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

Рабочая программа дисциплины
СОВРЕМЕННАЯ КОМПЬЮТЕРНАЯ АЛГЕБРА

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.15.01.02**
Трудоемкость в зачетных единицах:	**6 семестр - 4; 7 семестр - 4; всего - 8**
Часов (всего) по учебному плану:	**288 часа**
Лекции	**6 семестр - 28 часа; 7 семестр - 32 часа; всего - 60 часов**
Практические занятия	**6 семестр - 28 часа; 7 семестр - 32 часа; всего - 60 часов**
Лабораторные работы	**не предусмотрено учебным планом**
Консультации	**6 семестр - 2 часа; 7 семестр - 2 часа; всего - 4 часа**
Самостоятельная работа	**6 семестр - 85,5 часа; 7 семестр - 77,5 часа; всего - 163,0 часа**
в том числе на КП/КР	**не предусмотрено учебным планом**
Иная контактная работа	**проводится в рамках часов аудиторных занятий**
включая: Проверочная работа Тестирование	
Промежуточная аттестация:	
Экзамен Экзамен	**6 семестр - 0,5 часа; 7 семестр - 0,5 часа; всего - 1,0 час**

Москва 2020

ПРОГРАММУ СОСТАВИЛ:

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)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: состоит в изучении и освоении математических и компьютерных моделей, методов и алгоритмов современной компьютерной алгебры

Задачи дисциплины

- изучение алгоритмов операций в различных алгебраических структурах;
- освоение методов генерации и анализа псевдослучайных последовательностей, тестирования и генерации простых чисел, неприводимых и примитивных многочленов;
- освоение подходов к решению задач целочисленной факторизации и дискретного логарифмирования;
- освоение примеров применения современной компьютерной алгебры в теории кодирования и криптографии.

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 участвовать в компьютерной реализации математических моделей	ИД-1$_{ПК-2}$ Демонстрирует знание терминологии, базовых результатов и методов фундаментальной математики	знать: - основные алгебраические структуры; - принципы преобразования информации алгебраическими методами, в частности, с применением структуры полугруппы. уметь: - применять основные определения и свойства полугрупп; - применять современную компьютерную алгебру в теории кодирования и криптографии; - применять основные алгебраические структуры.
ПК-2 Способен участвовать в компьютерной реализации математических моделей	ИД-3$_{ПК-2}$ Использует базовые знания и методы фундаментальной математики для анализа простейших свойств математических моделей	уметь: - использовать алгоритмы тестирования алгебраических примитивов при построении основанных на них алгебраических систем.
ПК-2 Способен участвовать в компьютерной реализации математических моделей	ИД-5$_{ПК-2}$ Выбирает, модифицирует и реализует алгоритмы численной и алгебраической реализации математических моделей	уметь: - применять алгоритмы операций в различных алгебраических структурах; - разрабатывать алгоритмы алгебраических преобразований и алгоритмы численной и алгебраической реализации математических моделей.
ПК-2 Способен участвовать в компьютерной реализации математических моделей	ИД-6$_{ПК-2}$ Демонстрирует понимание основ теории сложности реализации математических моделей	знать: - подходы к решению задач целочисленной факторизации и дискретного логарифмирования. уметь:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
		- ускорять алгебраические вычисления.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Математическое моделирование (далее – ОПОП), направления подготовки 01.03.02 Прикладная математика и информатика, уровень образования: высшее образование - бакалавриат.

Требования к входным знаниям и умениям:

- знать общую алгебру, дискретную математику, теорию вероятностей и математическую статистику

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 8 зачетных единиц, 288 часа.

