ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПРАВОСЛАВНЫЙ СВЯТО-ТИХОНОВСКИЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ»
(ПСТГУ)

Факультет информатики и прикладной математики
Кафедра информатики

УТВЕРЖДАЮ

Проректор по учебной работе

_____ / Тарасова И.В. /

«_03_» ____04____ 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Математические основы компьютерной алгебры»

02.03.03 Математическое обеспечение и администрирование информационных систем

Профиль подготовки:
Администрирование информационных систем

Квалификация выпускника: бакалавр

Форма обучения: очная

Москва, 2021 г.

Год начала обучения по учебному плану: 2019

1. Цели освоения дисциплины

Целями освоения дисциплины являются ознакомление студентов с основными алгебраическими системами и возможностями из применения для решения прикладных задач.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к блоку Б1.В.ДВ.04.02 вариативной части (дисциплины по выбору) образовательной программы.

Дисциплина изучается на 3 курсе, в 6 семестре.

Для изучения дисциплины необходимы знания, умения и навыки, сформированные в процессе изучения дисциплин «Линейная алгебра», «Алгебра и теория чисел», «Информатика», «Программирование».

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины обучающийся должен продемонстрировать следующие результаты:

Коды компетенций	Наименование компетенции	Перечень планируемых результатов обучения по дисциплине
ОПК-1	Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности	В результате освоения дисциплины обучающийся должен **ЗНАТЬ:** • важнейшие свойства алгебраических систем. **УМЕТЬ:** • использовать аналитический аппарат компьютерной алгебры • доказывать основные свойства фактор-групп (фактор-колец) • доказывать основные свойства колец (полей) вычетов **ВЛАДЕТЬ:** навыками исследования свойств основных объектов компьютерной алгебры.
ПК-1	Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий	В результате освоения дисциплины обучающийся должен **ЗНАТЬ:** • основные понятия абстрактной и компьютерной алгебры, • основные классы алгебраических систем и их примеры. **УМЕТЬ:** • формулировать типичные прикладные задачи на языке компьютерной алгебры; • применять методы компьютерной алгебры к решению вычислительных задач. **ВЛАДЕТЬ:** навыками исследования свойств основных объектов компьютерной алгебры.

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 5 зачетные единицы, 180 академических часов.

На учебные занятия лекционного типа отводится 36 часов,

на занятия практического (семинарского) типа — 36 часов.

Самостоятельная работа составляет 108 часов.

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Тематические разделы дисциплины и компетенции, которые формируются при их изучении

№ п/п	Наименование раздела дисциплины	Содержание раздела	Код формируемой компетенции
1.	Классификация и структура систем компьютерной алгебры	Аппаратные требования. Системы компьютерной математики для численных расчетов. Универсальные системы компьютерной математики. Задачи, решаемые системами компьютерной алгебры.	ОПК-1; ПК-1
2.	Основные виды алгебраических систем.	Полугруппы, моноиды, группы, коммутативные группы, кольца, поля, булевы алгебры. Алгебры, алгебраические системы. Теория делимости в кольце целых чисел. Кольца класса вычетов. Поле комплексных чисел	ОПК-1; ПК-1
3.	Идеалы и факторкольца. Кольцо многочленов.	Подгруппы. Смежные классы по подгруппе, факторгруппы. Подкольца. Идеалы кольца, факторкольца. Кольцо многочленов от одной переменной, теорема делимости. Многочлены от нескольких переменных.	ОПК-1; ПК-1
4.	Первоначальное представление о теории кодирования.	Криптография с секретным ключом: шифры Цезаря, Виженера, Кардано, скиталы.	ОПК-1; ПК-1
5.	Криптография с открытым ключом.	Односторонняя функция, алгоритм RSA, подбор параметров: генерация псевдопростых чисел.	ОПК-1; ПК-1
6.	Криптоанализ, пассивные атаки.	Факторизация модуля, проблема инвариантных блоков, атака "малых показателей". Активная атака,	ОПК-1; ПК-1

		хеширование, атака "парадокса дней рождения".	
7.	Аутентификация, цифровая подпись	Шифрование по алгоритму Эль-Гамаля.	ОПК-1; ПК-1
8.	Элементы компьютерной алгебры	Типы данных математических систем.	ОПК-1; ПК-1
9.	Системы счисления.	Правила ввода и вывода чисел.	ОПК-1; ПК-1
10.	Операции символьной математики.	Установка форматов вывода результатов символьных исчислений.	ОПК-1; ПК-1
11.	Представление символьных данных в компьютере.	Представление символьных данных в компьютере.	ОПК-1; ПК-1
12.	Алгоритмы символьных преобразований (числа, многочлены, выражения).	Алгоритмы символьных преобразований (числа, многочлены, выражения).	ОПК-1; ПК-1
13.	Алгоритмы символьных преобразований (дифференцирование).	Алгоритмы символьных преобразований (дифференцирование).	ОПК-1; ПК-1
14.	Алгоритмы символьных преобразований (интегрирование).	Алгоритмы символьных преобразований (интегрирование).	ОПК-1; ПК-1

