

**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

**Оценочные материалы
по дисциплине
Цифровые технологии защиты информации**

**Москва
2023**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:


Разработчик

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Рытов А.А.
	Идентификатор	R37263e31-RytovAA-c7235577

А.А. Рытов


СОГЛАСОВАНО:

Руководитель
образовательной
программы

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Зейн А.Н.
	Идентификатор	R54353a8f-ZeynAIN-7d1f3849

А.Н. Зейн

Заведующий
выпускающей кафедрой

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Вишняков С.В.
	Идентификатор	R35b26072-VishniakovSV-02810d9

С.В.
Вишняков

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

- ПК-2 Способен осуществлять проектирование защищенных информационных систем
ИД-1 Демонстрирует знание нормативной базы, методов описания, анализа и проектирования в области обеспечения безопасности информационных систем
ИД-2 Демонстрирует знание методов и средств предотвращения утечки информации за счет побочных электромагнитных излучений и наводок
ИД-3 Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

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

Форма реализации: Смешанная форма

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

БРС дисциплины

1 семестр

Раздел дисциплины	Веса контрольных мероприятий, %						
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5	КМ-6
	Срок КМ:	4	4	8	14	14	16
Эллиптическая криптография							
Эллиптическая криптография		+	+	+			
Стеганография							
Стеганография					+	+	+
Вес КМ:		5	12,5	32,5	5	12,5	32,5

§Общая часть/Для промежуточной аттестации§

БРС курсовой работы/проекта

1 семестр

Раздел дисциплины	Веса контрольных мероприятий, %					
	Индекс КМ:	КМ- 1	КМ- 2	КМ- 3	КМ- 4	КМ- 5
	Срок КМ:	4	8	10	12	14
Часть 1 Разработка программной реализации электронно-цифровой подписи		+	+	+		
Часть 2 Встраивание информации из студенческого билета в контейнер-изображение					+	+
Вес КМ:		5	45	10	5	35

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ПК-2	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	Контроль посещения лекций №1-2 по курсу ЦТЗИ Модуль 1 (10%) (Интервью) Контроль выполнения комплекса лабораторных работ №1-2 по курсу МСЗИ Модуль 1 (25%) (Лабораторная работа) Контрольно-зачетное занятие (К331) по курсу МСЗИ Модуль 1 (65%) (Тестирование)
ПК-2	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-	Контроль посещения лекций № 3-8 по курсу ЦТЗИ Модуль 2 (10%) (Интервью) Контроль выполнения комплекса лабораторных работ №3- 6 по курсу ЗИ Модуль 2 (25%) (Лабораторная работа) Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) (Тестирование)

		контейнерах	
ПК-2	ИД-ЗПК-2 Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем	<p>Знать:</p> <ul style="list-style-type: none"> – источники научно-технической информации (журналы, сайты Интернет) по теме дисциплины; алгоритмы встраивания и извлечения конфиденциальной информации, а также стеганоанализа мультимедиа-контейнеров <p>Уметь:</p> <ul style="list-style-type: none"> разрабатывать системы цифровой стеганографии для защиты объектов интеллектуальной собственности; проводить исследования и оценку эффективности стеганографических систем. 	<p>Контроль посещения лекций № 3-8 по курсу ЦТЗИ Модуль 2 (10%) (Интервью)</p> <p>Контроль выполнения комплекса лабораторных работ №3- 6 по курсу ЗИ Модуль 2 (25%) (Лабораторная работа)</p> <p>Контрольно-зачетное занятие (К332) по курсу МСЗИ Модуль 2 (65%) (Тестирование)</p>

II. Содержание оценочных средств. Шкала и критерии оценивания

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

Формы реализации: Смешанная форма

Тип контрольного мероприятия: Интервью

Вес контрольного мероприятия в БРС: 5

Процедура проведения контрольного мероприятия: При очной форме обучения - заполнение ведомости присутствия в течение лекции. При дистанционной форме обучения - регистрация участников мероприятия в Webex.

Краткое содержание задания:

Проставить в ведомости свою фамилию и подпись. Зарегистрироваться в Webex и присутствовать на лекции.