№ 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	Алгебры и подалгебры	20	6	6	-	6	-	-	-	-	-	8	-	***Изучение материалов литературных источников:*** [7], с. 4-29
1.1	Алгебры и подалгебры	20		6	-	6	-	-	-	-	-	8	-	
2	Проблема полноты в алгебрах	20		6	-	6	-	-	-	-	-	8	-	***Изучение материалов литературных источников:*** [1], с. 31-40
2.1	Проблема полноты в алгебрах	20		6	-	6	-	-	-	-	-	8	-	
3	Решетки понятий и шкалы	8		2	-	2	-	-	-	-	-	4	-	***Изучение материалов литературных источников:*** [5], с. 71-76
3.1	Решетки понятий и шкалы	8		2	-	2	-	-	-	-	-	4	-	
4	Полугруппы	16		4	-	4	-	-	-	-	-	8	-	***Изучение материалов литературных источников:*** [1], с. 41-48, 49-60 [8], с. 253-289
4.1	Полугруппы	16		4	-	4	-	-	-	-	-	8	-	
5	Кольца	12		2	-	2	-	-	-	-	-	8	-	***Изучение материалов литературных источников:*** [1], с. 61-70 [5], с. 390-401
5.1	Кольца	12		2	-	2	-	-	-	-	-	8	-	
6	Модулярная арифметика	16		4	-	4	-	-	-	-	-	8	-	***Изучение материалов литературных источников:*** [8], с. 88-101
6.1	Модулярная арифметика	16		4	-	4	-	-	-	-	-	8	-	
7	Поля и их применение в кодировании	16		4	-	4	-	-	-	-	-	8	-	***Изучение материалов литературных источников:*** [8], с. 230-252
7.1	Поля и их применение	16		4	-	4	-	-	-	-	-	8	-	

	в кодировании													
	Экзамен	36.0		-	-	-	-	2	-	-	0.5	-	33.5	
	Всего за семестр	**144.0**		**28**	**-**	**28**	**-**	**2**	**-**	**-**	**0.5**	**52**	**33.5**	
	Итого за семестр	**144.0**		**28**	**-**	**28**	**2**		**-**		**0.5**	**85.5**		
8	Методы ускорения алгебраических вычислений	14	7	4	-	4	-	-	-	-	-	6	-	***Самостоятельное изучение теоретического материала:*** Повторение материала по разделу «Методы ускорения алгебраических вычислений». ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу «Методы ускорения алгебраических вычислений». ***Подготовка к текущему контролю:*** Подготовка к тесту № 5: «Методы ускорения алгебраических вычислений, квадратичные вычеты и квадратные корни». ***Изучение материалов литературных источников:*** [2], с. 22-34, с. 194-237 [6], с. 5-10
8.1	Методы ускорения алгебраических вычислений	14		4	-	4	-	-	-	-	-	6	-	
9	Квадратичное вычеты и квадратные корни	14		4	-	4	-	-	-	-	-	6	-	***Самостоятельное изучение теоретического материала:*** Повторение материала по разделу «Квадратичные вычеты и квадратные корни». ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу «Квадратичные вычеты и квадратные корни». ***Подготовка к текущему контролю:*** Подготовка к тесту № 5: «Методы ускорения алгебраических вычислений, квадратичные вычеты и квадратные корни». ***Изучение материалов литературных источников:*** [2], с. 92-99 [3], с. 48-57
9.1	Квадратичное вычеты и квадратные корни	14		4	-	4	-	-	-	-	-	6	-	
10	Генерация и	13		4	-	4	-	-	-	-	-	5	-	***Самостоятельное изучение***

	тестирование простых чисел и неприводимых многочленов													***теоретического материала:*** Повторение материала по разделу "Генерация и тестирование простых чисел и неприводимых многочленов".
10.1	Генерация и тестирование простых чисел и неприводимых многочленов	13		4	-	4	-	-	-	-	-	5	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Генерация и тестирование простых чисел и неприводимых многочленов". ***Подготовка к текущему контролю:*** Подготовка к тесту № 6 :«Методы тестирования и генерации простых чисел, неприводимых и примитивных многочленов». ***Изучение материалов литературных источников:*** [2], с. 139-155 [3], с. 5-6
11	Генерация и анализ псевдослучайных последовательностей	13		4	-	4	-	-	-	-	-	5	-	***Самостоятельное изучение теоретического материала:*** Повторение материала по разделу "Генерация и анализ псевдослучайных последовательностей".
11.1	Генерация и анализ псевдослучайных последовательностей	13		4	-	4	-	-	-	-	-	5	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Генерация и анализ псевдослучайных последовательностей". ***Подготовка к текущему контролю:*** Подготовка к тесту № 6:«Методы тестирования и генерации простых чисел, неприводимых и примитивных многочленов». ***Изучение материалов литературных источников:*** [3], с. 6-18, 35-47
12	Алгоритмы факторизации и дискретного логарифмирования	13		4	-	4	-	-	-	-	-	5	-	***Самостоятельное изучение теоретического материала:*** Повторение материала по разделу "Алгоритмы факторизации и дискретного

