МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

26 мая 2020 г.

Кафедра «Управление и защита информации»

Автор Сидоренко Валентина Геннадьевна, д.т.н., профессор

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Стеганографические методы защиты информации»

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	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 26 мая 2020 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 16 21 мая 2020 г. Заведующий кафедрой  Л.А. Баранов

Москва 2020 г.

1. Цели освоения учебной дисциплины

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 видами 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.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Стеганографические методы защиты информации" 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-1	Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов
ПКС-1	Способен разрабатывать модели угроз, формировать требования 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 «Стеганографические методы защиты информации» осуществляется в форме лекций и практических занятий. Лекции проводятся в традиционной классно-урочной организационной форме.Практические занятия организованы с использованием технологий развивающего обучения. В ходе обучения 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.Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на разделы, представляющие 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..

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

РАЗДЕЛ 1
Общие вопросы стеганографии

Тема: 1.1.
Введение. Предмет курса и его связь со смежными дисциплинами. Библиография. Постановка задачи стеганографической защиты информации.

Тема: 1.2.
Структурная схема системы стеганографической защиты информации
Типы стеганографических систем. Принцип Керкгоффса. Методы стеганографии и их классификация.

Тема: 1.3.
Анализ угроз и оценка устойчивости системы стеганографической защиты информации.

Тема: 1.4.
Генераторы псевдослучайных чисел. Их классификация. Уязвимости, связанные с некачественным генерированием случайных чисел.

РАЗДЕЛ 2
Общие теоретические положения цифровой обработки сигналов

Тема: 2.1.
Представление сигналов во временной (пространственной) и частотной областях. Непрерывные, дискретные и цифровые сигналы. Элементы теории дискретизации сигналов. Z-преобразование.

Тема: 2.2.
Ортогональные преобразования. Введение в ортогональные преобразования и быстрые алгоритмы. Понятие системы ортогональных функций. Ортогональные преобразования на базе функций в виде прямоугольных импульсов.

Тема: 2.3.
Вейвлет-преобразования. Типы вейвлет-функций. Применение вейвлет-преобразования.

Тема: 2.4.
Дискретное преобразование Фурье (ДПФ). Типы преобразований Фурье. Алгоритмы Кули-Тьюки для вычисления быстрого преобразования Фурье (БПФ).

Тема: 2.5.
Автокорреляционная функция (АКФ) и взаимнокорреляционная функция (ВКФ). Определение АКФ и ВКФ. Вычисление АКФ и ВКФ.

Тема: 2.6.
Анализ и обработка изображений. Задачи линейной фильтрации изображений. Задачи нелинейной фильтрации изображений. Задачи выделения контуров. Показатели визуального искажения.

Тема: 2.6.
Устный опрос

Тема: 2.7.
Анализ форматов хранения графической информации. Анализ графической информации в частотной области.

Тема: 2.8.
Анализ информации об устройстах, используемых для получения графической информации.

РАЗДЕЛ 3
Скрытие данных в контейнерах различной природы

Тема: 3.1.
Классификация методов скрытия данных в графических контейнерах. Скрытие данных в пространственной области изображения. Скрытие данных в частотной области изображения. Методы расширения спектра. Другие методы скрытия данных в

неподвижных изображениях. Статистические методы. Структурные методы.

Тема: 3.2.
Скрытие данных в графических контейнерах в пространственной области изображения. Метод сокрытия в наименьших значащих битах. Метод блочного скрытия. Метод замены палитры. Метод квантования. Метод Куттера-Джордана-Боссена. Метод псевдослучайного интервала. Метод псевдослучайной перестановки. Метод Дармстедтера-Делейгла-Квисквотера-Макка.

Тема: 3.2.
Устный опрос

Тема: 3.3.
Скрытие данных в графических контейнерах в частотной области изображения. Метод сокрытия с использованием нелинейной модуляции встраиваемого сообщения. Метод сокрытия с использованием знаковой модуляции встраиваемого сообщения. Метод сокрытия, основанный на вейвлет-преобразовании. графической информации. Метод сокрытия, основанный на косинусном преобразовании графической информации. Метод Коха и Хао. Метод Бенгама-Мемона-Эо-Юнг. Метод Хсу-Ву. Метод Фридрих.

Тема: 3.4.
Скрытие данных в аудиоконтейнерах. Метод сокрытия в наименьших значащих битах. Метод сокрытия на основе распределения по спектру. Метод сокрытия на основе использования эхо-сигнала. Метод сокрытия в фазе сигнала.

Тема: 3.5.
Скрытие данных в текстовых файлах. Методы сокрытия на основе пробелов. Метод изменения интервала между предложениями. Метод изменения количества пробелов в конце текстовых строк. Метод изменения количества пробелов между словами выровненного по ширине текста.

Тема: 3.6.
Скрытие данных в текстовых файлах на основе синтаксических особенностей текста. Метод сокрытия на основе синонимов. Метод сокрытия на основе использования ошибок. Метод сокрытия на основе генерации квазитекста. Метод сокрытия на основе использования особенностей шрифта. Метод сокрытия на основе использования кода документа и файла. Метод сокрытия на основе использования жаргона.
Метод сокрытия на основе использования чередования длины слов. Метод сокрытия на основе использования первых букв.

РАЗДЕЛ 4
Зачет с оценкой