вопросы: 10.1. Средства аудита. 10.2.Сканеры уязвимости. 10.3. Сетевые средства защиты информации.
11	Управление инцидентами информационной безопасности. Рассматриваемые вопросы: 11.1. Алгоритм выявление инцидентов информационной безопасности. 11.2. Классификация инцидентов информационной безопасности. 11.3 Меры реагирования.
12	Оценка значимости информационных ресурсов и степени ее защищенности. Рассматриваемые вопросы: 12.1. Понятие и оценка значимости информационных ресурсов. 12.2. Оценка степени защищенности информационных ресурсов.
13	Аудит информационной безопасности. Рассматриваемые вопросы: 13.1 Понятие аудита информационной безопасности. 13.2. Процесс проведение аудита. 13.3 Стандарты аудита.
14	Системы антивирусной защиты. Рассматриваемые вопросы: 14.1 Понятие и устройство антивируса. 14.2. Эвристический и сигнатурный метод анализа.
15	Система оценки защищенности тедекоммуникационных систем ОАО “РЖД”. Рассматриваемые вопросы: 15.1 Обзор регламентов ФСТЭК,ФСБ РФ и др. 15.2 Методология оценки защищенности.
16	Система мониторинга состояния информационной безопасности. Рассматриваемые вопросы: 16.1 Программно-аппаратный комплекс Cisco Mars.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Введение в сетевые технологии. Рассматриваемые вопросы: Модель OSI. Уровни модели OSI.
2	Профили защиты и системы обеспечения информационной безопасности корпоративных и телекоммуникационных сетей. Рассматриваемые вопросы: Система обеспечения информационной безопасности в ОАО “РЖД”. Описание профилей защиты.
3	Профили защиты и системы обеспечения информационной безопасности автоматизированных и информационно-управляющих систем.

№ п/п	Тематика практических занятий/краткое содержание
	Рассматриваемые вопросы: ЭТРАН. Специфика обеспечения информационной безопасности ЭТРАН.
4	Методы криптографической защиты информации. Рассматриваемые вопросы: Туннелирование и криптографические протоколы как технология защищенных виртуальных сетей. VPN, протоколы IPSec, SSL.
5	Способы предотвращения перехвата информации. Рассматриваемые вопросы: Способы перехвата. Классификация угроз.
6	Архитектура и средства защиты информации в корпоративных вычислительных системах на основе мейнфреймов z-series. Рассматриваемые вопросы: Архитектура и средства защиты информации в корпоративных вычислительных системах.
7	Системы обеспечения информационной безопасности корпоративного уровня. Рассматриваемые вопросы: Разработка и построение системы обеспечения информационной безопасности корпоративного уровня. Система управления доступом, антивирусной защиты, защиты электронной почты.
8	Типовые программно-аппаратные средства защиты информации на железной дороге. Рассматриваемые вопросы: Основное назначение программно- аппаратных средств защиты информации. Разбор функций основных групп программно- аппаратных средств.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к практическим занятиям.
2	Работа с лекционным материалом.
3	Работа со справочной литературой.
4	Выполнение курсовой работы.
5	Подготовка к промежуточной аттестации.
6	Выполнение курсовой работы.
7	Подготовка к промежуточной аттестации.
8	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

1. Защита сетевой инфраструктуры (на примере объекта железнодорожного транспорта).

2. Разработка и реализация необходимых меры при обнаружении попыток несанкционированного доступа к информационным ресурсам (на примере объекта железнодорожного транспорта).

3. Совершенстование системы мониторинга состояния информационной безопасности (на примере объекта железнодорожного транспорта).

4. Методы и механизмы обеспечения доступности баз данных и сервера СУБД (на примере объекта железнодорожного транспорта).

5. Разработка системы обеспечения целостности и защиты данных (на примере объекта железнодорожного транспорта).

6. Разработка системы управления доступом (на примере объекта железнодорожного транспорта).

7. Разработка системы обеспечения конфиденциальности данных (на примере объекта железнодорожного транспорта).

8. Разработка и реализация системы анализа защищенности данных (на примере объекта железнодорожного транспорта).

9. Система оценки защищенности автоматизированных информационных систем (на примере объекта железнодорожного транспорта).

10. Разработка и реализация криптографической системы безопасности (на примере объекта железнодорожного транспорта).

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

№ п/п	Библиографическое описание	Место доступа
1	Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4	Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/index.php/bcode/434171 (дата обращения: 13.06.2024).
2	Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 84 с. — ISBN 978-5-507-48808-7	Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/394547 (дата обращения: 13.06.2024).

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);

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 «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).

Обязательный набор:

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

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.

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:

Курсовая работа в 9 семестре.
Экзамен в 9 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 «Системы управления транспортной инфраструктурой» И.М. Губенко

Согласовано:

Директор О.Н. Покусаев

Заместитель руководителя О.В. Ефимова

Председатель учебно-методической комиссии Д.В. Паринов