Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 09.04.01 Информатика и вычислительная техника

Наименование образовательной программы: Автоматизированные системы обработки информации и управления

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Рабочая программа дисциплины
ЦИФРОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.02**
Трудоемкость в зачетных единицах:	**1 семестр - 5;**
Часов (всего) по учебному плану:	**180 часов**
Лекции	**1 семестр - 16 часов;**
Практические занятия	**не предусмотрено учебным планом**
Лабораторные работы	**1 семестр - 32 часа;**
Консультации	**1 семестр - 18 часов;**
Самостоятельная работа	**1 семестр - 109,2 часов;**
в том числе на КП/КР	**1 семестр - 15,7 часов;**
Иная контактная работа	**1 семестр - 4 часа;**
включая: **Интервью** **Лабораторная работа** **Тестирование**	
Промежуточная аттестация:	
Защита курсовой работы **Экзамен**	**1 семестр - 0,3 часа;** **1 семестр - 0,5 часа;** **всего - 0,8 часа**

Москва 2020

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Рытов А.А. Идентификатор: R37263e31-RytovAA-c7235577	А.А. Рытов
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Вишняков С.В. Идентификатор: R35b26072-VishniakovSV-02810d9	С.В. Вишняков
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Вишняков С.В. Идентификатор: R35b26072-VishniakovSV-02810d9	С.В. Вишняков
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: изучение современных способов защиты информации, в том числе интеллектуальной собственности, на основе методов компьютерной стеганографии

Задачи дисциплины

- освоение методов проектирования основных типов стеганографических систем;
- изучение методов и алгоритмов формирования цифровых водяных знаков в пространственной области и области преобразования;
- анализ возможностей защиты медиафайлов на базе современных методов цифровой обработки сигналов;
- приобретение навыков применения методов стегоанализа.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ПК-2 Способен осуществлять проектирование защищенных информационных систем	ИД-1$_{ПК-2}$ Демонстрирует знание нормативной базы, методов описания, анализа и проектирования в области обеспечения безопасности информационных систем	знать: - протоколы эллиптической криптографии, стандарты ЭЦП на эллиптических кривых. уметь: - применять системы ЭЦП на основе эллиптических кривых для защиты информации.
ПК-2 Способен осуществлять проектирование защищенных информационных систем	ИД-2$_{ПК-2}$ Демонстрирует знание методов и средств предотвращения утечки информации за счет побочных электромагнитных излучений и наводок	знать: - методы реализации стеганографических систем в пространственной области, а также с применением дискретного косинусного, вейвлет и фрактального преобразований. уметь: - – применять форматные и неформатные способы сокрытия информации для встраивания цифровых водяных знаков в медиа-контейнерах.
ПК-2 Способен осуществлять проектирование защищенных информационных систем	ИД-3$_{ПК-2}$ Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем	знать: - – источники научно-технической информации (журналы, сайты Интернет) по теме дисциплины; алгоритмы встраивания и извлечения конфиденциальной информации, а также стеганоанализа мультимедиа-контейнеров. уметь: - разрабатывать системы цифровой стеганографии для защиты объектов интеллектуальной собственности;

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		проводить исследования и оценку эффективности стеганографических систем..

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Автоматизированные системы обработки информации и управления (далее – ОПОП), направления подготовки 09.04.01 Информатика и вычислительная техника, уровень образования: высшее образование - магистратура.

