

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

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очно-заочная

**Оценочные материалы
по дисциплине
Математические основы криптологии**

**Москва
2022**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Евтеев Б.В.
	Идентификатор	Rbb7ca24a-YevteevBV-e22a6fbb

(подпись)

Б.В. Евтеев

(расшифровка
подписи)

СОГЛАСОВАНО:

Руководитель
образовательной
программы

(должность, ученая степень, ученое
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

(подпись)

О.Р. Баронов

(расшифровка
подписи)

Заведующий
выпускающей кафедры

(должность, ученая степень, ученое
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

(подпись)

А.Ю.

Невский

(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. ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Контрольная работа №1 Основы модулярной арифметики (Контрольная работа)
2. Контрольная работа №2. Факторизация и дискретное логарифмирование (Контрольная работа)
3. Контрольная работа №3. Абелевы группы и вычисления в конечных полях (Контрольная работа)
4. Контрольная работа №4 Группы точек эллиптических кривых. (Контрольная работа)

БРС дисциплины

6 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Теоретико-числовые основы криптологии					
Введение.		+			
Тема 1. Основы модулярной арифметики.		+			
Тема 2. Генерация простых чисел, факторизация целых чисел и задача дискретного логарифмирования.			+		
Алгебраические основы криптологии					
Тема 3. Алгебраические системы.				+	
Тема 4. Элементы теории конечных групп.				+	
Тема 5. Элементы теории конечных полей, многочленов и эллиптических кривых над конечными полями.					+
Тема 6. Элементы криптографических приложений теории булевых функций.					+
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
ОПК-2	ОПК-2(Компетенция)	Знать: теоретико-числовые основы, используемые для защиты информации алгебраические основы, используемые для защиты информации Уметь: формулировать задачу и искать пути ее решения применять математические методы для решения задач обеспечения информационной безопасности	Контрольная работа №1 Основы модулярной арифметики (Контрольная работа) Контрольная работа №2. Факторизация и дискретное логарифмирование (Контрольная работа) Контрольная работа №3. Абелевы группы и вычисления в конечных полях (Контрольная работа) Контрольная работа №4 Группы точек эллиптических кривых. (Контрольная работа)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольная работа №1 Основы модулярной арифметики

Формы реализации: Письменная работа

Тип контрольного мероприятия: Контрольная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: Контрольная работа проводится в письменной форме. В шапке контрольной работы указывается: наименование предмета; номер группы, Ф.И.О. студента. Для выполнения контрольной работы предусматривается несколько вопросов. Время выполнения 2 академических часа. После проверки контрольной работы оглашаются результаты.

Краткое содержание задания:

Ответить на вопросы контрольной работы

Контрольные вопросы/задания:

Знать: теоретико-числовые основы, используемые для защиты информации	1.1. Сформулировать задачу линейаризации наибольшего общего делителя Решить задачу линейаризации наибольшего общего делителя трех чисел 2428 , 788 , 120.
--	---

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. Контрольная работа №2. Факторизация и дискретное логарифмирование

Формы реализации: Письменная работа

Тип контрольного мероприятия: Контрольная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: Контрольная работа проводится в письменной форме. В шапке контрольной работы указывается: наименование предмета; номер группы, Ф.И.О. студента. Для выполнения контрольной работы предусматривается несколько вопросов. Время выполнения 2 академических часа. После проверки контрольной работы оглашаются результаты.

Краткое содержание задания:

Ответить на вопросы контрольной работы

Контрольные вопросы/задания:

Знать: алгебраические основы, используемые для защиты информации	1. Сформулировать задачу факторизации целых чисел. 1. Выяснить методом выделения множителей Ферма является ли число 116939 простым или составным?
--	--

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. Контрольная работа №3. Абелевы группы и вычисления в конечных полях****Формы реализации:** Письменная работа**Тип контрольного мероприятия:** Контрольная работа**Вес контрольного мероприятия в БРС:** 25**Процедура проведения контрольного мероприятия:** Контрольная работа проводится в письменной форме. В шапке контрольной работы указывается: наименование предмета; номер группы, Ф.И.О. студента. Для выполнения контрольной работы предусматривается несколько вопросов. Время выполнения 2 академических часа. После проверки контрольной работы оглашаются результаты.**Краткое содержание задания:**

Ответить на вопросы контрольной работы

Контрольные вопросы/задания:

Уметь: применять математические методы для решения задач обеспечения информационной безопасности	1. Найти количество неизоморфных абелевых групп порядка 27648 и описать строение циклических групп этого порядка.
--	---

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. Контрольная работа №4 Группы точек эллиптических кривых.

