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
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информации в телекоммуникационных системах железнодорожного транспорта

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Дисциплина «Защита информации в телекоммуникационных системах железнодорожного транспорта» реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 100501 « Компьютерная безопасность». Дисциплина «Защита телекоммуникационных систем железнодорожного транспорта» относится к числу дисциплин специализации профессионального цикла. Целью преподавания дисциплины «Защита информации в телекоммуникационных системах железнодорожного транспорта» является изложение слушателям основных принципов и методов защиты информации, комплексного проектирования и анализа защищенных компьютерных систем КС.

Задачами изучения дисциплины являются: изучение основ устройства и принципов функционирования, методологии проектирования и построения защищенных, критериев и методов оценки защищенности КС, средств и методов защиты от несанкционированного доступа (НСД) к информации. Основной целью изучения учебной дисциплины «Защита информации в телекоммуникационных системах железнодорожного транспорта» является формирование у обучающегося компетенций для следующих видов деятельности: - научно-исследовательской; - проектной. Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности): Научно-исследовательская деятельность: сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности; участие в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах. Проектная деятельность: разработка и конфигурирование программно-аппаратных средств защиты информации; разработка технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов; разработка проектов систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием; проектирование программных и аппаратных средств защиты информации в соответствии с техническим заданием с использованием средств автоматизации проектирования.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-16 - Способен разрабатывать программные и программно-аппаратные средства для систем защиты информации автоматизированных систем;

ПК-20 - Способен подготовить обоснование необходимости защиты информации в автоматизированной системе;

ПК-21 - Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой;

ПК-25 - Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации.

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

Знать:

- основные процессы проектирования систем обеспечения информационной безопасности.
- программные и программно-аппаратные средства для систем защиты информации автоматизированных систем
- угрозы безопасности информации, обрабатываемой автоматизированной системой

Уметь:

- Разрабатывать программные средства для систем защиты информации автоматизированных систем высокоскоростного транспорта.
- Разрабатывать программные средства для систем защиты информации автоматизированных систем в беспилотных автоматизированных системах.
- разрабатывать и реализовывать технологию проведения аудита информационной безопасности на объектах информатизации.

Владеть:

- навыками анализа уязвимости и устанавливает необходимые средства защиты информации для технологической базы автоматизированных систем высокоскоростного транспорта.
- навывками анализа уязвимости и устанавливает необходимые средства защиты информации для технологической базы беспилотных автоматизированных систем.
- навыками анализа угроз безопасности информации, обрабатываемой

автоматизированными системами высокоскоростного транспорта.

- навыками анализа угроз безопасности информации, обрабатываемой беспилотными автоматизированными системами.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 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. №10
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
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 80 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	Информационная безопасность и уровни ее обеспечения Рассматриваемые вопросы: - Понятие "информационная безопасность" - Составляющие информационной безопасности - Система формирования режима информационной безопасности - Нормативно-правовые основы информационной безопасности в РФ - Стандарты информационной безопасности: "Общие критерии" 2. - Стандарты информационной безопасности распределенных систем - Стандарты информационной безопасности в РФ - Административный уровень обеспечения информационной безопасности - Классификация угроз "информационной безопасности"
2	Компьютерные вирусы и защита от них Рассматриваемые вопросы: - Вирусы как угроза информационной безопасности - Классификация компьютерных вирусов - Характеристика "вирусоподобных" программ - Антивирусные программы - Профилактика компьютерных вирусов - Обнаружение неизвестного вируса
3	Информационная безопасность вычислительных сетей Рассматриваемые вопросы: - Вирусы как угроза информационной безопасности - Классификация компьютерных вирусов - Характеристика "вирусоподобных" программ - Антивирусные программы - Профилактика компьютерных вирусов - Обнаружение неизвестного вируса
4	Механизмы обеспечения "информационной безопасности" Рассматриваемые вопросы: - Идентификация и аутентификация. - Криптография и шифрование. - Методы разграничение доступа. Регистрация и аудит. - Межсетевое экранирование. Технология виртуальных частных сетей (VPN)
5	Корпоративные защищенные сети Рассматриваемые вопросы: - Введение в MPLS, TE и QoS. - Архитектура мультипротокольной коммутации пакетов по меткам (MPLS). - Защита в MPLS с использованием генератора специализованных последовательностей.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Компьютерные атаки В результате выполнения практического задания студент рассматривает особенности стандартизации в области обнаружения атак, основные технологии обнаружения компьютерных атак и их возможности и типы атак.

№ п/п	Тематика практических занятий/краткое содержание
2	Создание защищенных сегментов при работе в сети Интерн В результате работы на практическом занятии студент отрабатывает умения создавать защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов и изучает фильтрацию пакетов
3	Туннелирование в VPN. В результате работы на практическом занятии студент отрабатывает навык составления Туннелирование в VPN.
4	LDAP В результате работы на практическом занятии студент рассматривает основные службы каталогов, LDAP, Open LDAP.
5	Протокол BGP4, IS-IS. В результате работы на практическом занятии студент отрабатывает умения работать с протоколами BGP4, IS-IS, рассматривает автономная системы AS, маршрутизация в MPLS.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к практическим занятиям.
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.
5	Подготовка к промежуточной аттестации.
6	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства) А.А. Корниенко, М.А. Еремеев, С.Е. Ададуров; Ред. А.А. Корниенко; Под Ред. А.А. Корниенко Однотомное издание Маршрут , 2006	НТБ (ЭЭ); НТБ (уч.3); НТБ (фб.); НТБ (чз.2)
2	Безопасность коммуникационных сетей В.П. Соловьев, А.Е. Шубарев, Н.Н. Пуцко; Ред. В.П. Соловьев; МИИТ. Центр компетентности "Защита и безопасность информации" Однотомное издание МИИТ , 2007	НТБ (ЭЭ); НТБ (фб.); НТБ (чз.2)
3	Разработка корпоративной сети на основе MPLS.Защита информации [Электронный ресурс] : учебно-метод. пособие по курс. работе для специалистов напр. "Компьютерная безопасность" В.М. Алексеев МИИТ , 2017	НТБ МИИТ

4	Технические средства защиты информации А.А. Титов Томский государственный университет систем управления и радиоэлектроники, , 2010	Internet
1	Криптография Н. Смарт Однотомное издание Техносфера , 2006	НТБ (фб.)
2	Компьютерные системы и сети В.П. Косарев, Л.В. Еремин, О.В. Машникова и др.; Под ред. В.П. Косарева, Л.Б. Еремина Однотомное издание Финансы и статистика , 1999	НТБ (уч.2); НТБ (уч.4); НТБ (фб.); НТБ (чз.2)

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

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

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

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/).

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

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

Work 9, интегрированная среда разработки программного обеспечения для эиуляции сетевого оборудования OmniGraffle;

среда разработки программного обеспечения HTML5 и PHP. Для проведения практических занятий и выполнения курсовой работы необходимо иметь комплекс программ для ПЭВМ, обеспечивающих возможность выполнения работ: в области построения программных и аппаратных средств защиты информации в телекоммуникационных сетях (iOS15 Cisco и выше) с поддержкой MPLS;

программные продукты Mac OS server, XSan.

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

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Зачет в 10 семестре.

10. Оценочные материалы.

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

Авторы:

профессор, профессор, д.н. кафедры
«Управление и защита информации» В.М. Алексеев

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической
комиссии С.В. Володин