12.1	Алгоритмы факторизации и дискретного логарифмирования	13		4	-	4	-	-	-	-	-	5	-	логарифмирования". ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Алгоритмы факторизации и дискретного логарифмирования". ***<u>Подготовка к текущему контролю:</u>*** Подготовка к тесту № 7: «Алгоритмы факторизации и дискретного логарифмирования». ***<u>Изучение материалов литературных источников:</u>*** [2], с. 128-159
13	Эллиптические кривые. Группа точек эллиптической кривой	13		4	-	4	-	-	-	-	-	5	-	***<u>Самостоятельное изучение теоретического материала:</u>*** Повторение материала по разделу "Эллиптические кривые. Группа точек эллиптической кривой". ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Эллиптические кривые. Группа точек эллиптической кривой". ***<u>Подготовка к текущему контролю:</u>*** Подготовка к тесту № 8: «Элементы эллиптической криптографии». ***<u>Изучение материалов литературных источников:</u>*** [4], с. 92-98 [6], с. 11-22
13.1	Эллиптические кривые. Группа точек эллиптической кривой	13		4	-	4	-	-	-	-	-	5	-	
14	Генерация точек и представление данных в группе точек эллиптической кривой	14		4	-	4	-	-	-	-	-	6	-	***<u>Самостоятельное изучение теоретического материала:</u>*** Повторение материала по разделу "Генерация точек и представление данных в группе точек эллиптической кривой". ***<u>Самостоятельное изучение теоретического материала:</u>*** Изучение дополнительного материала по разделу "Генерация точек и представление данных в
14.1	Генерация точек и представление данных в группе точек эллиптической кривой	14		4	-	4	-	-	-	-	-	6	-	

														группе точек эллиптической кривой". ***Подготовка к текущему контролю:*** Подготовка к тесту № 8:«Элементы эллиптической криптографии». ***Изучение материалов литературных источников:*** [4], с. 98-109 [6], с. 23-54
15	Применение эллиптических кривых в криптографии	14		4	-	4	-	-	-	-	-	6	-	***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу по разделу "Применение эллиптических кривых в криптографии". ***Самостоятельное изучение теоретического материала:*** Повторение материала по разделу "Применение эллиптических кривых в криптографии". ***Подготовка к текущему контролю:*** Подготовка к тесту № 8: «Элементы эллиптической криптографии». ***Изучение материалов литературных источников:*** [4], с. 109-120 [6], с. 55-70
15.1	Применение эллиптических кривых в криптографии	14		4	-	4	-	-	-	-	-	6	-	
	Экзамен	36.00		-	-	-	-	2	-	-	0.5	-	33.50	
	Всего за семестр	**144.00**		**32**	**-**	**32**	**-**	**2**	**-**	**-**	**0.5**	**44**	**33.50**	
	Итого за семестр	**144.00**		**32**	**-**	**32**	**2**		**-**		**0.5**	**77.50**		
	ИТОГО	**288.00**	**-**	**60**	**-**	**60**	**4**		**-**		**1.0**	**163.00**		

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. Алгебры и подалгебры

1.1. Алгебры и подалгебры

Операция на множестве. Замыкание относительно операций. Замкнутые множества. Универсальная алгебра, ее тип и сигнатура. Примеры: алгебра комплексных чисел и ее подалгебры, алгебра множеств, алгебра матриц, алгебра многочленов, алгебра случайных событий, линейное пространство. Гомоморфизм и изоморфизм. Функциональные системы и их примеры.

2. Проблема полноты в алгебрах

2.1. Проблема полноты в алгебрах

Полные системы, базисы, конечная и бесконечная порождаемость. Свойства конечно порожденной алгебры. Предполные классы. Критериальные системы. Критерий полноты в конечно порожденной алгебре.

