МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Нижегородский государственный технический университет им. Р.Е. Алексеева» (НГТУ)

Дзержинский политехнический институт (филиал)

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 50680B7E282BE1190F7ADAFAB67930C8
Владелец: Петровский Александр Михайлович
Действителен: с 23.12.2024 до 18.03.2026

УТВЕРЖДАЮ:
Директор института
_____А.М. Петровский
“ 26 ”___марта_____2025г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.3.2«Стеганографические методы защиты информации»

(индекс и наименование дисциплины по учебному плану)
для подготовки магистров

Направление подготовки: **09.04.02 Информационные системы и технологии**

Направленность: Разработка, безопасность и сопровождение информационных систем

Форма обучения: очная

Год начала подготовки 2025

Выпускающая кафедра Автоматизация, энергетика, математика и информационные системы

Кафедра-разработчик Автоматизация, энергетика, математика и информационные системы

Объем дисциплины 144/ 4

Промежуточная аттестация экзамен

Разработчик: Наумова Е.Г., к.т.н.

Дзержинск,2025

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки 09.04.02 Информационные системы и технологии, утвержденного приказом МИНОБРНАУКИ РОССИИот19.09.2017 г. № 917

на основании учебного плана принятого УС ДПИ НГТУ
протокол от 20.03.2025 № 7

Рабочая программа одобрена на заседании кафедры-разработчика РПД Автоматизация, энергетика, математика и информационные системы
протокол от 20.03.2025 № 5

Заведующий кафедрой АЭМИС, к.т.н., доцент

Л.Ю. Вадова

(подпись) *(расшифровка подписи)*

СОГЛАСОВАНО:

Заведующий выпускающей кафедрой «Автоматизация, энергетика, математика и информационные системы»,
к.т.н., доцент

Л.Ю. Вадова

(подпись) *(расшифровка подписи)*

Начальник ОУМБО И.В. Старикова

(подпись) *(расшифровка подписи)*

Рабочая программа зарегистрирована в ОУМБО: 09.04.02 - 23

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цель освоения дисциплины: изучение математических моделей, методов и алгоритмов передачи информации, при которой скрывается сам факт передачи.

1.2. Задачи освоения дисциплины (модуля):

− Понимание сущности стеганографии;

− Изучение основных методов встраивания данных в текстовые, графические, аудио- и видео-контейнеры;

− Изучение основных методов анализа текстовых, графических, аудио и видео-контейнеров на предмет наличия скрытых данных.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Стеганографические методы защиты информации» включена в перечень, вариативной части дисциплин (формируемой участниками образовательных отношений) по выбору (запросу обучающихся), направленный на углубление уровня освоения компетенций. Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП.

Дисциплина «Стеганографические методы защиты информации» базируется на следующих дисциплинах: «Математические основы криптологии».

Дисциплина «Стеганографические методы защиты информации» является основополагающей для прохождения преддипломной практики и выполнения выпускной квалификационной работы.

Рабочая программа дисциплины «Стеганографические методы защиты информации» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся, по их личному заявлению.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Таблица 1

Формирование компетенций ПКС-2 дисциплинами
для обучающихся очной формы обучения

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки бакалавра /специалиста/магистра»			
	1	*2*	*3*	*4*
ПКС-1 Способен использовать методы научных исследований в профессиональной деятельности				
Предиктивная аналитика				
Технологии больших данных				
Стеганографические методы защиты информации				
Научно-исследовательская работа				
Преддипломная				
Выполнение и защита ВКР				
ПКС-2 Способен проводить разработку и анализ объектов информационной безопасности				
Математические основы криптологии				
Организационно-правовые основы информационной				

безопасности				
Интеллектуальные методы в информационной безопасности				
Компьютерная вирусология				
Моделирование систем информационной безопасности				
Технологии центров обработки данных				
Программирование на языках низкого уровня в задачах защиты информации				
Программно-аппаратная защита информации				
Управление информационной безопасностью				
Стеганографические методы защиты информации				
Алгоритмы цифровой обработки ЦСП в системах управления				
Ознакомительная				
Практика по получению профессиональных умений и опыта научно-исследовательской деятельности				
Научно-исследовательская работа				
Преддипломная				
Выполнение и защита ВКР				

ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОП

Таблица 2

Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**			**Оценочные средства**	
					Текущего контроля	**Промежуточной аттестации**
ПКС-1. Способен использовать методы научных исследований в профессиональной дея тельности	ИПКС-1.2 Использует практические методы научных исследований в профессиональной деятельности	***Знать:*** – методы имитозащиты информации; – принципы работы эволюционных алгоритмов оптимизации и обработки информации	***Уметь:*** – находить и изучать современные методы скрытия информации		Тестирование в системе MOODLE (2 тестирования, в базе каждого тестирования около 10 вопросов), собеседование и отчёты при сдаче лабораторных работ	По результатам накопительного рейтинга или в форме компьютерного тестирования для обучающихся очной формы обучения или в форме традиционного зачёта с оценкой
ПКС-2 Способен проводить разработку и анализ объектов информационной безопасности	ИПКС-2.1 Выполняет анализ угроз информационной безопасности в сетях	**Знать:** -Модели угроз НСД к сетям электросвязи -Методики оценки уязвимостей сетей электросвязи с точки зрения возможности НСД к ним -Средства анализа и контроля защищенности СССЭ -Организационно-технические мероприятия по обеспечению защиты сетей электросвязи от НСД и их	**Уметь:** - Выявлять и оценивать угрозы НСД к сетям электросвязи - Выявлять и оценивать угрозы НСД к сетям электросвязи - Проводить инструментальный мониторинг защищенности СССЭ – встраивать данные в контейнеры; – анализировать контейнеры на предмет наличия	**Владеть:** Навыками выявления угроз НСД к сетям электросвязи; сбором и систематизацией (анализом и оценкой) сведений об угрозах НСД к сетям электросвязи; оценкой уязвимостей сетей электросвязи с точки зрения возможности НСД к ним; выработки предложений по предотвращению и		

		эффективность – основные понятия стеганографии и стеганоанализа; – основные методы встраивания данных в текстовые, графические, аудио и видео-контейнеры; – основные методы анализа контейнеров на предмет наличия скрытых данных	скрытых данных.	нейтрализации угроз НСД к сетям электросвязи, основными методами сокрытия данных в текстовые и основными методами анализа контейнеров на предмет наличия скрытых данных.		

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 4 зач.ед. / 144 часа, распределение часов по видам работ и семестрам представлено в таблице 3.

Формат изучения дисциплины: с использованием элементов электронного обучения.

Таблица 3

Распределение трудоёмкости дисциплины по видам работ по семестрам для обучающихся очной формы обучения

Вид учебной работы	Всего часов	Семестр
		3
1. Контактная работа обучающихся с преподавателем (по видам учебных занятий) **(всего),** в том числе:	**40**	**40**
1.1. Аудиторные занятия (всего), в том числе:	**34**	34
- лекции (Л)	**17**	17
- лабораторные работы (ЛР)	**17**	17
- практические занятия (ПЗ)		
- практикумы (П)		
1.2. Внеаудиторные занятия (всего), в том числе:	**6**	6
- групповые консультации по дисциплине	**6**	6
- групповые консультации по промежуточной аттестации (экзамен)		
- индивидуальная работа преподавателя с обучающимся: - по проектированию: проект (работа) - по выполнению РГР - по выполнению КР - по составлению реферата, доклада, эссе		
2. Самостоятельная работа обучающихся (СРС) (всего)	**68**	**68**
Вид промежуточной аттестации зачёт с оценкой	**Экзамен 36**	**Экзамен 36**
Общая трудоемкость, часы/зачетные единицы	**144 / 4**	**144 / 4**

4.2. Содержание дисциплины, структурированное по темам

Содержание дисциплины, структурированное по темам, приведено в таблице4.2.

Таблица 4

Содержание дисциплины, структурированное по темам
для обучающихся очной формы обучения

Планируемые (контролируемые) результаты освоения: код УК;ОПК; ПКи индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках практической подготовки (трудоемкость в часах)	Наименование разработанного электронного курса (трудоемкость в часах)
		Контактная работа			Самостоятельная работа обучающихся (СРС), час				
		Лекции, час	Лабораторные работы, час	Практические занятия, час					
3 семестр									
ПКС-2, ИПКС-2.1	**Раздел 1** Основы защиты информации					Подготовка к лекциям, тестированию, выполнение заданий для самостоятельной работы. 6.1.1 : разд. 1, 2; 6.1.2 : разд. 1.1, 1.2			
	Тема 1.1. Основные понятия	1			4		Тестирование в системе MOODLE (Тест 1)		
	Тема 1.2. Угрозы безопасности информации	1			6				
	Тема 1.3.Средства защиты	2			6				
	Итого по разделу 1	***4***			***16***				
ПКС-2, ИПКС-2.1	**Раздел 2** Стеганография					Подготовка к лекциям, тестированию, выполнение заданий для самостоятельной работы. 6.1.3 : разд. 1 6.1.4 : стр. 46 – 98 6.1.5 : разд. 1			
	Тема 2.1. История развития стеганографии	1			5		Тестирование в системе MOODLE (Тест 1)		
	Тема 2.2. Основные понятия стеганографии и стеганоанализа	2			5				