Пример выполнения (не выполнения) задания:

1	2	Модуль 1 ЦТЗИ Осенний семестр 2020г.																				
		А-08м-20					Лекции 10					Лабораторные 25										
3	4	№1	№2	№3	№4	№5	№1	№2	№3	№4	№5	№6	№7	№8	№9	№10	№11	№12	№13	№14	№15	
1	Азаров Василий Михайлович	1	1			2	10	19,0	25,0												44	25,00
2	Алещин Дмитрий Олегович	1	1			2	10	19,0	25,0												44	25,00
3	Бакунинов Максим Ильич					0	0														0	0,00
4	Бактин Евгений Валерьевич	1	1			2	10	19,0	25,0												44	25,00
5	Банков Артем Михайлович	1	1			2	10	19,0	25,0												44	25,00
6	Винокуров Илья Леонидович					0	0														0	0,00
7	Галикова Алёна Валерьевна	1	1			2	10	19,0	25,0												44	25,00
8	Корозин Владислав Михайлович	1	1			2	10	19,0	25,0												40	22,73
9	Коротченко Кирилл Николаевич	1	1			2	10	19,0	25,0												44	25,00

Контрольные вопросы/задания:

Знать: протоколы эллиптической криптографии, стандарты ЭЦП на эллиптических кривых	<ol style="list-style-type: none"> 1.Определение поля 2.Геометрия эллиптических кривых 3.Теорема Хассе
Уметь: применять системы ЭЦП на основе эллиптических кривых для защиты информации	<ol style="list-style-type: none"> 1.Сложить точки эллиптической кривой 2.Сформировать системные параметры для протокола Massey-Omura 3.Выбрать параметры для реализации схемы Nyberg-Rueppel электронной подписи с использованием группы точек эллиптической кривой

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 2 лекций модуля 1 равно 10. Оценка 5 находится в диапазоне 9-10 баллов.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 2 лекций модуля 1 равно 10. Оценка 4 находится в диапазоне 7-8 баллов.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 2 лекций модуля 1 равно 10. Оценка 3 находится в диапазоне 4-6 баллов.

Оценка: 2

Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 3 баллов.
При отсутствии на всех лекциях по неуважительным причинам проставляется 0.

КМ-2. Контроль выполнения комплекса лабораторных работ №1-2 по курсу МСЗИ Модуль 1 (25%)

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 12,5

Процедура проведения контрольного мероприятия: При очной форме обучения лабораторные работы выполняются в компьютерном классе, в котором доступна сетевая версия Wolfram Mathematica 9. Одна лабораторная работа длится 2 академических часа. Отчет формируется в бумажном варианте. При дистанционной форме обучения лабораторные работы выполняются в Wolfram Cloud | Open Access system. Контроль и консультации в течение лабораторной работы в системе Webex. Рабочее задание и необходимые методические материалы размещаются в системе Moodle. Отчет по выполненной лабораторной работе загружается в систему Moodle, где производится контроль выполнения и выставляется суммарное число баллов по правильно выполненным пунктам рабочего задания.

Краткое содержание задания:

Пример рабочего задания лабораторной работы №1 максимальный балл 19

Лабораторная работа №1

По курсу «Цифровые технологии защиты информации»

Исследование свойств эллиптических кривых.

1. Построить график эллипса $x^2 + 2y^2 = 3$, используя функцию `ContourPlot[]` пакета Mathematica.
2. В поле рациональных чисел построить графики эллиптических кривых $Y^2 = X^3 + aX + b$ для положительного и отрицательного коэффициента "a" (см. Табл.1), проверить выполнение условия гладкости кривой $-16(4a^3 + 27b^2) \neq 0$, а также проверить, является ли заданный в правой части уравнения многочлен неприводимым, используя функцию `Factor[]`.
3. Проверить выполнение условия гладкости кривой в $GF(p)$. Определить число точек заданной кривой в поле $GF(p)$ (см. \articles\Cryptology\10.1- пример 3, а также Mathematica_5_6 – раздел 5.5.9) и построить точечный график.
4. Сложить две точки, принадлежащие заданной эллиптической кривой, зафиксировать полученный результат на точечном графике.

Операцию сложения можно выполнить, используя следующий программный модуль(\articles\Cryptology\10.3-4):

При использовании данного модуля следует учитывать, что он реализует сложение точек эллиптических кривых вида: $y^2 = x^3 + ax^2 + bx + c$.

1. Провести тестирование операции сложения, повторив следующие действия:

```
p=11;a=0;b=6;c=3;EllipticAdd[p,a,b,c,{4,6},{9,4}]
```

```
EllipticAdd[p,a,b,c,{9,4},{9,4}]
```

```
EllipticAdd[p,a,b,c,{4,6},{4,6}]
```

```
EllipticAdd[p,a,b,c,{4,6},{0}]
```

```
EllipticAdd[p,a,b,c,{4,6},{4,5}]
```

```
EllipticAdd[p,a,b,c,{0},{9,4}]
```

Ожидаемый результат:

{3,9} {7,6} {4,5} {4,6} {0} {9,4}

6. Нарисовать алгоритм выполнения программного модуля п.4. (Этот пункт можно выполнить в качестве домашнего задания).

