МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором 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

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 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. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-13 - Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;

ПК-24 - Способен разрабатывать модели угроз, формировать требования по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации.

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

Уметь:

Строит математические модели для оценки безопасности компьютерных систем.

Уметь:

Анализирует компоненты системы безопасности с использованием современных математических методов.

Знать:

Знать основные формальные модели изолированной программной среды и безопасности информационных потоков.

Уметь:

Уметь разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем.

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	Сем. №7
Контактная работа при проведении учебных занятий (всего):	84	84
В том числе:		
Занятия лекционного типа	50	50
Занятия семинарского типа	34	34

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 60 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
2	Введение. Предмет курса и его связь со смежными дисциплинами. Библиография. Постановка задачи стеганографической защиты информации.
3	Структурная схема системы стеганографической защиты информации Типы стеганографических систем. Принцип Керкгоффса. Методы стеганографии и их классификация.

№ п/п	Тематика лекционных занятий / краткое содержание
4	Анализ угроз и оценка устойчивости системы стеганографической защиты информации.
5	Генераторы псевдослучайных чисел. Их классификация. Уязвимости, связанные с некачественным генерированием случайных чисел.
6	Общие теоретические положения цифровой обработки сигналов
7	Представление сигналов во временной (пространственной) и частотной областях. Непрерывные, дискретные и цифровые сигналы. Элементы теории дискретизации сигналов. Z-преобразование.
8	Ортогональные преобразования. Введение в ортогональные преобразования и быстрые алгоритмы. Понятие системы ортогональных функций. Ортогональные преобразования на базе функций в виде прямоугольных импульсов.
9	Вейвлет-преобразования. Типы вейвлет-функций. Применение вейвлет-преобразования.
10	Дискретное преобразование Фурье (ДПФ). Типы преобразований Фурье. Алгоритмы Кули-Тьюки для вычисления быстрого преобразования Фурье (БПФ).
11	Автокорреляционная функция (АКФ) и взаимнокорреляционная функция (ВКФ). Определение АКФ и ВКФ. Вычисление АКФ и ВКФ.
12	Анализ и обработка изображений. Задачи линейной фильтрации изображений. Задачи нелинейной фильтрации изображений. Задачи выделения контуров. Показатели визуального искажения.
13	Анализ форматов хранения графической информации. Анализ графической информации в частотной области.
14	Анализ информации об устройстах, используемых для получения графической информации.
15	Скрытие данных в контейнерах различной природы
16	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.
17	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.
18	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.

№ п/п	Тематика лекционных занятий / краткое содержание
19	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.
20	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.
21	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.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	ЛР1 Генераторы псевдослучайных чисел.
2	ЛР2 Оцифровка и восстановление сигнала
3	ЛР3 Вейвлет-преобразование.
4	ЛР4 Обработка изображений
5	ЛР5 Показатели визуального искажения
6	ЛР6 Текущий контроль по разделам 1-2. (Устный опрос № 1). Разбор наиболее частых ошибок.
7	ЛР7 Анализ форматов хранения графической информации. Анализ графической информации в частотной области.
8	ЛР8 Анализ информации об устройстах, используемых для получения графической инфомарции.
9	ЛР9 Скрытие данных в графических контейнерах в пространственной области изображения.
10	ЛР10 Текущий контроль по разделу 3. (Устный опрос № 2). Разбор наиболее частых ошибок
11	ЛР11 Скрытие данных в графических контейнерах в частотной области изображения.
12	ЛР12 Скрытие данных в аудиоконтейнерах

№ п/п	Наименование лабораторных работ / краткое содержание
13	ЛР13 Скрытие данных в текстовых файлах

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР1 1. Подготовка к опросу для прохождения первого текущего контроля. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [1], [2, стр. 4-28], [3]-[6] 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 5. Конспектирование изученного материала.
2	СР2 1. Подготовка к опросу для прохождения первого текущего контроля. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [1], [2, стр. 4-28], [5]-[8]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 5. Конспектирование изученного материала.
3	СР3 1. Подготовка к опросу для прохождения первого текущего контроля. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [1], [2, стр. 4-28], [5]-[8]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 5. Конспектирование изученного материала.
4	СР4 1. Подготовка к опросу для прохождения первого текущего контроля. 2. Подготовка к практическому занятию № 1. 3. Повторение лекционного материала. 4. Изучение учебной литературы из приведенных источников: [1], [2, стр. 4-28], [5]-[8]. 5. Изучение ресурсовинформационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала.
5	СР5 1. Подготовка к опросу для прохождения первого текущего контроля. 2. Подготовка к практическому занятию № 2. 3. Повторение лекционного материала. 4. Изучение учебной литературы из приведенных источников: [4]. 5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала.
6	СР6 1. Подготовка к опросу для прохождения первого текущего контроля. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [3]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 5. Конспектирование изученного материала.
7	СР7 1. Подготовка к опросу для прохождения первого текущего контроля. 2. Повторение лекционного материала. 3. Подготовка к практическому занятию № 3. 4. Изучение учебной литературы из приведенных источников: [3]. 5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала.
8	СР8 1. Подготовка к опросу для прохождения первого текущего контроля. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [3]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала.