3. Решетки понятий и шкалы

3.1. Решетки понятий и шкалы

Булева алгебра. Конечные булевы алгебры. Теорема Стоуна, атомы решетки. Решетки понятий как примеры булевых алгебр и шкалы как примеры полных систем. Минимальная шкала., Шкала в произведении решеток понятий.

4. Полугруппы

4.1. Полугруппы

Полугруппа как пример алгебры с одной ассоциативной бинарной операцией. Алгоритм проверки ассоциативности. Полугруппы преобразований. Полугруппы слов. Циклические полугруппы, их индекс и порядок. Изоморфизм полугрупп. Группа. Группа автоморфизмов графа. Цикловой индекс. Число геометрически различных окрасок вершин графа. Задача об ожерельях.

5. Кольца

5.1. Кольца

Кольцо как пример алгебры с двумя бинарными операциями. Делители нуля. Кольцо многочленов.

6. Модулярная арифметика

6.1. Модулярная арифметика

Кольцо вычетов по модулю m. Система линейных уравнений по модулю m. Полиномиальные уравнения. Полиномиальная реализация функций k- значной логики. Китайская теорема об остатках. Многомодульная арифметика. Контроль вычислений.

7. Поля и их применение в кодировании

7.1. Поля и их применение в кодировании

Поле как частный случай кольца. Конечное поле, его характеристика, порядок, единственность с точностью до изоморфизма. Построение поля путем расширения.

Примеры: поле комплексных чисел как расширение поля действительных чисел. Поле многочленов над простым полем как расширение этого простого поля. Три способа представления конечного поля: полиномиальный, степенной и векторный. Уравнения в конечном поле. Линейный код, его матрицы, кодовое расстояние и корректирующие способности. Частные случаи линейных кодов: коды с повторениями, бинарный код проверки на четность, коды Хэмминга, циклические коды.

8. Методы ускорения алгебраических вычислений

8.1. Методы ускорения алгебраических вычислений

Сложение, умножение и деление в кольцах целых чисел и многочленов над конечным полем. Расширенный алгоритм Евклида. Обращение элемента конечного кольца или поля. Возведение в степень в кольце и в поле. Возведение элемента поля в степень, равную характеристике поля. Нахождение образующих элементов и элементов максимального порядка. Метод умножения Карацубы. Метод умножения и возведения в степень Монтгомери. Метод Штрассена умножения матриц. Варианты китайской теоремы об остатках. Оценка сложности рекурсивных алгоритмов..

9. Квадратичное вычеты и квадратные корни

9.1. Квадратичное вычеты и квадратные корни

Квадратичные вычеты и квадратичные невычеты. Символы Лежандра и Якоби и их свойства, рекурсивный алгоритм их вычисления. Числа блома и их свойства. Алгоритмы извлечения квадратных корней по простому модулю. Проблемы квадратного корня и квадратичного вычета. Применение в криптографии: криптосистемы Рабина и Блюма-Голлдвассер.

10. Генерация и тестирование простых чисел и неприводимых многочленов

10.1. Генерация и тестирование простых чисел и неприводимых многочленов

Критерии разложимости и простоты чисел. Генерация больших простых чисел. Алгоритмы тестирования неприводимости многочлена над конечным полем. Алгоритмы генерации неприводимых многочленов.

11. Генерация и анализ псевдослучайных последовательностей

11.1. Генерация и анализ псевдослучайных последовательностей

Линейные рекуррентные последовательности (ЛРП) над конечным полем. Статистические свойства ЛРП максимального периода, формула общего члена ЛРП. Линейные конгруэнтные последовательности (ЛКП) над конечным полем. Первообразные элементы и их получение.

12. Алгоритмы факторизации и дискретного логарифмирования

12.1. Алгоритмы факторизации и дискретного логарифмирования

Проблемы факторизации и дискретного логарифмирования. Метод Ферма факторизации, ро-метод и метод факторных баз и другие методы факторизации. Метод согласавания дискретного логарифмирования. Субэкспоненциальные алгоритмы факторизации и дискретного логарифмирования: метод квадратичного решета и индексный метод. Применение в криптографии: криптосистемы RSA и Диффи-Хеллмана.

