

**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
Теоретико-числовые методы криптографии**

**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

2. ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Контрольная работа №1 Основы модулярной арифметики (Контрольная работа)
2. Контрольная работа №2. Простые числа и факторизация целых чисел (Контрольная работа)
3. Контрольная работа №3. Дискретное логарифмирование (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					
Введение		+			
Основы модулярной арифметики		+			
Эллиптические кривые				+	
Теоретико-числовые методы					
Простые числа и факторизация целых чисел			+	+	
Дискретное логарифмирование			+	+	
Применение теоретико-числовых методов в криптографии					

Асимметричные криптосистемы				+
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: достижения в теоретико-числовой области математики, используемые при решении задач защиты информации Уметь: определять требования к параметрам криптографических систем защиты информации	Контрольная работа №1 Основы модулярной арифметики (Контрольная работа) Контрольная работа №3. Дискретное логарифмирование (Контрольная работа)
ПК-10	ПК-10(Компетенция)	Знать: алгоритмы факторизации целых чисел и дискретного логарифмирования Уметь: применять теоретико-числовые методы для оценки стойкости криптографических систем	Контрольная работа №2. Простые числа и факторизация целых чисел (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: достижения в теоретико-числовой области математики, используемые при решении задач защиты информации	1.1. Сформулировать задачу линейаризации наибольшего общего делителя Решить задачу линейаризации наибольшего общего делителя трех чисел 2428 , 788 , 120. 2.1. Найти наибольший общий делитель двух чисел $6...6$ и $2...2$, где цифра 6 повторяется 101 раз, а цифра 2 повторяется 1000 раз.
---	---

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. Простые числа и факторизация целых чисел

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: алгоритмы факторизации целых чисел и дискретного логарифмирования	1.Сформулировать задачу факторизации целых чисел. 2.Назовите известные вам методы проверки чисел на простоту
--	---

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. 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:

Уметь: определять требования к параметрам криптографических систем защиты информации	Найти LOG_{56} в кольце классов вычетов по модулю 43 методом Шэнкса 1. Найти LOG_{754} в кольце классов вычетов по модулю 61 методом Полига-Силвера-Хеллмана. 2.
--	---

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: применять теоретико-числовые методы для оценки стойкости криптографических систем	1. Даны точки $P(58,139)$, $Q(67,667)$, на кривой $E_{751}(-1,1)$. Найти точку $P + Q$ 2. Для точки $R(82,481)$ эллиптической кривой $E_{751}(-1,1)$ 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 «Теоретико-числовые методы криптографии»	Утверждаю: Зав. каф. БИТ
		(подпись).
1. Сравнения и их свойства. 2. Разложение чисел на простые множители и функция Эйлера 3. Практический вопрос: Решить задачу линеаризации наибольшего общего делителя трех чисел 2428, 788 и 120.		

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.Теоремы Ферма (малая) и Эйлера. Обоснование криптосистемы RSA.

Материалы для проверки остаточных знаний

- 1.Задача линеаризации наибольшего общего делителя чисел имеет единственное решение или нет

Ответы:

-

Верный ответ: Нет

2. Компетенция/Индикатор: ПК-10(Компетенция)

Вопросы, задания

- 1.Метод Ферма проверки числа на простоту.
- 2.Метод Полларда -Флойда
- 3.Алгоритм Полига-Хеллмана
- 4.Криптографическая система RSA

Материалы для проверки остаточных знаний

- 1.Является ли группа точек эллиптической кривой абелевой группой

Ответы:

-

Верный ответ: Да

2.К какому виду тестов относится тест Соловья-Штрассена?

Ответы:

-

Верный ответ: К вероятностным тестам

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.