Требования к входным знаниям и умениям:

- знать Методы и средства защиты информации
- знать Защита информации
- знать Цифровая обработка сигналов
- уметь инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем и подсистем их защиты
- уметь использовать современные информационные технологии при решении задач защиты информации; формализовать задачу по защите информации; применять стандарты по оценке защищенности АСОИ при анализе и проектировании систем защиты информации в АСОИ
- уметь обосновывать принимаемые проектные решения; применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач, разрабатывать модели открытого текста различного уровня сложности; проводить обработку открытого текста для подготовки к операциям шифрования
- уметь осуществлять постановку и выполнять эксперименты по проверке корректности принимаемого проектного решения и его эффективности
- уметь использовать современные инструментальные средства и технологии программирования

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Эллиптическая криптография	46	1	6	12	-	-	-	-	-	-	28	-	***Подготовка к аудиторным занятиям:*** Защита лабораторной работы №2,КЗ31 - [2], стр. 76-93; [3], стр. 208 –230; ***Подготовка к аудиторным занятиям:*** Защита лабораторной работы №1 - [1], стр. 82 – 111; [4], стр. 298 –313; ***Изучение материалов литературных источников:*** [1], стр. 82 – 111 [2], стр. 76-93 [3], стр. 298 –313
1.1	Эллиптическая криптография	46		6	12	-	-	-	-	-	-	28	-	
2	Стеганография	62		10	20	-	-	-	-	-	-	32	-	***Подготовка к аудиторным занятиям:*** Защиты лабораторных работ№5,6,КЗ32 стр. 190 – 286 ***Подготовка к аудиторным занятиям:*** Защита лабораторной работы №4 - [5], стр. 56 – 83; ***Изучение материалов литературных источников:*** [4], стр. 1-24 [5], п. 1, 5, 6 [6], п. 1,2,3
2.1	Стеганография	62		10	20	-	-	-	-	-	-	32	-	
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Курсовая работа (КР)	36.0		-	-	-	16	-	4	-	0.3	15.7	-	
	Всего за семестр	**180.0**		**16**	**32**	**-**	**16**	**2**	**4**	**-**	**0.8**	**75.7**	**33.5**	
	Итого за семестр	**180.0**		**16**	**32**	**-**	**18**		**4**		**0.8**	**109.2**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Эллиптическая криптография

1.1. Эллиптическая криптография

Поля. Основные понятия. Кольцо многочленов. Эллиптические кривые. Геометрия эллиптических кривых. Закон сложения точек эллиптической кривой. Арифметика по модулю неприводимых многочленов. Сложение точек эллиптических кривых для полей Галуа характеристики 2. Построение односторонней функции на основе эллиптической кривой. Алгоритмы вычисления кР. Протоколы эллиптической криптографии. Распределение ключей для классической криптосистемы (протокол Massey-Omura). Протокол распределения ключей Менезеса-Кью-Ванстона. ГОСТ Р 34.10-2001. Область применения. Определения и обозначения. Общие положения. Математические соглашения. Инвариант эллиптической кривой. Параметры цифровой подписи. Контрольный пример..

2. Стеганография

2.1. Стеганография

Обзор литературы. Классификация стеганографических методов. Структурная схема и математическая модель типичной стеганосистемы. Алгоритм встраивания сообщения. Цифровая стеганография. Свойства зрения, используемые при построении стегоалгоритмов. Цветовое зрение. Законы смешения цветов. Диаграмма цветности. Цветовые модели. Форматы графических файлов BMP. Форматные методы сокрытия в файлах BMP. Неформатные методы сокрытия в графических изображениях – пространственная область. Методы замены. Метод замены наименьшего значащего бита (НЗБ). Метод случайного интервала. Метод псевдослучайной перестановки. Метод блочного сокрытия. Метод квантования изображений. Методы замены палитры. Алгоритмы встраивания ЦВЗ в пространственной области. Алгоритм “Kutter”. Алгоритм ДДКМ. Алгоритм «Langelaar».Инструментальные средства встраивания ЦВЗ в пространственную область. Программы S-TOOLS, AISWPP20, ImageBridgeReader, Stego, bmp.exe, Watermark. Алгоритмы встраивания ЦВЗ в области преобразования. Алгоритм сжатия JPEG. Дискретное косинусное преобразование. Алгоритм «LangelaarDCT». Алгоритм «Barni». Алгоритм «Cox». Алгоритм «Koch». Алгоритм «Fridrich». Методы встраивания данных в области преобразования. Дискретное вейвлет - преобразование.Алгоритм «Corvi». Алгоритм «Kundur-1». Алгоритм «Barni - DWT». Алгоритм «Chae» Методы встраивания данных с использованием фрактального преобразования. Методы стеганоанализа мультимедиа-контейнеров. Метод определения порога обнаружения. Основные задачи построения систем распознавания. Вероятностные методы распознавания. Метод моментов. Методы контроля искажений, вносимых стеганографическими системами. Метрические пространства. Свойства функций расстояния. Метрики искажения растровых изображений. Методы стеганоанализа. Метод анализа пар значений. Анализ числа близких цветовых пар в палитре изображения. Метод учета двойственных статистик..

