МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

26 июня 2019 г.

Кафедра «Управление и защита информации»

Автор Алексеев Виктор Михайлович, д.т.н., профессор

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Защита информации в телекоммуникационных системах железнодорожного транспорта»

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2019

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 25 июня 2019 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 21 24 июня 2019 г. Заведующий кафедрой  Л.А. Баранов

Москва 2019 г.

1. Цели освоения учебной дисциплины

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 ПСК-8 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. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Защита информации в телекоммуникационных системах железнодорожного транспорта" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПКР-4	Способен разрабатывать программные и программно-аппаратные

	средства для систем защиты информации автоматизированных систем
ПКР-8	Способен подготовить обоснование необходимости защиты информации в автоматизированной системе
ПКР-9	Способен определять возможные угрозы безопасности информации, обрабатываемой автоматизированной системой
ПКС-2	Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Защита информации в телекоммуникационных систем железнодорожного транспорта» осуществляется в форме лекций, лабораторных работ и практических занятий.Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью на 30% являются традиционными классически-лекционными (объяснительно-иллюстративные), и на 70% с использованием интерактивных (диалоговых) технологий, в том числе мультимедиа лекция.Практические занятия и лабораторные работы организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач). Остальная часть практического курса проводится с использованием интерактивных (диалоговые) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а так же использованием компьютерной тестирующей системы.В ходе выполнения курсовой работы реализуются проектные и исследовательские методы обучения. Это позволяет развивать индивидуальные творческие способности обучающихся, более осознанно подходить к профессиональному и социальному самоопределению, самостоятельно пополнять свои знания, глубоко вникать в изучаемую проблему и предполагать пути ее решения, что важно при формировании мировоззрения. Это важно для определения индивидуальной траектории развития каждого обучающегося.Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относиться отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов.Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 5 разделов, представляющих собой логически завершенный объём учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые опросы, решение тестов с использованием компьютеров или на бумажных носителях. .

6. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1
Информационная безопасность и уровни ее обеспечения
1. 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"

РАЗДЕЛ 2
Компьютерные вирусы и защита от них
1. Вирусы как угроза информационной безопасности Классификация компьютерных вирусов
2. Характеристика "вирусоподобных" программ Антивирусные программы
3. Профилактика компьютерных вирусов Обнаружение неизвестного вируса

РАЗДЕЛ 3
Информационная безопасность вычислительных сетей
опросы

РАЗДЕЛ 3
Информационная безопасность вычислительных сетей
1.Особенности обеспечения информационной безопасности в компьютерных сетях
Сетевые модели передачи данных
2. Модель взаимодействия открытых систем OSI/ISO Адресация в глобальных сетях
Классификация удаленных угроз в вычислительных сетях
3. Типовые удаленные атаки и их характеристика Причины успешной реализации удаленных угроз в вычислительных сетях Принципы защиты распределенных вычислительных сетей

РАЗДЕЛ 4
Механизмы обеспечения "информационной безопасности»
1. Идентификация и аутентификация.
2. Криптография и шифрование.
3. Методы разграничение доступа. Регистрация и аудит.
4. Межсетевое экранирование. Технология виртуальных частных сетей (VPN)

РАЗДЕЛ 5
Корпоративные защищенные сети
1. Введение в MPLS, TE и QoS.
2. Архитектура мультипротокольной коммутации пакетов по меткам (MPLS).
3. Защита в MPLS с использованием генератора специализованных последовательностей.

РАЗДЕЛ 5
Корпоративные защищенные сети
опросы

РАЗДЕЛ 7
Зачет с оценкой