МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором ФГАОУ ВО
РУТ (МИИТ) Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Стеганографические методы защиты информации

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная ФГАОУ ВО РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.09.2026

1. 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.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-3 - Способен на основании совокупности математических методов, физических законов и моделей разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;

ПК-3 - Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- сновные формальные модели изолированной программной среды и безопасности информационных потоков.
- математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов.

Уметь:

- Строить математические модели для оценки безопасности компьютерных систем.
- разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем.

Владеть:

- навыками анализа компонентов системы безопасности с использованием современных математических методов.

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 №7
Контактная работа при проведении учебных занятий (всего):	80	80
В том числе:		
Занятия лекционного типа	48	48
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 64 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	Общие вопросы стеганографии Рассматриваемые вопросы: - Основные понятия, термины и определения - Предмет курса и его связь со смежными дисциплинами. - Библиография. - Постановка задачи стеганографической защиты информации.
2	Стенографические системы. Рассматриваемые вопросы: - Структурная схема системы стеганографической защиты информации

№ п/п	Тематика лекционных занятий / краткое содержание
	- Типы стеганографических систем. - Принцип Керкгоффса. - Методы стеганографии и их классификация.
3	Угрозы стенографической системы Рассматриваемые вопросы: - Анализ угроз и оценка устойчивости системы стеганографической защиты информации.
4	Генератор псевдослучайных чисел. Рассматриваемые вопросы: - Генераторы псевдослучайных чисел. - Их классификация. - Уязвимости, связанные с некачественным генерированием случайных чисел.
5	Общие теоретические положения цифровой обработки сигналов Рассматриваемые вопросы: - Представление сигналов во временной (пространственной) и частотной областях. - Непрерывные, дискретные и цифровые сигналы. - Элементы теории дискретизации сигналов. - Z-преобразование.
6	Ортогональные преобразования Рассматриваемые вопросы: - Ортогональные преобразования. - Введение в ортогональные преобразования и быстрые алгоритмы. - Понятие системы ортогональных функций. - Ортогональные преобразования на базе функций в виде прямоугольных импульсов.
7	Вейвлет-преобразования. Рассматриваемые вопросы: - основные понятия вейвлет-преобразования. - Типы вейвлет-функций. - Применение вейвлет-преобразования.
8	Дискретное преобразование Фурье. Рассматриваемые вопросы: - основыне понятия дискретного преобразования Фурье (ДПФ). - Типы преобразований Фурье. - Алгоритмы Кули-Тьюки для вычисления быстрого преобразования Фурье (БПФ).
9	Автокорреляционная функция (АКФ) и взаимнокорреляционная функция (ВКФ). Рассматриваемые вопросы: - основыне термины и определения автокорреляционной функции (АКФ) и взаимнокорреляционной функции (ВКФ). - Определение АКФ и ВКФ. - Вычисление АКФ и ВКФ.
10	Обработка изображений Рассматриваемые вопросы: - Анализ и обработка изображений. - Задачи линейной фильтрации изображений. - Задачи нелинейной фильтрации изображений. - Задачи выделения контуров. - Показатели визуального искажения.
11	Графическая информация. Рассматриваемые вопросы: - Анализ форматов хранения графической информации. - Анализ графической информации в частотной области.

№ п/п	Тематика лекционных занятий / краткое содержание
12	Устройства графической информации. Рассматриваемые вопросы: - Анализ информации об устройстах, используемых для получения графической информации.
13	Скрытие данных в контейнерах различной природы Рассматриваемые вопросы: - 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.
14	Скрытие данных в графических контейнерах в пространственной области изображения. Рассматриваемые вопросы: - Особенности скрытия 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.
15	Скрытие данных в графических контейнерах в частотной области изображения. Рассматриваемые вопросы: - Особенности скрытия 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.
16	Скрытие данных в аудиоконтейнерах. Рассматриваемые вопросы: - Особенности скрытия 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.
17	Скрытие данных в текстовых файлах. Рассматриваемые вопросы: - Особенности скрытия 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.