Формы реализации: Письменная работа

Тип контрольного мероприятия: Контрольная работа

Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: Контрольная работа проводится в письменной форме. В шапке контрольной работы указывается: наименование предмета; номер группы, Ф.И.О. студента. Для выполнения контрольной работы предусматривается несколько вопросов. Время выполнения 2 академических часа. После проверки контрольной работы оглашаются результаты.

Краткое содержание задания:

Ответить на вопросы контрольной работы

Контрольные вопросы/задания:

Уметь: формулировать задачу и искать пути ее решения	1.Даны точки $P(58,139)$, $Q(67,667)$, на кривой $E751 (-1,1)$. Найти точку $P + Q$ 2.Для точки $R(82,481)$ эллиптической кривой $E751 (-1,1)$ найти точку $3R(82,481)$.
--	---

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

6 семестр

Форма промежуточной аттестации: Зачет с оценкой

Пример билета

НИУ МЭИ	БИЛЕТ №1 Кафедра <i>Безопасности и информационных технологий</i> Дисциплина «Математические основы криптологии»	Утверждаю: Зав. каф. БИТ А.Ю.Невский Протокол № «» от 20 г.
1. Разложение чисел на простые множители и функция Эйлера. 2. Линейная сложность последовательности. Алгоритм Берлекемпа-Мессис. 3. Практический вопрос. Найти нелинейность булевой функции $f(x) = (01011100)$.		

Процедура проведения

Зачет проводится в устной форме по билетам согласно программе зачета

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

1. Компетенция/Индикатор: ОПК-2(Компетенция)

Вопросы, задания

1. Сравнения и их свойства.
- 2.Расширенный алгоритм Евклида и его использование для формирования открытого и секретного ключей в системе шифрования RSA.
3. Разложение чисел на простые множители и функция Эйлера.
- 4.Теоремы Ферма (малая) и Эйлера. Обоснование криптосистемы RSA.
5. Функция Мебиуса и ее применение.
6. Система сравнений первой степени. Китайская теорема об остатках.
- 7.Симметрическая группа степени n . Представление ее элементов в виде произведения независимых циклов или транспозиций. Уравнение шифрования роторной машины Энигма.
8. Кольцо многочленов над конечным полем. Алгоритм деления в кольце многочленов над конечным полем и расширенный алгоритм Евклида.
- 9.Строение конечного поля.
- 10.Распределение ключей с использованием группы точек на эллиптической кривой.

Материалы для проверки остаточных знаний

- 1.Условие на идеал, при котором фактор-кольцо является полем

Ответы:

-

Верный ответ: Идеал должен быть максимальным.

- 2.Для группы из 10 элементов укажите невозможные варианты количества элементов ее подгрупп

Ответы:

-

Верный ответ: 3, 4, 6, 7, 8, 9

3. Решить рекуррентное соотношение: $a_n - a_{n-1} - 5 = 0$, при $a_0 = 9$.

Ответы:

-

Верный ответ: $5n + 9$

4. Решить сравнение $37X \equiv 25 \pmod{107}$

Ответы:

-

Верный ответ: $X \equiv 99 \pmod{107}$

5. Решить сравнение $111X \equiv 75 \pmod{321}$

Ответы:

-

Верный ответ: $X \equiv 99 \pmod{321}$, $X \equiv 206 \pmod{321}$, $X \equiv 313 \pmod{321}$

6. Решить систему сравнений $X \equiv 1 \pmod{4}$, $X \equiv 3 \pmod{5}$, $X \equiv 2 \pmod{7}$

Ответы:

-

Верный ответ: $X \equiv 93 \pmod{140}$

7. С помощью расширенного алгоритма Евклида решить задачу линейаризации для чисел 72 и 100

Ответы:

-

Верный ответ: Коэффициенты равны 7 и -5 соответственно.

8. Найти количество абелевых групп порядка 10

Ответы:

-

Верный ответ: 14

9. Найти количество неприводимых многочленов пятой степени над полем из двух элементов

Ответы:

-

Верный ответ: 6

Опишите группу точек эллиптической кривой $Y^2 = X^3 + X + 1$ над простым полем из семи элементов

10.

Ответы:

-

Верный ответ: Циклическая группа пятого порядка

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

III. Правила выставления итоговой оценки по курсу

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и зачетной составляющих.