3.3. Темы практических занятий

не предусмотрено

3.4. Темы лабораторных работ

1. Исследование свойств эллиптических кривых 19;
2. Использование группы точек эллиптической кривой в протоколе Диффи-Хеллмана 25;
3. Сокрытие информации в текстовом документе методом изменения формата текста 31;

4. Алгоритм встраивания ЦВЗ "Bruyndonckx" 17;
5. Встраивание невидимого ЦВЗ в пространственной области 40;
6. Встраивание видимого ЦВЗ в пространственной области
Цветовая модель RGB 40.

3.5 Консультации

Аудиторные консультации по курсовому проекту/работе (КПР)

1. Обсуждение особенностей реализации протоколов ЭЦП
2. Обсуждение особенностей методов встраивания информации в пространственной области

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Эллиптическая криптография"
2. Обсуждение материалов по кейсам раздела "Стеганография"

3.6 Тематика курсовых проектов/курсовых работ

1 Семестр

Курсовая работа (КР)
Темы:
- Эллиптическая криптография
- Защита интеллектуальной собственности методами стеганографии
- Электронно-цифровая подпись

График выполнения курсового проекта

Неделя	1 - 4	5 - 8	9 - 10	11 - 12	13 - 14	Зачетная
Раздел курсового проекта	1	1	1	2	2	Защита курсового проекта
Объем раздела, %	5	45	10	5	35	-
Выполненный объем нарастающим итогом, %	5	50	60	65	100	-

Номер раздела	Раздел курсового проекта
1	Часть 1 Разработка программной реализации электронно-цифровой подписи
2	Часть 2 Встраивание информации из студенческого билета в контейнер-изображение

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)		Оценочное средство (тип и наименование)
		1	2	
Знать:				
протоколы эллиптической криптографии, стандарты ЭЦП на эллиптических кривых	ИД-1$_{ПК-2}$	+		Лабораторная работа/Контроль выполнения комплекса лабораторных работ №1-2 по курсу МСЗИ Модуль 1 (25%) Тестирование/Контрольно-зачетное занятие (К331) по курсу МСЗИ Модуль 1 (65%) Интервью/Контроль посещения лекций №1-2 по курсу ЦТЗИ Модуль 1 (10%)
методы реализации стеганографических систем в пространственной области, а также с применением дискретного косинусного, вейвлет и фрактального преобразований	ИД-2$_{ПК-2}$		+	Лабораторная работа/Контроль выполнения комплекса лабораторных работ №3- 6 по курсу ЗИ Модуль 2 (25%) Тестирование/Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) Интервью/Контроль посещения лекций № 3-8 по курсу ЦТЗИ Модуль 2 (10%)
– источники научно-технической информации (журналы, сайты Интернет) по теме дисциплины; алгоритмы встраивания и извлечения конфиденциальной информации, а также стеганоанализа мультимедиа-контейнеров	ИД-3$_{ПК-2}$		+	Лабораторная работа/Контроль выполнения комплекса лабораторных работ №3- 6 по курсу ЗИ Модуль 2 (25%) Тестирование/Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) Интервью/Контроль посещения лекций № 3-8 по курсу ЦТЗИ Модуль 2 (10%)
Уметь:				
применять системы ЭЦП на основе эллиптических кривых	ИД-1$_{ПК-2}$	+		Лабораторная работа/Контроль выполнения

