Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 01.03.02 Прикладная математика и информатика

Наименование образовательной программы: Математическое моделирование

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Математические методы криптографии

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Фролов А.Б. Идентификатор: Ref8507cb-FrolovAB-a54b01e2	А.Б. Фролов
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Черепова М.Ф. Идентификатор: R9267877e-CherepovaMF-dbb9bf1	М.Ф. Черепова
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Зубков П.В. Идентификатор: R4920bc6f-ZubkovPV-8172426c	П.В. Зубков
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

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:

1. ПК-2 Способен участвовать в компьютерной реализации математических моделей
   ИД-5 Выбирает, модифицирует и реализует алгоритмы численной и алгебраической реализации математических моделей
   ИД-6 Демонстрирует понимание основ теории сложности реализации математических моделей

и включает:

для текущего контроля успеваемости:

Форма реализации: Билеты (письменный опрос)

1. Формальные модели шифров и кодов аутентификации (Тестирование)

Форма реализации: Письменная работа

1. Оценивание стойкости криптографических преобразований и надежности шифров (Контрольная работа)
2. Применение простейших шифров и формальных моделей кодов аутентификации (Контрольная работа)

Форма реализации: Проверка задания

1. Криптографическая терминология и основные задачи криптографии (Тестирование)

БРС дисциплины

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Основные задачи и модели криптографии					
Основные задачи и модели криптографии		+			
Комбинаторные блок-схемы в криптографии					
Комбинаторные блок-схемы в криптографии			+		
Свойства криптографических преобразований					
Свойства криптографических преобразований				+	

Надёжность шифров				
Надёжность шифров				+
Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

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-5$_{ПК-2}$ Выбирает, модифицирует и реализует алгоритмы численной и алгебраической реализации математических моделей	Знать: криптографическую терминологию и основные задачи криптографии формальные модели шифров и кодов аутентификации Уметь: применять простейшие шифры и строить формальные модели кодов аутентификации	Криптографическая терминология и основные задачи криптографии (Тестирование) Формальные модели шифров и кодов аутентификации (Тестирование) Применение простейших шифров и формальных моделей кодов аутентификации (Контрольная работа)
ПК-2	ИД-6$_{ПК-2}$ Демонстрирует понимание основ теории сложности реализации математических моделей	Знать: методы оценки качества криптографических преобразований	Оценивание стойкости криптографических преобразований и надежности шифров (Контрольная работа)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Криптографическая терминология и основные задачи криптографии

Формы реализации: Проверка задания
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Тестирование по вариантам. Работа содержит 4 задания на 20 минут

Краткое содержание задания:
Тестирование связано с проверкой знания криптографической терминологии и основных задач криптографии

Контрольные вопросы/задания:

Знать: криптографическую терминологию и основные задачи криптографии	1.Дайте определения конфиденциальности и целостности информации и аутентификации. 2.В чем состоит различие асимметричных и симметричных криптосистем? 3.В чем отличие терминов расшифрование и дешифрование? 4.Назовите два основные вида атак на криптосистемы

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется, если задание выполнено в полном объеме или выполнено преимущественно верно.

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется, если большинство вопросов раскрыто. выбрано верное направление для решения задач.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется, если задание преимущественно выполнено

КМ-2. Формальные модели шифров и кодов аутентификации

Формы реализации: Билеты (письменный опрос)
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Тестирование проводится по вариантам. Работа содержит 4 задания на 20 минут

Краткое содержание задания:
Тест № 2 «Формальные модели шифров и кодов аутентификации» связан с проверкой знания формальных моделей шифров и кодов аутентификации

Контрольные вопросы/задания:

Знать: формальные модели шифров и кодов аутентификации	1.Приведите общую формулу алгебраической модели шифра. 2.Приведите общую формулу алгебраической модели кода аутентификации. 3.Какие комбинаторные блок-схемы используются в алгебраических моделях кодов аутентификации? 4.В чем различие алгебраических зависимостей ключей зашифрования и расшифрования в симметричнсых и асимметричных криптосистемах?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется, если задание выполнено в полном объеме или выполнено преимущественно верно.