5.2. Разделы дисциплины, виды учебных занятий и формы текущего контроля успеваемости

№ семестра	**Наименование раздела дисциплины (модуля)**	**Трудоемкость в часах**					**Формы СРС**	**Формы текущего контроля**	**Формы текущего контроля с указанием баллов (при использовании балльной системы оценивания)**
		Всего (вкл. СРС)	На контактную работу по видам учебных занятий		На СРС	Контроль			
			Л	ПЗ					
1.	Классификация и структура систем компьютерной алгебры.	11	2	2	7			д.з.	5
2.	Основные классы алгебраических систем.	11	2	2	7			д.з., к.р.	5
3.	Идеалы и факторкольца. Кольцо многочленов.	11	2	2	7				5
4.	Первоначальное представление о теории кодирования	12	2	2	8			д.з., к.р.	5
5.	Криптография с открытым ключом	11	2	2	7			д.з.	5
6.	Криптоанализ	12	2	2	8				5

7.	Аутентификация	12	2	2	8			д.з., к.р.	5
8.	Элементы компьютерной алгебры	15	3	4	8			д.з., к.р.	5
9.	Системы счисления. Правила ввода и вывода чисел.	15	4	3	8			д.з., к.р.	5
10.	Операции символьной математики.	15	3	4	8			д.з., к.р.	5
11.	Представление символьных данных в компьютере.	15	4	3	8			д.з.	5
12.	Алгоритмы символьных преобразований: числа, многочлены, выражения	16	4	4	8			к.р.	5
13.	Алгоритмы символьных преобразований: дифференцирование	12	2	2	8			д.з., к.р.	5
14.	Алгоритмы символьных преобразований:интегрирование.	12	2	2	8			к.р.	5
15.	Зачет							Зачет	30
	ИТОГО:	180	36	36	108				100

Виды учебных занятий указаны в сокращенном виде: Л — лекция, ПЗ — практическое занятие (семинар), СРС — самостоятельная работа, К.р. – контрольные работы, Дз – домашнее задание.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Студентам выдается Программа курса (примерный список вопросов к экзамену), список тем контрольных работ и домашних заданий. Критерии оценивания и способы повышения оценки. Список литературы.

7. Проведение промежуточной аттестации обучающихся по дисциплине

7.1. Общие условия

Промежуточная аттестация по дисциплине – зачет, проводится на основании результатов текущего контроля и результата, полученного на зачете. Зачет проводится в форме устного опроса.

Дисциплина оценивается по 100-балльной системе. Максимальное количество баллов, которое студент может набрать за один семестр – 30. Максимальное количество баллов, которое студент может набрать за ответ на экзамене – 70.

7.2. Критерии и шкалы оценивания результатов обучения по дисциплине

Код компетенции	Показатели достижения результатов обучения	Критерии и шкала оценивания			Перечень оценочных средств
		удовлетворительно	хорошо	Отлично	
ОПК-1	В результате освоения дисциплины обучающийся должен **ЗНАТЬ:** • важнейшие свойства алгебраических систем. **УМЕТЬ:** • использовать аналитический аппарат компьютерной алгебры • доказывать основные свойства фактор-групп (фактор-колец) • доказывать основные свойства колец (полей) вычетов **ВЛАДЕТЬ:** навыками исследования свойств основных объектов компьютерной алгебры.	Удовлетворительное владение основными понятиями Умение применять знания в стандартной ситуации	хорошее владение основными понятиями Умение применять знания в сложной стандартной ситуации	свободное владение основными понятиями Умение применять знания в сложной нестандартной ситуации	Зачет
ПК-1	В результате освоения дисциплины обучающийся должен **ЗНАТЬ:** • основные понятия абстрактной и компьютерной алгебры, • основные классы алгебраических систем и их примеры. **УМЕТЬ:** • формулировать типичные прикладные задачи на языке компьютерной алгебры; • применять методы компьютерной алгебры к решению вычислительных задач. **ВЛАДЕТЬ:** навыками исследования свойств основных объектов компьютерной алгебры.	Удовлетворительное владение основными понятиями Умение применять знания в стандартной ситуации	хорошее владение основными понятиями Умение применять знания в сложной стандартной ситуации	свободное владение основными понятиями Умение применять знания в сложной нестандартной ситуации	Зачет

7.3. Оценочные средства для промежуточной аттестации

Промежуточная аттестация (в конце семестра) – зачет.

Итоговая оценка за дисциплину выставляется по результатам текущего контроля и результатам сдачи зачета. Зачет проходит в форме устного.

Примерный перечень вопросов к зачету:

1. Классификация и структура систем компьютерной алгебры. Аппаратные требования.
2. Системы компьютерной математики для численных расчетов.
3. Универсальные системы компьютерной математики.
4. Задачи, решаемые системами компьютерной алгебры.