№ п/п	Вид самостоятельной работы
9	СР9 1. Подготовка к опросу для прохождения первого текущего контроля. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [3]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 5. Конспектирование изученного материала.
10	СР10 1. Подготовка к опросу для прохождения первого текущего контроля. 2. Подготовка к практическим занятиям № 4-6. 3. Повторение лекционного материала. 4. Изучение учебной литературы из приведенных источников: [3]. 5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала.
11	СР11 1. Подготовка к опросу для прохождения второго текущего контроля. 2. Подготовка к практическому занятию № 8. 3. Повторение лекционного материала. 4. Изучение учебной литературы из приведенных источников: [3]. 5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала.
12	СР12 1. Подготовка к опросу для прохождения второго текущего контроля. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [3]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала.
13	СР13 1. Подготовка к опросу для прохождения второго текущего контроля. 2. Подготовка к практическому занятию № 9. 3. Повторение лекционного материала. 4. Изучение учебной литературы из приведенных источников: [2, стр. 29-42]. 5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала.
14	СР14 1. Подготовка к устному опросу для прохождения второго текущего контроля. 2. Подготовка к практическим занятиям № 10-11. 3. Повторение лекционного материала. 4. Изучение учебной литературы из приведенных источников: [2, стр. 29-42]. 5. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 6. Конспектирование изученного материала.
15	СР15 1. Подготовка к практическому занятию № 12. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [2, стр. 29-42]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 5. Конспектирование изученного материала.
16	СР16 1. Подготовка к практическому занятию № 13. 2. Повторение лекционного материала. 3. Изучение учебной литературы из приведенных источников: [2, стр. 43-47]. 4. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 5. Конспектирование изученного материала.
17	СР17 1. Повторение лекционного материала. 2. Изучение учебной литературы из приведенных источников: [2, стр. 48-52]. 3. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 4. Конспектирование изученного материала.

№ п/п	Вид самостоятельной работы
18	СР18 1. Повторение лекционного материала. 2. Изучение учебной литературы из приведенных источников: [2, стр. 48-52]. 3. Изучение ресурсов информационно-телекоммуникационной сети «ИНТЕРНЕТ», необходимых для освоения дисциплины. 4. Конспектирование изученного материала.
19	Выполнение курсовой работы.
20	Подготовка к промежуточной аттестации.
21	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

Курсовые работы (проекты) не предусмотрены.

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

№ п/п	Библиографическое описание	Место доступа
1	Единая транспортная система Н.А. Троицкая, А.Б. Чубуков Однотомное издание Academia , 2004	НТБ (уч.4); НТБ (фб.); НТБ (чз.1)
2	Стеганографические методы защиты информации А.В. Изычева, В.Г. Сидоренко РУТ (МИИТ), , 2017	
3	Цифровая обработка сигналов А.Б. Сергиенко Однотомное издание Питер , 2007	НТБ (уч.3); НТБ (фб.); НТБ (чз.2)
4	Теория автоматического управления С.Е. Душин, Н.С. Зотов, Д.Х. Имаев и др.; Ред. В.Б. Яковлев; Под Ред. В.Б. Яковлев Однотомное издание Высш. шк. , 2005	НТБ (уч.3); НТБ (фб.); НТБ (чз.2)
5	Анализ подлинности изображения А.А. Арцыбашева, А.А. Козлов, В.Г. Сидоренко РУТ (МИИТ), , 2018	
6	Генераторы случайных чисел Е.Г. Воронина, В.Г. Сидоренко РУТ(МИИТ) , 2018	
1	Аспекты информационной безопасности В.Г. Сидоренко, Н.Н. Скоробогатова РУТ(МИИТ) , 2018	
2	Информационные технологии на железнодорожном транспорте Э.К. Лецкий, В.И. Панкратов, В.В. Яковлев и др.; Под ред. Э.К. Лецкого, Э.С. Поддавашкина, В.В. Яковлева Однотомное издание УМК МПС России , 2000	НТБ (уч.2); НТБ (уч.3); НТБ (уч.4); НТБ (фб.); НТБ (чз.2)
3	Управление и информационные технологии на железнодорожном транспорте Л.П. Тулупов, Э.К. Лецкий, И.Н. Шапкин и др.; Под ред. Л.П. Тулупова Однотомное издание Маршрут , 2005	НТБ (БР.); НТБ (уч.4); НТБ (фб.); НТБ (чз.1)
4	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта В.В.	НТБ (уч.4); НТБ (фб.); НТБ (чз.1)

	Яковлев, А.А. Корниенко Однотомное издание УМК МПС России , 2002	

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ. http://elibrary.ru/ - научно-электронная библиотека. http://robotosha.ru/ www.chipinfo.ru. http://siblec.ru/ http://www.intuit.ru http://twirpx.com http://habrahabr.ru http://semestr.ru scholar.google.ru http://www.intersystems.ru http://www.comprog.ru http://ctf.sfedu.ru/about-ctf/ http://ctf.sfedu.ru/category/write-ups/ http://cs.dartmouth.edu/farid Поисковые системы: Yandex, Google, Mail.

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Компьютеры должны быть обеспечены лицензионными программными продуктами:Microsoft Office не ниже Microsoft Office 2007 (2013), пакет прикладных программ MATLAB, MATCad, пакет прикладных программ LABView, среда визуального программирования MicroSoft Visual Studio 2013. Для самостоятельной работы обучающихся необходим доступ к сети Интернет и к электронной информационно-образовательной среде университета.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Для проведения лекционных занятийнеобходима лекционная аудитория с меловой или маркерной доской, желательно наличие мультимедиа аппаратуры и интерактивной доски.Для проведения практических занятий и самостоятельной работы необходимыкомпьютеры с рабочими местами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами и доступом к сети Интернет, электронной информационно-образовательной среде университета.

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 «Управление и защита информации»	Сидоренко Валентина Геннадьевна

Лист согласования

Заведующий кафедрой УиЗИ	Л.А. Баранов
Председатель учебно-методической комиссии	С.В. Володин