Планируемые (контролируемые) результаты освоения: код УК;ОПК; ПКи индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках практической подготовки (трудоемкость в часах)	Наименование разработанного электронного курса (трудоемкость в часах)
		Контактная работа			Самостоятельная работа обучающихся (СРС), час				
		Лекции, час	Лабораторные работы, час	Практические занятия, час					
	Итого по разделу 2	***3***			***10***				
ПКС-2, ИПКС-2.1	**Раздел 3** Методы встраивания данных					Подготовка к лекциям, тестированию, выполнение заданий для самостоятельной работы. 6.1.3 : разд.1.6, 2.1, 3.1, 3.2; 6.1.4 : стр. 46 – 98 6.1.5 : разд. 3, 4, 6, 7, 8			
	Тема 3.1. Методы текстовой стеганографии	2			7		Тестирование в системе MOODLE (Тест 2)		
	Тема 3.2. Методы встраивания данных в неподвижных изображениях	2			7				
	Тема 3.3. Методы встраивания данных в аудиосигналах	2			7				
	Тема 3.4. Методы встраивания данных в видеопоследовательности				7				
	Лабораторная работа № 1 Текстовая стеганография.		3		2	Подготовка отчёта по ЛР № 1 и подготовка к собеседованию по отчёту 6.1.4: стр. 46 - 98	Собеседование по отчёту		
	Лабораторная работа № 2 Встраивание данных в неподвижных изображениях		6		2	Подготовка отчёта по ЛР № 2 и подготовка к собеседованию по отчёту 6.1.4: стр. 46 - 98; 6.1.5: разд. 3, 4, 6, 7	Собеседование по отчёту		
	Лабораторная работа № 3 Встраивание данных в аудиосигналах		4		2	Подготовка отчёта по ЛР № 3 и подготовка к собеседованию по отчёту 6.1.4: стр. 46 - 98;	Собеседование по отчёту		

Планируемые (контролируемые) результаты освоения: код УК;ОПК; ПКи индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках практической подготовки (трудоемкость в часах)	Наименование разработанного электронного курса (трудоемкость в часах)
		Контактная работа			Самостоятельная работа обучающихся (СРС), час				
		Лекции, час	Лабораторные работы, час	Практические занятия, час					
						6.1.5: разд. 8			
	Итого по разделу 3	***6***	***13***		***34***				
ПКС-2, ИПКС-2.1	**Раздел 4** Методы анализа контейнеров на предмет наличия скрытых данных					Подготовка к лекциям, тестированию, выполнение заданий для самостоятельной работы. 6.1.3 : разделы 1.6, 2.2, 3.1, 3.2, 3.4; 6.1.4 : стр. 46 – 98 6.1.5 : разд. 9			
	Тема 4.1. Методы анализа текстовых, графических, аудио- и видеоконтейнеров на предмет наличия скрытых данных	4			6		Тестирование в системе MOODLE (Тест 2)		
	Лабораторная работа № 4 Анализ контейнеров на предмет наличия скрытых данных		4		2	Подготовка отчёта по ЛР № 4 и подготовка к собеседованию по отчёту 6.1.4 : стр. 46 – 98 6.1.5 : разд. 9	Собеседование по отчёту		
	Итого по разделу 4	*4*	***4***		***8***				
	ИТОГО по дисциплине	**17**	**17**		**68**				

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

5.1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

Тесты для текущего и промежуточного контроля знаний обучающихся

Тесты проводятся на электронной платформе Moodle на сайте ДПИ НГТУ по адресу: http://dpingtu.ru/Moodle. Примеры типовых тестовых заданий приведены в разделе 11.1.1 настоящей рабочей программы.

Вопросы для подготовки к контрольным мероприятиям и защите отчётов по лабораторным работам (текущий контроль)

1. Основные понятия защиты информации и информационной безопасности
2. Модель безопасности информации
3. Угрозы доступности
4. Угрозы конфиденциальности
5. Угрозы доступности
6. Какие существуют угрозы безопасности информации?
7. Какие существуют угрозы автоматизированным системам обработки данных?
8. Какие существуют угрозы объектам информационных отношений?
9. Основные направления защиты информации
10. История стеганографии.
11. Техническая стеганография.
12. Лингвистическая стеганография.
13. Основные понятия стеганографии
14. Основные понятия стеганоанализа.
15. Виды атак на стеганографическую систему.
16. Методы встраивания данных в ASCII-текст.
17. Методы встраивания данных в HTML-код.
18. Методы встраивания данных, использующие возможности типографики
19. Примитивные семантические и полуавтоматизированные методы встраивания данных.
20. Синтаксические методы встраивания данных.
21. Методы мимикрии.
22. Форматные методы встраивания данных.
23. Методы встраивания данных в изображения с палитрой.
24. Методы встраивания данных в пространственной области изображения.
25. Методы встраивания данных в частотной области изображения.
26. Методы встраивания данных в видеопоследовательностях.
27. Методы анализа текстовых и графических контейнеров на предмет наличия скрытых данных.
28. Методы анализа аудио- и видео-контейнеров на предмет наличия скрытых данных

Перечень вопросов, выносимых на промежуточную аттестацию (зачёт с оценкой)

1. Основные понятия защиты информации и информационной безопасности
2. Модель безопасности информации
3. Угрозы доступности
4. Угрозы конфиденциальности
5. Угрозы доступности
6. Какие существуют угрозы безопасности информации?
7. Какие существуют угрозы автоматизированным системам обработки данных?

