МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИУЦТ

С.П. Вакуленко

06 октября 2020 г.

Кафедра «Цифровые технологии управления транспортными процессами»

Автор Андреева Татьяна Алексеевна

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Информационная безопасность и защита информации на транспорте»

Направление подготовки:	09.03.02 – Информационные системы и технологии
Профиль:	Информационные системы и технологии на транспорте
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2017

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 3 05 октября 2020 г. Председатель учебно-методической комиссии Н.А. Клычева	Протокол № 2 02 октября 2020 г. Заведующий кафедрой В.Е. Нутович

Москва 2020 г.

1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины «Информационная безопасность и защита информации на транспорте» – является изучение студентами основ создания защищенных компьютерных систем.
Основной целью изучения учебной дисциплины «Информационная безопасность и защита информации на транспорте» является формирование у обучающегося компетенций в области защиты информации, необходимых при эксплуатации, техническом обслуживании, проектировании, производстве, испытаниях, модернизации технических и программных средств железнодорожного транспорта для следующих видов деятельности:
• проектно-конструкторская;
• научно-исследовательской.
Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):
проектно- конструкторская:
• использования типовых методов создания изображений;
• разработки технических требований, технических заданий и технических условий на информационные системы, для визуализации результатов испытаний работоспособности информационных систем, при создании сопроводительной документации;
научно-исследовательская деятельность:
• научных исследований в области эксплуатации и производства систем информационной безопасности железнодорожного транспорта, интерпретации и вероятностного моделирования отказов систем защиты с формулировкой аргументированных умозаключений и выводов; поиска и проверки новых технических и программных решений по совершенствованию этих систем; разработки планов, программ и методик проведения исследований уровня защищенности, анализ их результатов.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Информационная безопасность и защита информации на транспорте" 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:

ОПК-4	пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны
ПК-3	способностью проводить рабочее проектирование

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Информационная безопасность и защита информации на транспорте» осуществляется в форме лекций и лабораторных работ. Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью и на 50 % являются традиционными

классически-лекционными (объяснительно-иллюстративными), на 50 % с использованием интерактивных (диалоговых) технологий Проведении занятий по дисциплине (модулю) возможно с применением электронного обучения и дистанционных образовательных технологий, реализуемые с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.В процессе проведения занятий с применением электронного обучения и дистанционных образовательных технологий применяются современные образовательные технологии, такие как (при необходимости):- использование современных средств коммуникации;- электронная форма обмена материалами;- дистанционная форма групповых и индивидуальных консультаций;- использование компьютерных технологий и программных продуктов, необходимых для сбора и систематизации информации, проведения требуемых программой расчетов и т.д.Лабораторные работы организованы с использованием технологий развивающего обучения. Для проведения лабораторных занятий используется компьютерный класс, в котором каждый студент выполняет лабораторную работу индивидуально. Применяются необходимые средства: специальное программное обеспечение, методические указания. Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы (15 часов) относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям (10 часов) относится 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 7 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 (анализ конкретных ситуаций, 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
Проблемы информационной безопасности (ИБ) и защиты информации (ЗИ) в компьютерных системах (КС)

Тема: Основные понятия ИБ и ЗИ. Предмет защиты, объект защиты Угрозы ИБ в КС, случайные и преднамеренные.

РАЗДЕЛ 2
Защита информации в КС путем разграничения прав доступа ЗИ в КС от случайных угроз текущий контроль по разделам 1 - 2. (Тест №1)

Тема: Повышение надежности программных и аппаратных средств ЗИ в КС от преднамеренных угроз

РАЗДЕЛ 3
Криптографические методы защиты информации

Тема: Основные этапы развития криптографии Криптографические системы с симметричным ключом. Стандарты шифрования. Криптографические системы с

открытым ключом

РАЗДЕЛ 4
Стеганографические методы ЗИ

Тема: Стеганографические методы ЗИ Область применения. Основные понятия стеганографии. Классификация методов. Алгоритмы встраивания информации в изображения, в аудио-сигналы.

РАЗДЕЛ 5
Защита данных ЗИ в телекоммуникационных сетях

Тема: Категории атак: эксплойт, проникновение, хищение сеанса, отказ от обслуживания, присвоение пакетов. Защита периметра сети, защита от инсайдера, защита от вредоносных программ.

РАЗДЕЛ 6
Защищенные виртуальные сети
текущий контроль по разделам 5 - 6 (Тест №2)

Тема: Понятия инкапсуляции и туннелирования. Протоколы канального, сетевого и сеансового уровня.

РАЗДЕЛ 7
Законодательство в области ИБ

Тема: Ответственность в сфере компьютерной безопасности Защита персональных данных

Экзамен