для защиты информации				комплекса лабораторных работ №1-2 по курсу МСЗИ Модуль 1 (25%) Тестирование/Контрольно-зачетное занятие (К331) по курсу МСЗИ Модуль 1 (65%) Интервью/Контроль посещения лекций №1-2 по курсу ЦТЗИ Модуль 1 (10%)
– применять форматные и неформатные способы сокрытия информации для встраивания цифровых водяных знаков в медиа-контейнерах	ИД-2$_{ПК-2}$		+	Лабораторная работа/Контроль выполнения комплекса лабораторных работ №3- 6 по курсу ЗИ Модуль 2 (25%) Тестирование/Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) Интервью/Контроль посещения лекций № 3-8 по курсу ЦТЗИ Модуль 2 (10%)
разрабатывать системы цифровой стеганографии для защиты объектов интеллектуальной собственности; проводить исследования и оценку эффективности стеганографических систем.	ИД-3$_{ПК-2}$		+	Лабораторная работа/Контроль выполнения комплекса лабораторных работ №3- 6 по курсу ЗИ Модуль 2 (25%) Тестирование/Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) Интервью/Контроль посещения лекций № 3-8 по курсу ЦТЗИ Модуль 2 (10%)

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

1 семестр

Форма реализации: Компьютерное задание

1. Контроль выполнения комплекса лабораторных работ №1-2 по курсу МСЗИ Модуль 1 (25%) (Лабораторная работа)
2. Контроль выполнения комплекса лабораторных работ №3- 6 по курсу ЗИ Модуль 2 (25%) (Лабораторная работа)
3. Контрольно-зачетное занятие (К331) по курсу МСЗИ Модуль 1 (65%) (Тестирование)
4. Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) (Тестирование)

Форма реализации: Смешанная форма

1. Контроль посещения лекций № 3-8 по курсу ЦТЗИ Модуль 2 (10%) (Интервью)
2. Контроль посещения лекций №1-2 по курсу ЦТЗИ Модуль 1 (10%) (Интервью)

Балльно-рейтинговая структура дисциплины является приложением А.
Балльно-рейтинговая структура курсовой работы является приложением Б.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №1)

Итоговая оценка по курсу может быть рассчитана как среднее от текущей успеваемости и итогов промежуточной аттестации по 100 балльной шкале. Текущая успеваемость также рассчитывается как среднее по трем модулям по 100 бальной шкале. Только после этого можно переходить к 5-и балльной шкале. Промежуточное округление оценок в 5-и балльной системе и нелинейная шкала оценок в БАРС приводят к существенному завышению результирующих оценок.

Курсовая работа (КР) (Семестр №1)

Среднее по оценкам защиты и текущей успеваемости

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы / А. А. Болотов, и др. – 3-е изд., испр. и доп . – М. : Эдиториал УРСС, 2019 . – 376 с. – (Основы защиты информации ; № 3) . - ISBN 978-5-9710-5780-2 .;
2. Болотов, А. А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / А. А. Болотов, С. Б. Гашков, А. Б. Фролов . – 3-е изд., испр. и доп . – М. : Эдиториал УРСС, 2019 . – 376 с. – (Основы защиты информации ; № 4) . - ISBN 978-5-9710-5813-7 .;
3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата вузов по инженерно-техническим направлениям / И. Н. Васильева, С.-Петерб. гос. экономич. ун-т . – М. : Юрайт, 2017 . – 349 с. – (Бакалавр. Академический курс) . - ISBN 978-5-534-02883-6 .;

4. Рытов, А. А. Разработка биометрического идентификатора с электронно-цифровой подписью : методическое пособие по выполнению курсовой работы / А. А. Рытов, Нац. исслед. ун-т "МЭИ" . – М. : Изд-во МЭИ, 2017 . – 24 с. http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=8884;
5. В. Г. Грибунин, И. Н. Оков, И. В. Туринцев- "Цифровая стеганография", Издательство: "СОЛОН-ПРЕСС", Москва, 2009 - (264 с.) https://biblioclub.ru/index.php?page=book&id=117549;
6. Стеганография, цифровые водяные знаки и стеганоанализ / А. В. Аграновский, [и др.] . – М. : Вузовская книга, 2009 . – 220 с. - ISBN 978-5-9502-0401-2 ..