13. Эллиптические кривые. Группа точек эллиптической кривой

13.1. Эллиптические кривые. Группа точек эллиптической кривой

Уравнение эллиптической кривой в форме Вейерштрасса и его разновидности для кривых над полями характеристики два, три и больше трех. Группа точек эллиптической кривой. Эллиптические кривые над конечными полями. Порядок кривой и порядок точки эллиптической кривой. Сложение, удвоение и скалярное умножение в группе точек в аффинных и проективных координатах. Нахождениеобразующего элемента или элемента максимального порядка эллиптической кривой.

14. Генерация точек и представление данных в группе точек эллиптической кривой

14.1. Генерация точек и представление данных в группе точек эллиптической кривой

Методы решения квадратного уравнения над конечным полем характеристики два. Критерий существования решения. Генерация элемента группы точек суперсингулярной эллиптической кривой над полем характеристики два. Генерация элемента группы точек несуперсингулярной эллиптической кривой над полем характеристики два. Вложение данных в x-координату точки эллиптической кривой.

15. Применение эллиптических кривых в криптографии

15.1. Применение эллиптических кривых в криптографии

Проблема Диффи-Хеллмана в группе точек эллиптической кривой. Протоколы распределения ключей в компьютерной сети по этому протоколу и его модификациям. Передача ключа по открытым каналам: протокол Месси-Омуры. Особенности российского стандарта электронной подписи.

3.3. Темы практических занятий

1. Проверка ассоциативности методом Лайта. Построение полугрупп преобразований;
2. Построение групп автоморфизмов графов, вычисление циклового индекса и геометрически различных окрасок;
3. Вычисления в различных кольцах. Решение уравнений в модулярной арифметике, построение полиномиальных формул для функций k-значной логики;
4. Построение полей небольшого порядка. Решение уравнений;
5. Кодирование и декодирование с помощью линейных кодов;
6. Методы ускорения алгебраических вычислений;
7. Алгоритмы факторизации и дискретного логарифмирования;
8. Генерация и тестирование простых чисел и неприводимых многочленов;
9. Генерация и анализ псевдослучайных последовательностей;
10. Эллиптические кривые. Группа точек эллиптической кривой;
11. Генерация точек и представление данных в группе точек эллиптической кривой;
12. Применение эллиптических кривых в криптографии;
13. Нахождение предполных классов, критериев полноты, базисов, шкал в решетках понятий;
14. Квадратичное вычеты и квадратные корни;
15. Проверка замкнутости множеств. Нахождение подалгебр и построение их решетки.

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Алгебры и подалгебры"
2. Обсуждение материалов по кейсам раздела "Проблема полноты в алгебрах"
3. Обсуждение материалов по кейсам раздела "Решетки понятий и шкалы"
4. Обсуждение материалов по кейсам раздела "Полугруппы"
5. Обсуждение материалов по кейсам раздела "Кольца"
6. Обсуждение материалов по кейсам раздела "Модулярная арифметика"
7. Обсуждение материалов по кейсам раздела "Поля и их применение в кодировании"
8. Обсуждение материалов по кейсам раздела "Методы ускорения алгебраических вычислений"
9. Обсуждение материалов по кейсам раздела "Квадратичное вычеты и квадратные корни"
10. Обсуждение материалов по кейсам раздела "Генерация и тестирование простых чисел и неприводимых многочленов"
11. Обсуждение материалов по кейсам раздела "Генерация и анализ псевдослучайных последовательностей"
12. Обсуждение материалов по кейсам раздела "Алгоритмы факторизации и дискретного логарифмирования"
13. Обсуждение материалов по кейсам раздела "Эллиптические кривые. Группа точек эллиптической кривой"
14. Обсуждение материалов по кейсам раздела "Генерация точек и представление данных в группе точек эллиптической кривой"
15. Обсуждение материалов по кейсам раздела "Применение эллиптических кривых в криптографии"