8. Какие существуют угрозы объектам информационных отношений?
9. Основные направления защиты информации
10. История стеганографии.
11. Техническая стеганография.
12. Лингвистическая стеганография.
13. Основные понятия стеганографии
14. Основные понятия стеганоанализа.
15. Виды атак на стеганографическую систему.
16. Методы встраивания данных в ASCII-текст.
17. Методы встраивания данных в HTML-код.
18. Методы встраивания данных, использующие возможности типографики
19. Примитивные семантические и полуавтоматизированные методы встраивания данных.
20. Синтаксические методы встраивания данных.
21. Методы мимикрии.
22. Форматные методы встраивания данных.
23. Методы встраивания данных в изображения с палитрой.
24. Методы встраивания данных в пространственной области изображения.
25. Методы встраивания данных в частотной области изображения.
26. Методы встраивания данных в видеопоследовательностях.
27. Методы анализа текстовых и графических контейнеров на предмет наличия скрытых данных.
28. Методы анализа аудио- и видео-контейнеров на предмет наличия скрытых данных

5.2. Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенции по дисциплине может применяться балльно-рейтинговая система контроля и оценки успеваемости обучающихся очной формы или традиционная система контроля и оценки успеваемости обучающихся. Основные требования балльно-рейтинговой системы по дисциплине и шкала оценивания приведены в таблицах 5 – 7.

Таблица 5

Требования балльно-рейтинговой системы по дисциплине
для обучающихся очной формы обучения

Вид работ	**Количество подвидов работы**	**Макс. баллы за подвид работы**	**Дополнительные и штрафные баллы**	**Макс. количество баллов по виду работ**
1.Тестирование	2	20	0* -1 за повтор (3 попытки)	**40**
2. Выполнение лабораторных работ, в т.ч. на 1 работу	4	8		**32**
- выполнение		*3*	*(-) при наличии ошибок*	*15*
- оформление и защита отчётов		*4*	*(-) отсутствие ответов на вопросы по отчёту*	*20*
3. Посещение занятий	51	0,5	*(+) за сообщение*	**28**
- лекции	*17*			*8,5*
- лабораторныеработы	*34*			*17*
Итого**				**100**

*Если при тестировании верно выполнено менее 55% заданий, то количество баллов за работу приравнивается к «0»

** Освобождение от зачёта с оценкой возможно при условии выполнения всех лабораторных

работ, положительных оценок за тестирование, посещения не менее 50 % занятий.

Таблица 6

Критерии оценивания результата обучения по дисциплине и шкала оценивания

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Критерии оценивания результатов обучения**			
		Оценка **«неудовлетворительно»** 0-54% от max рейтинговой оценки контроля	Оценка **«удовлетворительно»** 55-70% от max рейтинговой оценки контроля	Оценка **«хорошо»** 71-85% от max рейтинговой оценки контроля	Оценка **«отлично»** 86-100% от max рейтинговой оценки контроля
ПКС-1. Способен использовать методы научных исследований в профессиональной деятельности	ИПКС-1.2 Использует практические методы научных исследований в профессиональной деятельности	Изложение учебного материала бессистемное, неполное, не освоены базовые принципы встраивания информации в медиа-контейнеры; не во всех случаях правильно оперирует основными понятиями стеганографии; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципы стеганографии; не во всех случаях находит правильные ответы на задаваемые вопросы по встраиванию информации в медиа-контейнеры	Знает материал на достаточно хорошем уровне; представляет основныеконцепции стеганографии; подтверждает теоретические знания отдельными практическими примерами по встраиванию информации в медиа-контейнеры; дает ответы на задаваемые вопросы	Имеет глубокие знания всего материала по встраиванию информации в медиа-контейнеры; дает развернутые ответы на задаваемые вопросы; имеет собственные суждения о решении задач стеганографической защите данных
ПКС-2 Способен проводить разработку и анализ объектов информационной безопасности	ИПКС-2.1 Выполняет анализ угроз информационной безопасности в сетях	Изложение учебного материала бессистемное, неполное, не знает возможные угрозы безопасности информации, методы внедрения информации и методы анализа контейнеров	Фрагментарные, поверхностные знания в области стеганографии. Изложение полученных знаний неполное, но это не препятствует усвоению последующего материала. Допускаются отдельные существенные ошибки, исправленные с помощью преподавателя. Затруднения при формулировании результатов и их решений	Знает материал на достаточно хорошем уровне; представляет методы внедрения информации и методы анализа контейнеров на наличие внедрённой информации.	Имеет глубокие знания всего материала структуры дисциплины; освоил новации лекционного курса по сравнению с учебной литературой; изложение полученных знаний полное, системное; допускаются единичные ошибки, самостоятельно исправляемые при собеседовании

Таблица 7

Критерии оценивания

Оценка	Критерии оценивания
Высокий уровень «5» (отлично)	оценку **«отлично»** заслуживает обучающийся, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку **«хорошо»** заслуживает обучающийся, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку **«удовлетворительно»** заслуживает обучающийся, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку **«неудовлетворительно»** заслуживает обучающийся, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебная литература

6.1.1. Ковалев, Д. В. Информационная безопасность: учебное пособие / Д.В. Ковалев, Е. А. Богданова. — Ростов-на-Дону: ЮФУ, 2016. — 74 с. — ISBN 978-5-9275-2364-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/114462

6.1.2. Шаньгин, В. Ф. Информационная безопасность: учебное пособие / В.Ф. Шаньгин. — Москва: ДМК Пресс, 2014. — 702 с. — ISBN 978-5-94074-768-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/50578.