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. Office;
2. Windows;
3. Acrobat Reader;
4. Mathematica.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
2. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	З-505, Учебная аудитория каф. "ВМСС"	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
Учебные аудитории для проведения практических занятий, КР и КП	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	З-505, Учебная аудитория каф. "ВМСС"	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
Учебные аудитории для проведения лабораторных занятий	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	З-506, Аналоговые и цифровые системы обработки и передачи информации	стол преподавателя, стул, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, лабораторный стенд, сервер, компьютер персональный, инвентарь специализированный
Учебные аудитории для проведения промежуточной аттестации	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
	З-505, Учебная аудитория каф. "ВМСС"	парта, стол преподавателя, стул, мультимедийный проектор, экран, доска маркерная, компьютер персональный
Помещения для самостоятельной	З-502, Компьютерный класс каф. "ВМСС"	стол преподавателя, стол компьютерный, стул, компьютерная сеть с выходом в

работы		Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный
Помещения для консультирования	Е-522/5, Кабинет сотрудников каф. "ВМСС"	
	Е-522/8, Учебная аудитория каф. "ВМСС"	парта, стол преподавателя, стул, доска меловая
	З-508, Кабинет сотрудников каф. "ВМСС"	
Помещения для хранения оборудования и учебного инвентаря	Е-403, Склад	стол для работы с документами, шкаф, шкаф для документов
	З-308, Помещение для инвентаря	

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Цифровые технологии защиты информации

(название дисциплины)

1 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-1 Контроль посещения лекций №1-2 по курсу ЦТЗИ Модуль 1 (10%) (Интервью)
КМ-2 Контроль выполнения комплекса лабораторных работ №1-2 по курсу МСЗИ Модуль 1 (25%) (Лабораторная работа)
КМ-3 Контрольно-зачетное занятие (К331) по курсу МСЗИ Модуль 1 (65%) (Тестирование)
КМ-4 Контроль посещения лекций № 3-8 по курсу ЦТЗИ Модуль 2 (10%) (Интервью)
КМ-5 Контроль выполнения комплекса лабораторных работ №3- 6 по курсу ЗИ Модуль 2 (25%) (Лабораторная работа)
КМ-6 Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) (Тестирование)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5	КМ-6
		Неделя КМ:	4	4	8	14	14	16
1	Эллиптическая криптография							
1.1	Эллиптическая криптография		+	+	+			
2	Стеганография							
2.1	Стеганография					+	+	+
Вес КМ, %:			5	12,5	32,5	5	12,5	32,5

Приложение Б

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Цифровые технологии защиты информации

(название дисциплины)

1 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по курсовой работе:

КМ-1 Разработка модуля умножения точки ЭК на константу; Разработка модуля расчета порядка точки ЭК.
КМ-2 Поиск ЭК и базовой точки по заданным параметрам
КМ-3 Разработка модуля расчета и верификации ЭЦП.
КМ-4 Разработка модуля подготовки данных.
КМ-5 Разработка модуля встраивания ЦВЗ в изображение – контейнер.

Вид промежуточной аттестации – защита КР.

Номер раздела	Раздел курсового проекта/курсовой работы	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5
		Неделя КМ:	4	8	10	12	14
1	Часть 1 Разработка программной реализации электронно-цифровой подписи		+	+	+		
2	Часть 2 Встраивание информации из студенческого билета в контейнер-изображение					+	+
		Вес КМ, %:	5	45	10	5	35