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

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	3	4	5	6	7	8	9	10	11	12	13	14	15	
Знать:																	
принципы преобразования информации алгебраическими методами, в частности, с применением структуры полугруппы	ИД-1$_{ПК-2}$				+												Проверочная работа/Полугруппы
основные алгебраические структуры	ИД-1$_{ПК-2}$	+	+														Проверочная работа/Проблемы полноты в алгебрах
подходы к решению задач целочисленной факторизации и дискретного логарифмирования	ИД-6$_{ПК-2}$												+				Тестирование/Алгоритмы факторизации и дискретного логарифмирования
Уметь:																	
применять основные алгебраические структуры	ИД-1$_{ПК-2}$	+	+														Проверочная работа/Проблемы полноты в алгебрах
применять современную компьютерную алгебру в теории кодирования и криптографии	ИД-1$_{ПК-2}$					+	+	+									Проверочная работа/Помехоустойчивое кодирование
применять основные определения и свойства полугрупп	ИД-1$_{ПК-2}$				+												Проверочная работа/Полугруппы
использовать алгоритмы тестирования алгебраических примитивов	ИД-3$_{ПК-2}$										+	+					Тестирование/Методы анализа и генерации простых чисел, неприводимых многочленов и

при построении основанных на них алгебраических систем																	псевдослучайных последовательностей
разрабатывать алгоритмы алгебраических преобразований и алгоритмы численной и алгебраической реализации математических моделей	ИД-5$_{ПК-2}$													+	+	+	Тестирование/Элементы эллиптической криптографии
применять алгоритмы операций в различных алгебраических структурах	ИД-5$_{ПК-2}$			+													Проверочная работа/Решётки
ускорять алгебраические вычисления	ИД-6$_{ПК-2}$								+	+							Тестирование/Методы ускорения алгебраических вычислений, квадратичные вычеты и квадратные корни

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

4.1. Текущий контроль успеваемости

6 семестр

Форма реализации: Проверка задания

1. Полугруппы (Проверочная работа)
2. Помехоустойчивое кодирование (Проверочная работа)
3. Проблемы полноты в алгебрах (Проверочная работа)
4. Решётки (Проверочная работа)

7 семестр

Форма реализации: Билеты (письменный опрос)

1. Алгоритмы факторизации и дискретного логарифмирования (Тестирование)
2. Методы анализа и генерации простых чисел, неприводимых многочленов и псевдослучайных последовательностей (Тестирование)
3. Методы ускорения алгебраических вычислений, квадратичные вычеты и квадратные корни (Тестирование)
4. Элементы эллиптической криптографии (Тестирование)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №6)

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

Экзамен (Семестр №7)

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

В диплом выставляется оценка за 7 семестр.

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Болотов, А. А. Алгебраические структуры : учебное пособие по курсам "Линейная алгебра и аналитическая геометрия", "Дискретная математика" для слушателей ФПКП по направлению "Прикладная математика и информатика" / А. А. Болотов, Д. Г. Мещанинов, А. Б. Фролов, Моск. энерг. ин-т (МЭИ ТУ) . – М. : Изд-во МЭИ, 2005 . – 80 с. - ISBN 5-7046-1312-8 .;
2. 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 .;
3. Фролов, А. Б. Псевдослучайные последовательности. Лабораторный практикум по криптографическим методам защиты информации : учебное пособие по курсам

"Математические основы криптографии", "Криптографические методы защиты информации" по направлениям 230100 "Вычислительная техника и информатика", 010500 "Прикладная математика и информатика" / А. Б. Фролов, Нац. исслед. ун-т "МЭИ" . – М. : Издательский дом МЭИ, 2012 . – 100 с. - ISBN 978-5-383-00722-8 . http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=4056;
4. 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 .;
5. Гашков, С. Б. Дискретная математика : учебник и практикум для студентов вузов, обучающихся по естественнонаучным направлениям / С. Б. Гашков, А. Б. Фролов . – 3-е изд., испр. и доп . – Москва : Юрайт, 2020 . – 483 с. – (Высшее образование) . - ISBN 978-5-534-11613-7 .;
6. Болотов, А. А. Криптографические протоколы на эллиптических кривых : учебное пособие по курсу "Криптографические методы защиты информации" по всем направлениям / А. А. Болотов, С. Б. Гашков, А. Б. Фролов, Моск. энерг. ин-т (МЭИ ТУ) . – М. : Издательский дом МЭИ, 2007 . – 84 с. - ISBN 978-5-383-00093-9 .;
7. Мамонтов, А. И. Указания к решению задач по общей алгебре. Основы дискретных математических моделей : методическое пособие по курсу "Общая алгебра" по направлению "Прикладная математика и информатика" / А. И. Мамонтов, Д. Г. Мещанинов, Нац. исслед. ун-т "МЭИ" . – М. : Изд-во МЭИ, 2015 . – 32 с. http://elib.mpei.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=7485;
8. Гаврилов Г. П., Сапоженко А. А.- "Задачи и упражнения по дискретной математике", (3-е изд., перераб.), Издательство: "ФИЗМАТЛИТ", Москва, 2009 - (416 с.) https://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=2157.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
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	М-710, Учебная аудитория каф. МКМ	стол преподавателя, стол учебный, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения практических занятий, КР и КП	М-710, Учебная аудитория каф. МКМ	стол преподавателя, стол учебный, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для	М-808, Учебная	стол учебный, стул, доска меловая