6.1.3. Хасанов, Р. И. Основы стеганографии : учебное пособие / Р. И. Хасанов. — Оренбург : ОГУ, 2016. — 101 с. — ISBN 978-5-7410-1555-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/110684.

6.1.4. Голиков, А. М. Методы шифрования информации в сетях и системах радиосвязи : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2012. — 329 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/11380.

6.1.5. Федосеев, В. А. Цифровые водяные знаки и стеганография : учебное пособие / В. А. Федосеев. — 2-е издание, исправленное и дополненное. — Самара : Самарский университет, 2019. — 144 с. — ISBN 978-5-7883-1370-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148589.

Библиотечный фонд укомплектован печатными изданиями из расчета не менее 0,25 экземпляра каждого из изданий, указанных ниже на каждого обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль).

6.2. Методические указания, рекомендации и другие материалы к занятиям

Отсутствуют

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебный процесс по дисциплине обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе

отечественного производства (состав по дисциплине определен в настоящей РПД и подлежит обновлению при необходимости).

Дисциплина, относится к группе дисциплин, в рамках которых предполагается использование информационных технологий как вспомогательного инструмента для выполнения задач, таких как:

- оформление отчетов по лабораторному занятию;
- использование электронной образовательной среды института;
- использование специализированного программного обеспечения;
- организация взаимодействия с обучающимися посредством электронной почты;
- использование видеоконференцсвязи;
- компьютерное тестирование.

7.1. Перечень информационных справочных систем

Таблица 8

Перечень электронных библиотечных систем

№	Наименование ЭБС	Ссылка к ЭБС
1	Консультант студента	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/

7.2. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства необходимого для освоения дисциплины

Таблица 9

Программное обеспечение

№ п/п	Программное обеспечение, используемое в университете на договорной основе	Программное обеспечение свободного распространения
1	MicrosoftWindows 10 (подписка MSDN 700593597, подписка DreamSparkPremium, 19.06.19)	Adobe Acrobat Reader https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader.html
2	Microsoft VISUAL STUDIO 2008 (подписка MSDN 700593597, подписка DreamSparkPremium, 19.06.19)	Visual Studio Code https://code.visualstudio.com/download
3	Microsoft office 2010 (Лицензия № 49487295 от 19.12.2011)	OpenOffice https://www.openoffice.org/ru/
4	Консультант Плюс	Python https://www.python.org

7.3. Перечень современных профессиональных баз данных и информационных справочных систем

В таблице 10 указанперечень профессиональных баз данных и информационных справочных систем, к которым обеспечен доступ (удаленный доступ). Данный перечень подлежит обновлению в соответствии с требованиями ФГОС ВО.

Таблица 10

Перечень современных профессиональных баз данных и информационных справочных систем

№ п/п	Наименование профессиональной базы данных, информационно-справочной системы	Доступ к ресурсу (удаленный доступ с указанием ссылки/доступ из локальной сети университета)
1	База данных стандартов и регламентов РОССТАНДАРТ	https://www.gost.ru/portal/gost //home/standarts
2	Перечень профессиональных баз данных и	https://cyberpedia.su/21x47c0.html

	информационных справочных систем	
3	Инструменты и веб-ресурсы для веб-разработки – 100+	https://techblog.sdstudio.top/blog/instrumenty-i-veb-resursy-dlia-veb-razrabotki-100-plus
4	Справочная правовая система «КонсультантПлюс»	доступ из локальной сети

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 11 указан перечень образовательных ресурсов, имеющих формы, адаптированные к ограничениям их здоровья, а также сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования.

Таблица 11

Образовательные ресурсы для инвалидов и лиц с ОВЗ

№	Перечень образовательных ресурсов, приспособленных для использования инвалидами и лицами с ОВЗ	Сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования
1	ЭБС «Консультант студента»	озвучка книг и увеличение шрифта
2	ЭБС «Лань»	специальное мобильное приложение - синтезатор речи, который воспроизводит тексты книг и меню навигации
3	ЭБС «Юрайт»	версия для слабовидящих

Согласно Федеральному Закону об образовании 273-ФЗ от 29.12.2012 г. ст. 79, п.8 "Профессиональное обучение и профессиональное образование обучающихся с ограниченными возможностями здоровья осуществляются на основе образовательных программ, адаптированных при необходимости для обучения указанных обучающихся". АОП разрабатывается по каждой направленности при наличии заявлений от обучающихся, являющихся инвалидами или лицами с ОВЗ и изъявивших желание об обучении по данному типу образовательных программ.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные аудитории для проведения занятий по дисциплине, оснащены оборудованием и техническими средствами обучения.

В таблице 12 перечислены:

- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения;
- помещения для самостоятельной работы обучающихся, которые должны быть оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ДПИ НГТУ.