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется, если большинство вопросов раскрыто. выбрано верное направление для решения задач.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется, если задание преимущественно выполнено

КМ-3. Применение простейших шифров и формальных моделей кодов аутентификации

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Контрольная работа проводится по вариантам. Работа содержит 4 задания на 20 минут

Краткое содержание задания:
Целью контрольной работы является проверка умения применять простейшие шифры и строить формальные модели кодов аутентификации

Контрольные вопросы/задания:

Уметь: применять простейшие шифры и строить формальные модели кодов аутентификации	1.Построить алгебраическую модель кода аутентификации, в которой $X=A=Z\_3$ и $K=Z\_3 x Z\_3$, а преобразование аутентификации для ключа $(i,j)\backslash in\ K$ определятся соотношением $e\_\{i,j\}(x)=(ix+ j\ )$ mod 3. 2.Построить ортогональный массив OA(3,3,1) 3.Построить ортогональный массив OA(3,4,1) 4.Вычислить вероятности имитации четырех равномерно распределенных сообщений при использовании трех ключей k_1,k_2, k_3 с заданным распределением вероятностей (p(k_1),p(k_2),p(k_3)))=(½,¼,¼) 5.Построить оптимальную стратегию навязывания

	при задании четырех равномерно распределенных сообщений при использовании трех ключей k_1,k_2, k_3 с заданным распределением вероятностей (p(k_1),p(k_2),p(k_3)))=(½,¼,¼) 6.Применить отрезок бинарной гаммы для зашифрования отрезка бинарного текста той же длины. 7.Применить отрезок бинарной гаммы для расшифрования отрезка бинарного текста той же длины. 8.Применить схему Грина для вычисления преобразования Уолша-Адамара двоичного вектора длины 8.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется, если задание выполнено в полном объеме или выполнено преимущественно верно.

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется, если большинство вопросов раскрыто. выбрано верное направление для решения задач.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется, если задание преимущественно выполнено

КМ-4. Оценивание стойкости криптографических преобразований и надежности шифров

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Контрольная работа проводится по вариантам. Работа содержит 4 задания на 20 минут

Краткое содержание задания:
Целью контрольной работы является проверка знания методов оценивания качества криптографических преобразований

Контрольные вопросы/задания:

Знать: методы оценки качества криптографических преобразований	1.Энтропия случайной величины. 2.Совместная и условная энтропия случайной величины 3.Совершенный шифр. 4.Теоретическая стойкость шифров. 5.Неопределенность шифра по ключу. 6.Имитостойкость шифров. Коды аутентификации и стратегии навязывания. 7.Нижние оценки вероятностей имитации и подмены

	сообщений.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется, если задание выполнено в полном объеме или выполнено преимущественно верно.

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется, если большинство вопросов раскрыто. выбрано верное направление для решения задач.

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется, если задание преимущественно выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7 семестр

Форма промежуточной аттестации: Зачет

Пример билета

1. 1.Шифры гаммирования и методы их вскрытия.
2. 2. Коды аутентификации и стратегии навязывания.
3. 3. Совершенный шифр

Процедура проведения

Зачет проводится в письменно-устной форме. На подготовку ответа дается 60 минут. Кроме ответа на вопросы билета, студент должен ответить на дополнительные вопросы.

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

1. Компетенция/Индикатор: ИД-5$_{ПК-2}$ Выбирает, модифицирует и реализует алгоритмы численной и алгебраической реализации математических моделей

Вопросы, задания

1.Формальные модели шифров: простой замены, перестановки, поточного шифра, блочного шифра.
2.Шифры гаммирования и методы их вскрытия.
3.Латинские квадраты, латинские прямоугольники, Ортогональные массивы.
4.Имитостойкость шифров. Коды аутентификации и стратегии навязывания.
5.Статистическая структура булевой функции и индуктивный метод ее построения.
6.Метрическая трактовка элементов преобразования Уолша-Адамара.
7.Энтропия случайной величины, энтропия и избыточность языка.
8.Совместная и условная энтропия случайных величин.
9.Неопределенность шифра по ключу. Расстояние единственности.
10.Построить алгебраическую модель кода аутентификации, в которой $X=A=Z\_3$ и $K=Z\_3 x Z\_3$, а преобразование аутентификации для ключа $(i,j)\backslash in\ K$ определятся соотношением $e\_\{i,j\}(x)=(ix+ j\ )$ mod 3.
11.Построить ортогональный массив OA(3,3,1)
12.Построить ортогональный массив OA(3,4,1)
13.Вычислить вероятности имитации четырех равномерно распределенных сообщений при использовании трех ключей k_1,k_2, k_3 с заданным распределением вероятностей (p(k_1),p(k_2),p(k_3)))=(½,¼,¼)
14.Построить оптимальную стратегию навязывания при задании четырех равномерно распределенных сообщений при использовании трех ключей k_1,k_2, k_3 с заданным распределением вероятностей (p(k_1),p(k_2),p(k_3)))=(½,¼,¼)
15.Применить отрезок бинарной гаммы для зашифрования отрезка бинарного текста той же длины.