проведения промежуточной аттестации	аудитория	
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	М-714, Преподавательская каф. МКМ	рабочее место сотрудника, стул, шкаф, шкаф для документов, шкаф для одежды, тумба, доска меловая, мультимедийный проектор, экран, книги, учебники, пособия
Помещения для хранения оборудования и учебного инвентаря	М-301/1, Кладовая	стул
	М-713/1, Учебно-научная лаборатория каф. МКМ	рабочее место сотрудника, стул, шкаф, шкаф для одежды, тумба, компьютерная сеть с выходом в Интернет, компьютер персональный, книги, учебники, пособия

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Современная компьютерная алгебра

(название дисциплины)

6 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по дисциплине:
КМ-1 Проблемы полноты в алгебрах (Проверочная работа)
КМ-2 Решётки (Проверочная работа)
КМ-3 Полугруппы (Проверочная работа)
КМ-4 Помехоустойчивое кодирование (Проверочная работа)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	7	10	13
1	Алгебры и подалгебры					
1.1	Алгебры и подалгебры		+			
2	Проблема полноты в алгебрах					
2.1	Проблема полноты в алгебрах		+			
3	Решетки понятий и шкалы					
3.1	Решетки понятий и шкалы			+		
4	Полугруппы					
4.1	Полугруппы				+	
5	Кольца					
5.1	Кольца					+
6	Модулярная арифметика					
6.1	Модулярная арифметика					+
7	Поля и их применение в кодировании					
7.1	Поля и их применение в кодировании					+
		Вес КМ, %:	25	25	25	25

7 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

КМ-5 Методы ускорения алгебраических вычислений, квадратичные вычеты и квадратные корни (Тестирование)

КМ-6 Методы анализа и генерации простых чисел, неприводимых многочленов и псевдослучайных последовательностей (Тестирование)

КМ-7 Алгоритмы факторизации и дискретного логарифмирования (Тестирование)

КМ-8 Элементы эллиптической криптографии (Тестирование)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-5	КМ-6	КМ-7	КМ-8
		Неделя КМ:	4	8	12	15
1	Методы ускорения алгебраических вычислений					
1.1	Методы ускорения алгебраических вычислений		+			
2	Квадратичное вычеты и квадратные корни					
2.1	Квадратичное вычеты и квадратные корни		+			
3	Генерация и тестирование простых чисел и неприводимых многочленов					
3.1	Генерация и тестирование простых чисел и неприводимых многочленов			+		
4	Генерация и анализ псевдослучайных последовательностей					
4.1	Генерация и анализ псевдослучайных последовательностей			+		
5	Алгоритмы факторизации и дискретного логарифмирования					
5.1	Алгоритмы факторизации и дискретного логарифмирования				+	
6	Эллиптические кривые. Группа точек эллиптической кривой					
6.1	Эллиптические кривые. Группа точек эллиптической кривой					+
7	Генерация точек и представление данных в группе точек эллиптической кривой					
7.1	Генерация точек и представление данных в группе точек эллиптической кривой					+
8	Применение эллиптических кривых в криптографии					
8.1	Применение эллиптических кривых в криптографии					+
		Вес КМ, %:	25	25	25	25