Таблица 12

Оснащенность аудиторий и помещений
для самостоятельной работы обучающихся по дисциплине

№	Наименование аудиторий и помещений для самостоятельной работы	Оснащенность аудиторий помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа

№	Наименование аудиторий и помещений для самостоятельной работы	Оснащенность аудиторий помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	**1448** Учебный кабинет, мультимедийный класс; Нижегородская обл., г. Дзержинск, ул. Гайдара, д. 49	Оснащён мультимедийным оборудованием: Проектор EPSON EB-FH06 HDMI 1920x1080 Ноутбук Intel Core i3/Ram 4 Gb/HDD 240 Gb/Intel HD	–
2	**1440** Компьютерный класс; Нижегородская обл., г. Дзержинск, ул. Гайдара, д. 49	ОснащёнПК,CPU Intel core i5-10400/Ram 16 Gb/SSD 500 Gb/ Intel UHD Graphics 630 – 16 шт.	• Microsoft Windows 10 (подписка DreamSpark Premium) • Apache OpenOffice 4.1.8(свободное ПО); • Mozilla Firefox(свободное ПО); • Adobe Acrobat Reader (свободное ПО); • 7-zip для Windows (свободное ПО); • КонсультантПлюс (ГПД № 0332100025418000079 от 21.12.2018)
3	**1234** Научно-техническая библиотека ДПИ НГТУ, студенческий читальный зал; Нижегородская обл., г. Дзержинск, ул. Гайдара, д. 49	Комплект демонстрационного оборудования: • ПК, с выходом на мультимедийный проектор, на базе Intel Pentium G4560 3.5 Ггц, 4 Гб ОЗУ, монитор 20’ – 1шт. • Мультимедийный проектор Epson- 1 шт; • Экран – 1 шт.; Набор учебно-наглядных пособий	• MicrosoftWindows 10 Домашняя (поставка с ПК) • LibreOffice 6.1.2.1. (свободное ПО) • Foxit Reader (свободное ПО); • 7-zip для Windows (свободное ПО)
4	**1443а** компьютерный класс - помещение для СРС, курсового проектирования (выполнения курсовых работ), Нижегородская обл., г. Дзержинск, ул. Гайдара, д. 49	ПК на базе IntelCeleron 2.67 ГГц, 2 Гб ОЗУ, монитор Acer 17’ – 4 шт. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета	• Microsoft Windows 7 (подписка DreamSpark Premium) • Apache OpenOffice 4.1.8(свободное ПО); • Mozilla Firefox(свободное ПО); • Adobe Acrobat Reader (свободное ПО); • 7-zip для Windows (свободное ПО); • КонсультантПлюс(ГПД № 0332100025418000079 от 21.12.2018)

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

10.1. Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

Контактная работа: аудиторная, внеаудиторная, а также проводиться в электронной информационно-образовательной среде университета (далее - ЭИОС).

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- балльно-рейтинговая технология оценивания;
- текущий контроль знаний в форме тестирования в среде MOODLE.

При преподавании дисциплины «Стеганографические методы защиты информации» используются современные образовательные технологии, позволяющие повысить

активность обучающихся при освоении материала курса и предоставить им возможность эффективно реализовать часы самостоятельной работы.

Лекционный материал курса сопровождается компьютерными презентациями, в которых наглядно преподносятся материал различных разделов курса и что дает возможность обсудить материал с обучающимися во время чтения лекций, активировать их деятельность при освоении материала. Материалы лекций в виде слайдов находятся в свободном доступе в системе MOODLE и могут быть получены до чтения лекций и проработаны обучающимися в ходе самостоятельной работы.

На лекциях, лабораторных занятиях реализуются интерактивные технологии, приветствуются вопросы и обсуждения, используется личностно-ориентированный подход, технология работы в малых группах, что позволяет обучающимся проявить себя, получить навыки самостоятельного изучения материала, выровнять уровень знаний в группе.

Все вопросы, возникшие при самостоятельной работе над домашним заданием, подробно разбираются на лабораторных занятиях и лекциях. Проводятся индивидуальные и групповые консультации с использованием, как встреч с обучающимися, так и современных информационных технологий (электронная почта, Zoom).

Инициируется активность обучающихся, поощряется задание любых вопросов по материалу, практикуется индивидуальный ответ на вопросы обучающегося, рекомендуются методы успешного самостоятельного усвоения материала в зависимости от уровня его базовой подготовки.

Для оценки знаний, умений, навыков и уровня сформированности компетенции применяется балльно-рейтинговая система контроля и оценки успеваемости обучающихся очной формы обучения в процессе текущего контроля.

Промежуточная аттестация проводится в форме зачёта с оценкой с учетом текущей успеваемости.

Результат обучения считается сформированным на повышенном уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях обучающийся исчерпывающе, последовательно, четко и логически излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, использует в ответе дополнительный материал. Все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, обучающийся способен анализировать полученные результаты, проявляет самостоятельность при выполнении заданий.

Результат обучения считается сформированным на пороговом уровне, если теоретическое содержание курса освоено полностью. При устных собеседованиях обучающийся последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, обучающийся способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий.