5. Полугруппы, моноиды, группы, коммутативные группы, кольца, поля, булевы алгебры.
6. Алгебры, алгебраические системы.
7. Теория делимости в кольце целых чисел. Кольца класса вычетов.
8. Поле комплексных чисел.
9. Подгруппы. Смежные классы по подгруппе, факторгруппы.
10. Подкольца. Идеалы кольца, факторкольца.
11. Кольцо многочленов от одной переменной, теорема делимости.
12. Многочлены от нескольких переменных.
13. Криптография с секретным ключом: шифры Цезаря, Виженера, Кардано, скиталы.
14. Криптография с открытым ключом: односторонняя функция, алгоритм RSA, подбор параметров: генерация псевдопростых чисел.
15. Криптоанализ, пассивные атаки: факторизация модуля, проблема инвариантных блоков, атака "малых показателей".
16. Активная атака, хеширование, атака "парадокса дней рождения".
17. Аутентификация, цифровая подпись.
18. Шифрование по алгоритму ЭльГамаля.
19. Элементы компьютерной алгебры.
20. Типы данных математических систем.
21. Системы счисления.
22. Правила ввода и вывода чисел.
23. Операции символьной математики.
24. Установка форматов вывода результатов символьных исчислений.
25. Представление символьных данных в компьютере.
26. Алгоритмы символьных преобразований (числа).
27. Алгоритмы символьных преобразований (многочлены).
28. Алгоритмы символьных преобразований (выражения).
29. Алгоритмы символьных преобразований (дифференцирование).
30. Алгоритмы символьных преобразований (интегрирование).

7.4. Шкала перевода оценок

Критерий выставления результирующей оценки по форме промежуточной аттестации.

Оценивание происходит на основании результатов текущего контроля и результатов, полученных на зачете в конце семестра.

Форма промежуточной аттестации	Шкала оценивания		Критерии оценивания
	в оценках или баллах по5-ти балльной шкале	в баллах по 100-балльной шкале	
Зачет	зачтено	Не менее 61	набрано не менее 61% максимального количества баллов в сумме за ответ на зачете и текущий контроль
Зачет	не зачтено	менее 61	набрано менее 61% максимального количества баллов в сумме за ответ на зачете и текущий контроль

8. Перечень образовательных технологий

В процессе преподавания дисциплины используются следующие образовательные технологии:

1. Лекции с обсуждением проблемных мест,
2. Практические занятия с решением задач,
3. Разбор домашних заданий с элементами дискуссии и взаимопомощи обучающихся друг другу,
4. Устные опросы.

9. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) Основная литература

1. Акритас А. Основы компьютерной алгебры с приложениями. М.: Мир, 1994. 543 с.
2. Компьютерная алгебра: Символьные и алгебраические вычисления / Под ред. Бухбергер Б., Коллинз Дж., Лоос Р. М.: Мир, 1986. 392 с.
3. Дэвенпорт Дж., Сирэ И., Турнье Э. Компьютерная алгебра. М.: Мир, 1991. 350 с.
4. Калинина Е.А., Утешев А.Ю. Теория исключения. СПб.: НИИ Химии СПбГУ, 2002. 72 с.
5. Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. М.: Мир, 2000. 687 с.
6. Ноден П., Китте К. Алгебраическая алгоритмика. М.: Мир, 1999, 719 с.
7. Саломаа А. Криптография с открытым ключом. М.: Мир, 1996. 318 с.
8. Утешев А.Ю., Черкасов Т.М., Шапошников А.А. Цифры и шифры. СПб.: Изд-во СПбГУ, 2001.
9. Введение в криптографию / Под ред. В.В.Ященко. М.: МЦНМО-ЧеРо, 1998. 271 с.

б) Дополнительная литература

1. Бухбергер Б., Коллинз Дж., Лаос Р. Компьютерная алгебра: Символьные и алгебраические вычисления. М.:Мир, 1986.
2. Кнут Д. Искусство программирования для ЭВМ. М.: Мир, т.1 - 1976, т.2 - 1977, т.3 - 1978.
3. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.: Мир, 1979.
4. Ван-дер-Варден Б.Л. Алгебра. М.: Наука, 1976.

10. Перечень ресурсов информационно-телекомуникационной сети «Интернет», профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

Не требуется.

11. Методические указания для обучающихся по освоению дисциплины

Студентам выдается Программа курса (примерный список вопросов к экзамену), список тем контрольных работ, Устных опросов и домашних заданий. Критерии оценивания и способы повышения оценки. Список литературы.

12. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Не требуется.

13. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Персональные компьютеры на каждого студента.

Разработчик программы:

профессор, к.т.н. Соловьев В.П.

Рецензент:

зав.кафедрой математики, профессор В.И.Богачев

Программа одобрена на заседании кафедры Информатики от «28» мая 2021 года, протокол № 05-21