Материалы для проверки остаточных знаний

1.Энтропия случайной величины равна нулю тогда и только тогда, когда принимает некоторое из n>2 значений с вероятностью (выбрать)

Ответы:

а. 1,
б. 0,
в. 0,5.

Верный ответ: а. 1.

2.Значение совместной энтропии двух случайных величин (выбрать) равно сумме значений энтропии каждой из этих величин.

Ответы:

а. равно сумме значений энтропии каждой из этих величин.
б. меньше или равно сумме значений энтропии каждой из этих величин.
в. больше или равно сумме значений энтропии каждой из этих величин.

Верный ответ: б. меньше или равно сумме значений энтропии каждой из этих величин.

3.Какой шифр называется совершенным?

Ответы:

а. совершенный шифр это шифр, для которого при любых x\in X, y\inY выполняется p(x/y)=p(x), или H(X/Y)=H(X), то есть распределения X и Y независимы, и по зашифрованному тексту y принципиально невозможно получение какой бы то ни было информации об открытом тексте x.
б. совершенный шифр это шифр, допускающий однозначное расшифрование.

Верный ответ: а.совершенный шифр это шифр, для которого при любых x\in X, y\inY выполняется p(x/y)=p(x), или H(X/Y)=H(X), то есть распределения X и Y независимы, и по зашифрованному тексту y принципиально невозможно получение какой бы то ни было информации об открытом тексте x.

4.Таблица совершенного шифрования является (выбрать)

Ответы:

а. латинским квадратом.
б. ортогональным массивом.

Верный ответ: а. латинским квадратом.

5.Таблица кода аутентификации задается (выбрать)

Ответы:

а. латинским квадратом,
б. латинским прямоугольником,
в. ортогональным массивом.

Верный ответ: в. ортогональным массивом.

6. Какие булевы функции и каким образом представляют столбцы матрицы Сильвестра-Адамара (выбрать)?

Ответы:

а. линейные,
б. аффинные,
в. нелинейные.

Верный ответ: а. линейные.

2. Компетенция/Индикатор: ИД-6$_{ПК-2}$ Демонстрирует понимание основ теории сложности реализации математических моделей

Вопросы, задания

1.Алгебраическая и вероятностная модели кода аутентификации. Вычисление вероятностей имитации и подмены сообщения.
2.Нижние оценки вероятностей имитации и подмены сообщений.
3.Преобразования Фурье и Уолша-Адамара булевой функции.
4.Статистические аналоги булевых функций. Бент функции. Расстояние до аффинных функций.

5.Теоретическая стойкость шифров. Совершенный шифр.

Материалы для проверки остаточных знаний

1.Условная энтропия $H(X/Y)$ определяет *меру неопределённости* шифра по (выбрать) открытому тексту.

Ответы:

а. открытому тексту.

б. шифр тексту.

Верный ответ: а. открытому тексту.

2.При каком числе переменных существуют бент-функции?

Ответы:

а. при четном числе переменных,

б. при нечетном числе переменных,

в. при любом числе переменных

Верный ответ: б. при нечетном числе переменных,

3.Преобразования, сохраняющие аффинность функции сохраняют расстояния до (выбрать)

Ответы:

а. аффинных функций,

б. бент-функций,

в. функций линейной структуры.

Верный ответ: а. аффинных функций,

4.Каков максимальный возможный порядок строгого лавинного критерия, которому может удовлетворять отображение от n переменных?

Ответы:

а. n,

б. *n-1,*

в. *n-2*

Верный ответ: в. n-2

5.Бент-отображения удовлетворяют СЛК и КР степени (выбрать).

Ответы:

а. n,

б. *n-1,*

в. *n-2*

Верный ответ: а. n.

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Оценка «ОТЛИЧНО» выставляется студенту, правильно выполнившему практическое задание, который показал при ответе на вопросы зачетного билета, и на дополнительные вопросы, что владеет материалом изученной дисциплины, свободно применяет свои знания для объяснения различных явлений и решения задач.

Оценка: 4

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Оценка «ХОРОШО» выставляется студенту, правильно выполнившему практическое задание и в основном правильно ответившему на вопросы зачетного билета (билета коллоквиума) и на дополнительные вопросы, но допустившему при этом непринципиальные ошибки.

Оценка: 3

Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка «УДОВЛЕТВОРИТЕЛЬНО» выставляется студенту, который в ответах на вопросы зачетного билета допустил существенные и даже грубые ошибки, но затем исправил их сам, а также не выполнил практическое задание из экзаменационного билета, но либо наметил правильный путь его выполнения, либо по указанию экзаменатора решил другую задачу из того же раздела дисциплины.

III. Правила выставления итоговой оценки по курсу

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»