Результат обучения считается несформированным, если обучающийся при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже трех по оценочной системе, что соответствует допороговому уровню.

10.2. Методические указания для занятий лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках

каждой темы дисциплины (Таблица 4). Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

10.3. Методические указания по освоению дисциплины на лабораторных работах

Подготовку к каждой лабораторной работе обучающийся должен начать с ознакомления с планом занятия, который отражает содержание предложенной темы. Каждая выполненная работа с оформленным отчетом подлежит защите у преподавателя.

При оценивании лабораторных работ учитывается следующее:

- качество выполнения экспериментально-практической части работы и степень соответствия результатов работы заданным требованиям;
- качество оформления отчета по работе;
- качество устных ответов на контрольные вопросы при защите работы.

10.4. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающихся к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающихся на занятиях, в качестве выполненных заданий для самостоятельной работы и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы, представленной в Разделе 6.

В процессе самостоятельной работы при изучении дисциплины обучающиеся могут работать на компьютере в специализированных аудиториях для самостоятельной работы (указано в таблице 9.1). В аудиториях имеется доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде университета (ЭИОС) и электронной библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении дисциплины.

11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

11.1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе текущего контроля успеваемости

Для текущего контроля знаний обучающихся по дисциплине проводится **комплексная оценка знаний,** включающая

- тестирование на сайте преподавателя по различным разделам курса;
- проведение лабораторных работ;
- ответы на вопросы для самостоятельной работы для обучающихся очной формы.

Далее для всех форм текущего контроля приведены примеры оценочных средств.

11.1.1. Типовые тестовые задания

Тестирование проводится в системе MOODLE. По приведённым в таблице 4.2 темам проводится два теста. В разделе приведены примеры тестовых заданий для каждого теста по всем темам.

Тест 1

Раздел 1

1. Суть компрометации информации

– внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации

– несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений

– *внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений*

2. Основные угрозы доступности информации:

– непреднамеренные ошибки пользователей
– злонамеренное изменение данных
– хакерская атака
– *отказ программного и аппаратного обеспечения*
– перехват данных

3. К формам защиты информации не относится…

– *аналитическая*
– правовая
– организационно-техническая
– криптографическая

Раздел 2

1. Ранее к методам стеганографии относилось ...

– письмо на восковых табличках
– газетный код
– *все перечисленное*
– татуировка на голове раба

2. Наука о скрытой передаче информации путем скрытия самого факта передачи информации называется ...

– *стеганографией*
– криптографией
– стегоанализом
– криптоанализом

3. Укажите основные характеристики цифрового водяного знака:

– *прозрачность*
– *безопасность*
– *надежность*
– глубина кодирования
– дискретность
– разрядность
– *обратимость*

4. Что такое Стеганография?

– Это наука о шифровании данных.
– *Это наука о скрытой передачи информации.*
– Это наука о методах получения доступа к зашифрованной информации без знания секретного ключа.
– Это наука о выявлении факта передачи скрытой информации в анализируемом сообщении

Тест 2

Раздел 3

1. В текстовый документ, содержащий 11 слов, были внедрены биты секретного

сообщения путем использования различных видов пробелов. Стандартный пробел кодирует 0, а неразрывный пробел кодирует 1.

Какое наибольшее десятичное целое число может быть секретно передано с помощью этого документа?

– *1023*
– 1024
– 10
– 9

2. Произведена стеганография черно-белого изображения (256 оттенков серого) методом замены младшего бита файла.

Во сколько раз число неизменившихся битов файла-контейнера больше числа битов, кодирующих засекреченное сообщение?

– *7*
– 256
– 8
– Невозможно рассчитать

3. Стеганография звуковых файлов осуществляется путем ...

– преобразования стерео в моно
– транспонирования аккордов мелодии
– уменьшения частоты дискретизации
– *замены младших битов кода амплитуды сигнала*

4. Простейшая стеганография изображений основана на ...

– инвертировании схемы RGB
– размытии изображения
– *замене младших битов в коде цвета пикселей*
– коррекции насыщенности и контрастности изображения

5. Метод замены младших битов при стеганографии изображений не может применяться к файлам с расширением ...

– bmp
– png
– *jpeg*
– метод замены младших битов применим к изображениям с любыми расширениями

Раздел 4

1. Что такое контейнер (в стеганографическом смысле)?

– *Любая информация, используемая для сокрытия тайного сообщения.*
– Информация, подлежащая сокрытию.
– Секретный ключ, нужный для сокрытия информации
– Такой термин в стеганографии не используется.

2. Что такое стеганоанализ?

– Это наука о шифровании данных.
– Это наука о скрытой передачи информации.
– Это наука о методах получения доступа к зашифрованной информации без знания секретного ключа.
– *Это наука о выявлении факта передачи скрытой информации в анализируемом сообщении*

3. К атакам на системы цифровых водяных знаков относят

– *Атаки против встроенного сообщения*
– Атака на основании известного пустого контейнера.
– Атака на основании известной математической модели контейнера или его части

– Атака на основании известного заполненного контейнера

11.1.2. Типовые задания для лабораторных работ

Лабораторная работа 1

Типовое задание.