7. Провести операцию умножения произвольной точки на число n (Табл.1) и построить граф переходов.

8. Для каждой точки заданной кривой определить её порядок (**Определение:** Порядком точки P эллиптической кривой называется

наименьшее натуральное число $m \neq 0$, для которого $mP = O$. См. также

articles\osnovy_elliptic.pdf, page 69). Построить гистограмму распределения порядков точек.

Таблица 1

№	a	b	p	n
1	31	28	149	5
2	29	51	107	6
3	22	11	83	5
4	40	18	41	7
5	23	15	43	8
6	7	3	101	7
7	15	5	127	5
8	30	15	89	6
9	60	9	113	8
10	29	1	31	7
11	36	4	53	5
12	120	8	137	6
13	101	2	109	8
14	53	4	59	5
15	65	30	67	6
16	33	11	37	7
17	42	5	47	7
18	60	43	61	5
19	23	7	71	6
20	25	25	73	8
21	17	24	83	7
22	51	57	79	6
23	55	22	139	5
24	88	18	131	8
25	23	9	107	7

Контрольные вопросы/задания:

Знать: протоколы эллиптической криптографии, стандарты ЭЦП на эллиптических кривых	<ol style="list-style-type: none"> 1. Условия гладкости эллиптической кривой 2. Протокол Диффи-Хеллмана для группы точек эллиптической кривой 3. Методы проверки числа на принадлежность к множеству простых чисел
Уметь: применять системы ЭЦП на основе эллиптических кривых для защиты информации	<ol style="list-style-type: none"> 1. Выбрать системные параметры для реализации протокола Диффи-Хеллмана 2. Получить общий ключ

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 2-х лабораторных работ модуля 1 равно 44. Оценка 5 находится в диапазоне 39 -44 балла.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 2-х лабораторных работ модуля 1 равно 44. Оценка 4 находится в диапазоне 30 -38 балла.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 2-х лабораторных работ модуля 1 равно 44. Оценка 3 находится в диапазоне 17 - 29 балла.

Оценка: 2

Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 16 балла. При отсутствии отчета по лабораторной работе по неуважительным причинам проставляется 0 баллов, и, в соответствии с настройками системы Moodle, студент не допускается к КЗЗ, пока не погасит задолженность.

КМ-3. Контрольно-зачетное занятие (КЗЗ1) по курсу МСЗИ Модуль 1 (65%)

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Тестирование

Вес контрольного мероприятия в БРС: 32,5

Процедура проведения контрольного мероприятия: При очной форме обучения контрольно-зачетное занятие проводится в компьютерном классе, оснащенный сетевой версией Mathematica. Длительность контрольной 2 академических часа. К занятию допускаются студенты, выполнившие цикл лабораторных работ модуля 1 и представившие отчеты по лабораторным работам. При дистанционной форме обучения контроль за участниками ведется в Webex, тестирование проводится в системе Moodle. К тестированию допускаются студенты, загрузившие в Moodle электронные отчеты и получившие по ним положительную оценку. Загрузка отчетов должна быть завершена за 24 часа до начала контрольной.

Краткое содержание задания:

Пример задания КЗЗ1:

Вопрос 1
 Ответ сохранен
 Балл: 3,00

Найти сумму $P_4 = P_1 + P_2 + P_3$ трех точек эллиптической кривой $y^2 = x^3 + bx + 1$ над полем $GF(p)$, где: $b = 3049$, $p = 3469$, $P_1 = (2843, 192)$, $P_2 = (3159, 2713)$, $P_3 = (1301, 420)$
 Ответ вводить как строку с фигурными скобками: {****,****}

Ответ:

Контрольные вопросы/задания:

Знать: протоколы эллиптической криптографии, стандарты ЭЦП на эллиптических кривых	1.Сложение трех точек Уровень 3 Число вариантов 48
Уметь: применять системы ЭЦП	1.Число точек ЭК Уровень 5 Число вариантов 48

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 24. Оценка 5 находится в диапазоне 21 - 24 баллов

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 24. Оценка 4 находится в диапазоне 16 - 20 баллов

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 24. Оценка 3 находится в диапазоне 9 - 14 баллов

Оценка: 2

Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 8 баллов. Оценка 2 проставляется при участии в контрольной, при отсутствии по неуважительным причинам проставляется 0.

