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).

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.

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:

- Методологию разработки программных и программно-аппаратных средств для систем защиты информации автоматизированных систем.
- Нормативно-правовую базу и методические основы для обоснования необходимости защиты информации в автоматизированной системе.
- Классификацию и характеристику возможных угроз безопасности информации, обрабатываемой в автоматизированных системах.
- Структуру и содержание плана мероприятий по защите информации в объектах информатизации, включая этапы проектирования, создания и модернизации.

Уметь:

- Разрабатывать программные средства для систем защиты информации автоматизированных систем, включая системы высокоскоростного и беспилотного транспорта.

- Подготавливать обоснование необходимости защиты информации в автоматизированной системе на основе анализа исходных данных.

- Определять и классифицировать возможные угрозы безопасности информации, обрабатываемой автоматизированной системой.

- Разрабатывать и реализовывать технологию проведения аудита информационной безопасности и планирования мероприятий по защите на объектах информатизации.

Владеть:

- Навыками анализа уязвимостей и определения необходимых средств защиты информации для технологической базы автоматизированных систем (в т.ч. высокоскоростного транспорта).

- Навыками анализа уязвимостей и определения необходимых средств защиты информации для беспилотных автоматизированных систем.

- Навыками анализа угроз безопасности информации, обрабатываемой автоматизированными системами различного назначения.

- Навыками разработки документации по планированию мероприятий по защите информации и обоснованию необходимости внедрения средств защиты.

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	Семестр №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

№ п/п	Тематика лекционных занятий / краткое содержание
	- 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	Анализ компьютерных атак и методы их обнаружения В результате выполнения практического задания студент рассматривает особенности стандартизации в области обнаружения атак, основные технологии обнаружения компьютерных атак, их возможности и типы атак. Изучаются сигнатурный и поведенческий методы анализа.
2	Создание защищенных сегментов сети с использованием межсетевых экранов В результате работы на практическом занятии студент отрабатывает умения создавать защищенные сегменты при работе в сети Интернет с использованием межсетевых экранов, изучает принципы фильтрации пакетов и настройки правил доступа.
3	Организация туннелирования и построение VPN В результате работы на практическом занятии студент отрабатывает навык настройки туннелей в VPN, изучает протоколы IPSec, GRE и их применение для защиты каналов связи.
4	Настройка служб каталогов и системы LDAP В результате работы на практическом занятии студент рассматривает основные службы каталогов, протокол LDAP, его реализацию в Open LDAP, а также вопросы безопасности при аутентификации и авторизации пользователей.
5	Протоколы маршрутизации BGP4 и IS-IS в защищенных сетях В результате работы на практическом занятии студент отрабатывает умения работать с протоколами BGP4 и IS-IS, рассматривает понятие автономной системы (AS), а также вопросы безопасности маршрутизации.
6	Технология MPLS и ее защита В результате работы студент изучает архитектуру мультипротокольной коммутации по меткам (MPLS), механизмы защиты в MPLS-сетях, включая использование генераторов специализированных последовательностей.
7	Обеспечение информационной безопасности на транспорте В результате работы студент анализирует особенности применения изученных технологий защиты информации в телекоммуникационных системах железнодорожного транспорта, включая требования к безопасности диспетчерских систем управления.
8	Разработка политики безопасности для корпоративной сети В результате работы студент разрабатывает фрагмент политики информационной безопасности для

№ п/п	Тематика практических занятий/краткое содержание
	корпоративной сети транспортного предприятия, включая меры по идентификации, аутентификации, разграничению доступа и аудиту.

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

№ п/п	Библиографическое описание	Место доступа
1	Криптография Часть II Донгак Ш. М. Практикум М.: МИРЭА - Российский технологический университет, - 64 с. , 2020	https://reader.lanbook.com/book/163935
2	Криптографические методы защиты информации: классическая криптография Борисова С. Н. Учебное пособие Пензенский государственный университет, - ISBN 978-5-907102-51-4, - 186 с. , 2018	https://reader.lanbook.com/book/162235

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:

Экзамен 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