Изучить возможности и методы текстовой стеганографии.

Лабораторная работа 2

Изучить возможности и методы встраивания данных в неподвижных изображениях.

Лабораторная работа 3

Типовое задание.

Изучить возможности и методы встраивания данных в аудиосигналах.

Лабораторная работа 4

Типовое задание.

Выполнить анализ контейнеров на предмет наличия скрытых данных.

11.1.3. Типовые вопросы для устного и письменного опроса обучающихся очной формы обучения

По завершении лекционных занятий может быть выполнен устный или письменный опрос обучающихся для оценки работы на занятии и для оценки самостоятельной работы обучающихся.

Раздел 1

1. Основные понятия защиты информации и информационной безопасности
2. Модель безопасности информации
3. Угрозы доступности
4. Угрозы конфиденциальности
5. Угрозы доступности
6. Какие существуют угрозы безопасности информации?
7. Какие существуют угрозы автоматизированным системам обработки данных?
8. Какие существуют угрозы объектам информационных отношений?
9. Основные направления защиты информации

Раздел 2

1. История стеганографии.
2. Техническая стеганография.
3. Лингвистическая стеганография.
4. Основные понятия стеганографии
5. Основные понятия стеганоанализа.
6. Виды атак на стеганографическую систему.

Раздел 3

1. Методы встраивания данных в ASCII-текст.
2. Методы встраивания данных в HTML-код.
3. Методы встраивания данных, использующие возможности типографики
4. Примитивные семантические и полуавтоматизированные методы встраивания данных.
5. Синтаксические методы встраивания данных.
6. Методы мимикрии.
7. Форматные методы встраивания данных.
8. Методы встраивания данных в изображения с палитрой.
9. Методы встраивания данных в пространственной области изображения.
10. Методы встраивания данных в частотной области изображения.
11. Методы встраивания данных в видеопоследовательностях.

Раздел 4

1. Методы анализа текстовых и графических контейнеров на предмет наличия скрытых данных.
2. Методы анализа аудио- и видео-контейнеров на предмет наличия скрытых данных

11.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе промежуточной аттестации по дисциплине

Форма проведения промежуточной аттестации по дисциплине: зачёт с оценкой (по результатам накопительного рейтинга или в форме компьютерного тестирования).

Структура теста для итогового тестирования: в итоговом тесте 10 вопросов: 9 вопросов с выбором ответа и один вопрос открытого типа.

Перечень вопросов для подготовки к зачёту с оценкой (ПКС-2, ИПКС-2.1)

Перечень вопросов, выносимых на промежуточную аттестацию, приведён в разделе 5.1 настоящей рабочей программы.

Примерный тест для итогового тестирования (ПКС-2, ИПКС-2.1)

1. Основные угрозы доступности информации:
- непреднамеренные ошибки пользователей
- злонамеренное изменение данных
- хакерская атака
- отказ программного и аппаратного обеспечения
- перехват данных

2. К формам защиты информации не относится…
- аналитическая
- правовая
- организационно-техническая
- криптографическая

3. Наука о скрытой передаче информации путем скрытия самого факта передачи информации называется ...
- стеганографией
- криптографией
- стегоанализом
- криптоанализом

4. Укажите основные характеристики цифрового водяного знака:
- прозрачность
- безопасность
- надежность
- глубина кодирования
- дискретность
- разрядность
- обратимость

5. Стеганография звуковых файлов осуществляется путем ...
- преобразования стерео в моно
- транспонирования аккордов мелодии
- уменьшения частоты дискретизации
- замены младших битов кода амплитуды сигнала

6. Простейшая стеганография изображений основана на ...
- инвертировании схемы RGB

– размытии изображения
– замене младших битов в коде цвета пикселей
– коррекции насыщенности и контрастности изображения

7. Метод замены младших битов при стеганографии изображений не может применяться к файлам с расширением ...
– bmp
– png
– jpeg
– метод замены младших битов применим к изображениям с любыми расширениями

8. Что такое контейнер (в стеганографическом смысле)?
– Любая информация, используемая для сокрытия тайного сообщения.
– Информация, подлежащая сокрытию.
– Секретный ключ, нужный для сокрытия информации
– Такой термин в стеганографии не используется.

9. Что такое стеганоанализ?
– Это наука о шифровании данных.
– Это наука о скрытой передачи информации.
– Это наука о методах получения доступа к зашифрованной информации без знания секретного ключа.
– Это наука о выявлении факта передачи скрытой информации в анализируемом сообщении

Открытый вопрос (ПКС-2, ИПКС-2.1)

10. Методы встраивания данных, использующие возможности типографики

Регламент проведения текущего контроля в форме компьютерного тестирования

Кол-во заданий в банке вопросов	**Кол-во заданий, предъявляемых обучающемуся**	**Время на тестирование, мин.**
не менее 100	**10**	**40**

Полный фонд оценочных средств для проведения промежуточной аттестации в форме компьютерного тестирования размещен в банке вопросов данного курса дисциплины в СДО MOODLE.