№ п/п	Тематика лекционных занятий / краткое содержание
18	Скрытие данных в текстовых файлах на основе синтаксических особенностей текста. Рассматриваемые вопросы: - Особенности скрытия 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.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Генераторы псевдослучайных чисел. В результате выполнения лабораторной работы студент рассматривает особенности генераторов псевдослучайных чисел.
2	Оцифровка и восстановление сигнала В результате выполнения работы студент отрабатывает умение по оцифровки и восстановлению сигнала.
3	Вейвлет-преобразование. В результате выполнения работы студент рассматривает вейвлет-преобразование.
4	Обработка изображений В результате выполнения работы студент отрабатывает умение по обработке изображений.
5	Показатели визуального искажения В результате выполнения лаюбораторной работы студент рассматривает основные показатели визуального искажения.
6	Графическая информация В результате выполнения лабораторной работы студент получает навык анализа форматов хранения графической информации, анализ графической информации в частотной области.
7	Устройства для работы с графической информации. В результате выполнения лабораторной работы студент отрабатывает умнеие анализировать информацию об устройстах, используемых для получения графической инфомарции.
8	Скрытие данных в графических контейнерах В результате выполнения работы студент отрабатывает умение по скрытию данных в графических контейнерах в пространственной области изображения.
9	Скрытие данных в графических контейнерах В результате выполнения лабораторной работы студент отрабатывает умение по скрытию данных в графических контейнерах в частотной области изображения.
10	Скрытие данных в аудиоконтейнерах В результате выполнения лабораторной работы студент отрабатывает умение по скрытию данных в аудиоконтейнерах
11	Скрытие данных в текстовых файлах В результате выполнения работы студент изучает скрытие данных в текстовых файлах

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к лабораторным работам.
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

1. Защита данных стеганографическими методами.

2. Скрытие данных в графических контейнерах в пространственной области изображения.

3. Скрытие данных в графических контейнерах в частотной области изображения.

4. Анализ и применение методов скрытия информации в аудиоконтейнерах.

5. Исследование методов скрытия данных в текстовых файлах на основе форматирования.

6. Разработка алгоритма скрытия информации с использованием вейвлет-преобразования.

7. Сравнительный анализ устойчивости стеганографических методов к атакам сжатия.

8. Программная реализация метода скрытия информации в наименьших значащих битах (LSB).

9. Методы обнаружения скрытой информации (стеганоанализ) в неподвижных изображениях.

10. Исследование генераторов псевдослучайных чисел для систем стеганографической защиты.

11. Применение дискретного косинусного преобразования (DCT) для встраивания информации в JPEG-файлы.

12. Разработка стеганографической системы на основе метода расширения спектра.

13. Анализ подлинности изображений и выявление признаков цифрового монтажа.

14. Скрытие данных в аудиоконтейнерах на основе использования эхо-сигнала.

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

№ п/п	Библиографическое описание	Место доступа
1	Стеганографические методы защиты информации (Современные симметричные криптосистемы. Методы стеганографии) Макаров В. Ф., Нечаев Д. Ю. Учебно-методическое издание М.: Московский гуманитарный университет, - 24 с. - ISBN 978-5-907194-64-9 , 2020	https://reader.lanbook.com/book/507998
2	Общий курс транспорта Фаталиев Н.Г. Учебное пособие Махачкала: Дагестанский ГАУ, - 178 с. , 2020	https://reader.lanbook.com/book/162218#1

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/).

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

Пакет прикладных программ MATLAB, MATCad

Пакет прикладных программ LABView

Среда визуального программирования MicroSoft Visual Studio 2013.

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:

Зачет в 7 семестре.
Курсовая работа в 7 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 «Интеллектуальное управление и информационная безопасность в высокоавтоматизированных транспортных системах» Института железнодорожного транспорта — В.Г. Сидоренко

Согласовано:

Заведующий кафедрой ИУиИБ — Л.А. Баранов

Председатель учебно-методической комиссии — Н.А. Андриянова