КМ-4. Контроль посещения лекций № 3-8 по курсу ЦТЗИ Модуль 2 (10%)

Формы реализации: Смешанная форма

Тип контрольного мероприятия: Интервью

Вес контрольного мероприятия в БРС: 5

Процедура проведения контрольного мероприятия: При очной форме обучения - заполнение ведомости присутствия в течение лекции. При дистанционной форме обучения - регистрация участников мероприятия в Webex.

Краткое содержание задания:

Проставить в ведомости свою фамилию и подпись. Зарегистрироваться в Webex и присутствовать на лекции.

Контрольные вопросы/задания:

<p>Знать: методы реализации стеганографических систем в пространственной области, а также с применением дискретного косинусного, вейвлет и фрактального преобразований</p>	<p>1.Модель процесса встраивания ЦВЗ</p>
<p>Знать: – источники научно-технической информации (журналы, сайты Интернет) по теме дисциплины; алгоритмы встраивания и извлечения конфиденциальной информации, а также стеганоанализа мультимедиа-контейнеров</p>	<p>1.Классификация стеганографических методов</p>
<p>Уметь: – применять форматные</p>	<p>1.Применить метод дописывания данных в конец</p>

и неформатные способы сокрытия информации для встраивания цифровых водяных знаков в медиа-контейнерах	ВМР-файла
Уметь: разрабатывать системы цифровой стеганографии для защиты объектов интеллектуальной собственности; проводить исследования и оценку эффективности стеганографических систем.	1.Выбирать тип контейнера в зависимости от поставленных условий 2.Оценить пропускную способность контейнера при реализации алгоритма «LangelaarDCT» 3.Провести анализ числа близких цветовых пар в палитре изображения

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 6 лекций модуля 1 равно 10. Оценка 5 находится в диапазоне 9-10 баллов.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 6 лекций модуля 1 равно 10. Оценка 4 находится в диапазоне 7-8 баллов.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при посещении всех 6 лекций модуля 1 равно 10. Оценка 3 находится в диапазоне 4-6 баллов.

Оценка: 2

Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 3 баллов. При отсутствии на всех лекциях по неуважительным причинам проставляется 0.

КМ-5. Контроль выполнения комплекса лабораторных работ №3- 6 по курсу ЗИ Модуль 2 (25%)

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Лабораторная работа

Вес контрольного мероприятия в БРС: 12,5

Процедура проведения контрольного мероприятия: При очной форме обучения лабораторные работы выполняются в компьютерном классе, в котором доступна сетевая версия Wolfram Mathematica 9. Одна лабораторная работа длится 2 академических часа. Отчет формируется в бумажном варианте. При дистанционной форме обучения лабораторные работы выполняются в Wolfram Cloud | Open Access system. Контроль и консультации в течение лабораторной работы в системе Webex. Рабочее задание и необходимые методические материалы размещаются в системе Moodle. Отчет по выполненной лабораторной работе загружается в систему Moodle, где производится контроль выполнения и выставляется суммарное число баллов по правильно выполненным пунктам рабочего задания.

Краткое содержание задания:

Пример рабочего задания лабораторной работы №4 максимальный балл 40

Встраивание видимого ЦВЗ в пространственной области

1. Сформировать контейнер-оригинал (`risO`): изображение в формате BMP24 размером 512*384 (Paint\Рисунок\Атрибуты) из рисунка с номером N, находящегося в папке \Lab4-2010\work task\Images.
2. Выделить и скопировать в файл (`box.bmp`) прямоугольную область с координатой верхнего левого угла (286,347) и размером 220x30 точек.
3. Импортировать файл `box.bmp` в пакет "Mathematica" (`Import[]`) и определить размеры рисунка - `ImageDimensions[]`.
4. Вывести первую и последнюю строку изображения в формате RGB- данных с помощью функции `ImageData[***,"Byte"]` .
5. Разделить изображение из `box.bmp` на три составляющие в соответствии цветовой RGB – моделью с помощью функции `ColorSeparate[]` и определить средние интенсивности красного, зеленого и синего цвета.
6. Сформировать в программе Paint рисунок (`ris-direct`) в формате BMP24 размером 220*30 и закрасить его цветом, соответствующем средним значениям RGB п. 5.
7. Сформировать в программе Paint рисунок (`ris-inverse`) в формате BMP24 размером 220*30 и закрасить его цветом, обратным (опция – обратить цвета) цвету `ris-direct`.
8. Запустить (установить) программу K-Lab Watermark (`bs1e-free.exe`). Провести настройку параметров:
 - General: Use watermark text.
 - Text: четные номера по списку группы \Font-Options\Цвет\Белый, Center, размер 20; нечетные номера по списку группы \Font-Options\Цвет\Черный, Center, размер 20;
 - Image: Отключить - Transparent background, включить позицию – Right bottom.
 - Output: Save in original format; отключить – Save protected image automatically.
9. Открыть подготовленный контейнер `risO` (Open Image) , ввести в поле Text свою фамилию, имя и отчество. Установить прозрачность ЦВЗ (Transparecy) равной 0%, и провести встраивание ЦВЗ (Protect). Сохранить (Save image as) рисунок со встроенным ЦВЗ, имя файла должно содержать индекс `w0`.
10. Установить прозрачность ЦВЗ равной 80%, провести встраивание ЦВЗ, сохранить результат (Save image as) , имя файла должно содержать индекс 80.
й Прозрачность ЦВЗ может меняться от 100% до 0%, при этом шкала прозрачности имеет 256 дискретных уровней, переход от одного уровня к другому может производиться с помощью клавиатуры с большей точностью(стрелки ← и →).
11. Открыть в K-Lab Watermark рисунок `risOw0.bmp` (из п.9), в настройках подключить General: Use watermark image, во вкладке Image загрузить рисунок `ris-direct` , установить прозрачность ЦВЗ (Transparecy) равной 0%, и провести встраивание ЦВЗ (Protect). Сохранить (Save image as) рисунок со встроенным ЦВЗ как `master_drawing` – контейнер для дальнейших исследований.
12. Открыть в K-Lab Watermark рисунок `master_drawing.bmp` (из п.10), во вкладке Image загрузить рисунок `ris-inverse`, установить прозрачность ЦВЗ (Transparecy) равной 0%, и провести встраивание ЦВЗ (Protect). Сохранить (Save image as) рисунок со встроенным ЦВЗ `w0.bmp`.
13. Создать последовательность рисунков – заполненных контейнеров, с ЦВЗ `ris-inverse` для значений прозрачности ЦВЗ 25%, 50%, 75%, 100%. Каждый новый (по

прозрачности) ЦВЗ желательно встраивать в один и тот же контейнер –оригинал master_drawing.bmp, для чего может быть использована опция "Undo".

ü Последовательность рисунков служит исходным материалом для проведения исследования методики встраивания ЦВЗ в программе K-Lab Watermark, поэтому она должна быть сформирована как можно более тщательно.

ü Freeware – версия программы может быть ограничена 5 циклами встраивания, для продолжения работы необходимо перезапустить программу K-Lab Watermark.

14. Определить параметры RGB- модели для любой точки ЦВЗ в зависимости от параметра прозрачности:

Прозрачность	0%	25%	50%	75%	100%
R					
G					
B					

15. По данным таблицы RGB - модели сформировать три списка – rR,gG,bB –в координатах " Прозрачность ", "Интенсивность цвета".

16. Для каждого из списков определить линейную аппроксимацию зависимости интенсивности цвета от параметра прозрачности в виде: $ssR=Fit[rR, \{1,x\},x]$.

17. Построить совмещенные точечные и линейные графики для каждого цвета используя следующие функции: Show[], ListPlot[], Plot[], PlotStyle->RGBColor[*,*,*].

18. Проверить полученные результаты для прозрачности 20% и 80% с использованием теоретической формулы для встраивания видимого ЦВЗ:

$$IW = p'I_0 + (1-p)I'$$

19. Импортировать контейнер-оригинал (risO) в пакет "Mathematica".

20. Создать графический объект- ЦВЗ, содержащий: фамилию, имя, отчество, используя следующую конструкцию - Graphics[Text["Фамилия Имя Отчество"]].

21. Произвести встраивание ЦВЗ в контейнер – оригинал с помощью функции ImageCompose[контейнер оригинал, {ЦВЗ, прозрачность}]. Величина прозрачности варьируется от 0 до 1, положение ЦВЗ регулируется опциями функции ImageCompose[[]].

22. Создать динамический модуль отображения ЦВЗ в виде :

Manipulate[ImageCompose[контейнер оригинал, {ЦВЗ, a}], {a,0,1,0.01}].

Контрольные вопросы/задания:

Знать: методы реализации стеганографических систем в пространственной области, а также с применением дискретного косинусного, вейвлет и фрактального преобразований	1.Метод блочного сокрытия
Знать: – источники научно-технической информации (журналы, сайты Интернет) по теме дисциплины; алгоритмы встраивания и извлечения конфиденциальной информации, а также стеганоанализа мультимедиа-контейнеров	1.Цветовая модель RGB 40 2.Метод замены младшего бита
Уметь: – применять форматные и неформатные способы	1.Провести визуализацию встроенной информации 2.Определить порог чувствительности:

сокрытия информации для встраивания цифровых водяных знаков в медиа-контейнерах	интенсивность встраивания, при которой искажения становятся незаметными
Уметь: разрабатывать системы цифровой стеганографии для защиты объектов интеллектуальной собственности; проводить исследования и оценку эффективности стеганографических систем.	1. Определить линейную аппроксимацию зависимости интенсивности цвета от параметра прозрачности 2. Произвести встраивание ЦВЗ в контейнер – оригинал

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 4-х лабораторных работ модуля 1 равно 128. Оценка 5 находится в диапазоне 115 -128 балла.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 4-х лабораторных работ модуля 1 равно 128. Оценка 4 находится в диапазоне 89-114 балла.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при успешном выполнении всех 4-х лабораторных работ модуля 1 равно 128. Оценка 3 находится в диапазоне 51 -88 балла.

Оценка: 2

Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 50 баллов. При отсутствии отчета по лабораторной работе по неуважительным причинам проставляется 0 баллов, и, в соответствии с настройками системы Moodle, студент не допускается к КЗЗ, пока не погасит задолженность.

КМ-6. Контрольно-зачетное занятие (КЗЗ) по курсу МСЗИ Модуль 2 (65%)

Формы реализации: Компьютерное задание

Тип контрольного мероприятия: Тестирование

Вес контрольного мероприятия в БРС: 32,5

Процедура проведения контрольного мероприятия: При очной форме обучения контрольно-зачетное занятие проводится в компьютерном классе, оснащенном сетевой версией Mathematica. Длительность контрольной 2 академических часа. К занятию допускаются студенты, выполнившие цикл лабораторных работ модуля 1 и представившие отчеты по лабораторным работам. При дистанционной форме обучения контроль за участниками ведется в Webex, тестирование проводится в системе Moodle. К тестированию допускаются студенты, загрузившие в Moodle электронные отчеты и получившие по ним положительную оценку. Загрузка отчетов должна быть завершена за 24 часа до начала контрольной.

Краткое содержание задания:

Пример задания КЗЗ2 :

Вопрос 1
Ответ сохранен
Балл: 5,00

Изображение contW.bmp состоит из 50 строк и 7 столбцов. В одном из цветовых каналов строки с номером 47, в младших битах, содержится 7-ми разрядный код числа. Найти десятичный эквивалент этого числа.

Ответ:

Контрольные вопросы/задания:

Знать: методы реализации стеганографических систем в пространственной области, а также с применением дискретного косинусного, вейвлет и фрактального преобразований	1.извлечь код Уровень 5 Число вариантов 50
Знать: – источники научно-технической информации (журналы, сайты Интернет) по теме дисциплины; алгоритмы встраивания и извлечения конфиденциальной информации, а также стеганоанализа мультимедиа-контейнеров	1.встроить блок с заданной интенсивностью Уровень 7 Число вариантов 24
Уметь: – применять форматные и неформатные способы сокрытия информации для встраивания цифровых водяных знаков в медиа-контейнерах	1.Число байт выравнивания Уровень 3 Число вариантов 36
Уметь: разрабатывать системы цифровой стеганографии для защиты объектов интеллектуальной собственности; проводить исследования и оценку эффективности стеганографических систем.	1.Стегопуть Уровень 3 Число вариантов 24 2.стереть биты Уровень 7 Число вариантов 36

Описание шкалы оценивания:

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 32. Оценка 5 находится в диапазоне 28 - 32 баллов.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 32. Оценка 4 находится в диапазоне 22 - 27 баллов.

Оценка: 3

Нижний порог выполнения задания в процентах: 40

Описание характеристики выполнения знания: Максимальное число набранных баллов при правильном решении 6 заданий равно 32. Оценка 3 находится в диапазоне 12 - 21 балл.

Оценка: 2

Описание характеристики выполнения знания: Оценка 2 находится в диапазоне 0 - 11 баллов. Оценка 2 проставляется при участии в контрольной, при отсутствии по неуважительным причинам проставляется 0.

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

МЭИ	ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 4 Цифровые технологии защиты информации И ВТИ	Утверждаю Зав.кафедрой
Задание №1 Теоретические вопросы		
1. Поля – определение, примеры, порядок поля, характеристика поля.		
2. Встраивание ЦВЗ в пространственной области. Алгоритм «Langelaar».		
Задание №2 Задания уровня 2		
Определить число байт сообщения, которое можно скрыть в байтах выравнивания, для рисунка в формате BMP24, размером $h \times w$, где: $h=686$ -вертикальный размер, $w=952$ -горизонтальный размер.		
Задание №3 Задания уровня 4		
Найти порядок точки $P = \{631, 1333\}$ эллиптической кривой $y^2 = x^3 + ax^2 + bx + c$ над полем $GF(p)$, где: $a=2011$ $b=2963$, $c=3407$ $p=1619$		
Задание №4 Задания уровня 6		
Скопировать по сети в рабочую папку рисунок <code>ris192x256.bmp</code> . Разбить его на блоки 16×16 . Для блока в строке 1 и столбце 11 матрицы разбиения установить максимальную интенсивность цветов для каждого пикселя. Собрать новое изображение с модифицированным блоком и определить значение его хэш-функции: <code>Hash[***, "CRC32"]</code> .		

Процедура проведения

Экзамен проводится в системе Moodle и Webex (идентификация и контроль, в том числе визуальный) и состоит из двух тестов (вопросы или задания выполняются строго последовательно): Первый тест содержит 30 простых вопросов по теоретической части курса. Среднее время на ответ 30-40 секунд. Общая продолжительность теста 20 минут. Максимальное число баллов по теоретической части - 40. Второй тест содержит 6 практических заданий, аналогичных заданиям КЗЗ. Среднее время на выполнение задания 10 минут. Общая продолжительность теста 60 минут. Максимальное число баллов по теоретической части - 60. Результирующая оценка за экзамен определяется как сумма баллов, набранных в первом и втором тестах и пересчитывается к пятибалльной системе (Традиционные оценки РФ).

1. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-1ПК-2 Демонстрирует знание нормативной базы, методов описания, анализа и проектирования в области обеспечения безопасности информационных систем

Вопросы, задания

1. Эллиптические кривые – определение, условие гладкости эллиптической кривой
2. Построение односторонней функции на основе эллиптической кривой, вычисление $κP$ методом аддитивных цепочек
3. Использование группы точек эллиптической кривой в протоколе Диффи-Хеллмана.

Материалы для проверки остаточных знаний

1. Какой из параметров эллиптической кривой можно оценить по теореме Хассе.

Ответы:

порядок группы точек эллиптической кривой
число точек эллиптической кривой
значение дискриминанта эллиптической кривой
модуль эллиптической кривой
число точек “O”

Верный ответ: число точек эллиптической кривой

2. В каком диапазоне может находиться простое число q - порядок циклической подгруппы группы точек эллиптической кривой стандарта ЭЦП ГОСТ 34.10.

Ответы:

$2^{254} < q < 2^{256}$
 $2^{124} < q < 2^{128}$
 $2^{1254} < q < 2^{1256}$
 $2^{1024} < q < 2^{2048}$
 $1 < q < \infty$

Верный ответ: $2^{254} < q < 2^{256}$

3. Чем определяется длина компоненты r электронно-цифровой подписи Nyberg-Rueppel.

Ответы:

порядком поля эллиптической кривой
порядком базовой точки ЭК
параметрами хэш-функции ЭЦП
значением дискриминанта ЭК

Верный ответ: порядком базовой точки ЭК

2. Компетенция/Индикатор: ИД-2ПК-2 Демонстрирует знание методов и средств предотвращения утечки информации за счет побочных электромагнитных излучений и наводок

Вопросы, задания

1. Встраивание ЦВЗ в области преобразования. Основные элементы алгоритма сжатия JPEG.
2. Методы контроля искажений, вносимых стеганографическими системами. Свойства функций расстояния
3. Модель процесса встраивания ЦВЗ

Материалы для проверки остаточных знаний

1. Какие из приведенных стего-алгоритмов могут быть реализованы в пространственной области:

Ответы:

Алгоритм "Kutter"

Алгоритм Дармстедтера-Делейгла-Квисквотера-Макка (ДДКМ) - Bruyndonckx

Алгоритм «Langelaar»

Алгоритм «LangelaarDCT»

Алгоритм «Barni»

Алгоритм «Сох»

Алгоритм «Koch»

Верный ответ: Алгоритм "Kutter" Алгоритм Дармстедтера-Делейгла-Квисквотера-Макка (ДДКМ) - Bruyndonckx Алгоритм «Langelaar»

2. К какому классу стеганографических систем относится алгоритм «Langelaar»

Ответы:

Закрытые тип 1

Закрытые тип 2

Закрытые тип 3

Полузакрытые

Открытые

Верный ответ: Открытые

3. Компетенция/Индикатор: ИД-3ПК-2 Осуществляет разработку аппаратных и программных средств, необходимых для обеспечения безопасности компьютерных систем

Вопросы, задания

1. Структурная схема стеганосистемы как системы связи

2. Методы стегоанализа мультимедиа-контейнеров. Метод анализа пар значений.

3. Встраивание ЦВЗ в пространственной области. Алгоритм «Langelaar».

4. Встраивание ЦВЗ в области преобразования. Алгоритм «Kundur-1»

Материалы для проверки остаточных знаний

1. Какие объекты необходимы для извлечения (восстановления) информации по алгоритму "Kutter"

Ответы:

заполненный контейнер

исходный контейнер

цифровой водяной знак

корреляционный детектор

случайный контейнер

Верный ответ: заполненный контейнер

2. Какие объекты необходимы для извлечения (восстановления) информации по алгоритму "Langelaar"

Ответы:

заполненный контейнер

исходный контейнер

цифровой водяной знак

корреляционный детектор

случайный контейнер

Верный ответ: заполненный контейнер

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Максимальное число баллов, набранных в двух тестах равно 100 (или с умножением на 4 при очной форме). Оценка 5 находится в интервале от 90 до 100 баллов.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Максимальное число баллов, набранных в двух тестах равно 100 (или с умножением на 4 при очной форме). Оценка 4 находится в интервале от 70 до 89 баллов.

Оценка: 3

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Максимальное число баллов, набранных в двух тестах равно 100 (или с умножением на 4 при очной форме). Оценка 3 находится в интервале от 60 до 69 баллов.

Оценка: 2

Описание характеристики выполнения знания: Максимальное число баллов, набранных в двух тестах равно 100 (или с умножением на 4 при очной форме). Оценка 2 находится в интервале от 0 до 59 баллов.

III. Правила выставления итоговой оценки по курсу

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 балльной 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.

Для курсового проекта/работы:

1 семестр

Форма проведения: Защита КП/КР

I. Процедура защиты КП/КР

Материалы к защите курсовой работы ЦТЗИ: 1. Пояснительная записка - титульный лист, оглавление, задание с индивидуальными параметрами ,текст, список использованных источников. Формат PDF. 2. Исходный контейнер. Формат BMP. 3. Заполненный контейнер. Формат BMP. 4. Модуль встраивания текста - входные параметры: контейнер, строка текста. Выход - заполненный контейнер. Формат модуля: zip - архив .nb. 5. Модуль извлечения текста - входные параметры: заполненный контейнер. Выход - строка текста. Формат модуля: zip - архив .nb. 6. Модуль формирования ЭЦП. Вход: контейнер, порядок точки q, случайное число k. Выход: r,c. Формат модуля: zip - архив .nb. 7. Модуль верификации ЭЦП. Вход: контейнер, r,c. Выход - результат проверки ЭЦП. Формат модуля: zip - архив .nb. Любой неработоспособный модуль не дает возможности выполнить проверку работы, что приводит к оценке неудовлетворительно на защите курсовой работы. Файлы, представленные на защиту курсовой работы должны иметь (в строгой последовательности) следующий формат: название материала (напр. Пояснительная записка), фамилию и инициалы автора, номер группы. Процедура защиты стандартная, с двумя членами комиссии.

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: «Отлично» – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Оценка: 4

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: «Очень хорошо» – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному. «Хорошо» – теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками.

Оценка: 3

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: «Удовлетворительно» – теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнены, некоторые из выполненных заданий, возможно, содержат ошибки «Посредственно» – теоретическое содержание курса освоено частично, некоторые

практические навыки работы не сформированы, предусмотренные программой обучения учебные задания выполнены с ошибками, либо качество выполнения некоторых из них оценено числом баллов, близким к минимальному.

Оценка: 2

Описание характеристики выполнения знания: 31 – 59 FX «Условно неудовлетворительно» – теоретическое содержание курса освоено частично, необходимые практические навыки работы не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, либо качество их выполнения оценено числом баллов, близким к минимальному; при дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий 0 – 30 F «Безусловно неудовлетворительно» – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, все выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к какому-либо значимому повышению качества выполнения учебных заданий.

III. Правила выставления итоговой оценки по курсу

Среднее по оценкам защиты и текущей успеваемости