МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Стеганографические методы защиты информации

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Форма обучения:	Очная

Общие сведения о дисциплине (модуле).

Целями изучения дисциплины «Стеганографические методы защиты информации» являются теоретическая и практическая подготовка специалистов к деятельности, связанной с применением средств вычислительной техники в технологических процессах управления железнодорожным транспортом (ЖТ), требующих соблюдения условий безопасности движения поездов.

Задачи дисциплины: - изучение математических основ стеганографических методов защиты информации; - изучение различных методов генерации случайных и псевдослучайных чисел-основы создания криптографических и стеганографических систем; - получение навыков программной реализации генераторов случайных и псевдослучайных чисел различных типов; - изучение методов стеганографического встраивания информации в графические, аудио и текстовые файлы и алгоритмов, их реализующих; - получение навыков программной реализации методов стеганографического встраивания информации в графические, аудио и

текстовые файлы; - изучение методов анализа подлинности изображений; получение навыков программной реализации методов анализа подлинности изображений. Основной целью изучения учебной дисциплины «Стеганографические методы защиты информации» является формирование у обучающегося компетенций для следующих видов деятельности: научно-исследовательская; проектная; контрольно-аналитическая. Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с типами задач профессиональной деятельности): Научно-исследовательская деятельность: сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности; изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте; подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований. Проектная деятельность: 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. Контрольно-аналитическая деятельность: предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей; применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты; подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей.

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов).