

Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«Самарский государственный технический университет»

Инженерно-экономический факультет
Кафедра Прикладная математика и информатика

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

текущего контроля и промежуточной аттестации

дисциплины «Интегрированные системы в символьной математике»

в составе основной образовательной программы по направлению подготовки (специальности): 01.04.02 (010400.68) Прикладная математика и информатика

по уровню высшего образования: магистратура

направленность (профиль) программы: Прикладная математика и информатика

Самара 2014г.

Паспорт фонда оценочных средств

по дисциплине «Интегрированные системы в символьной математике»

№ п/п	Контролируемые разделы (темы) дисциплины (модуля)*	Код контролируемой компетенции***	Наименование оценочного средства**
1	Введение	<p>ОК-4 Способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять свое научное мировоззрение.</p> <p>ПК-3 Способность углубленного анализа проблем, постановки и обоснования задач научной и проектно-технологической деятельности.</p> <p>Знаний:</p> <ul style="list-style-type: none"> - особенностей символьных вычислений как методологии точного решения вычислительных задач; - критериев качества математических исследований, принципы экспериментальной и эмпирической проверки научных теорий; - тенденций и перспектив развития инструментальных средств компьютерной алгебры и символьных вычислений; - основополагающих фактов элементарной теории чисел, лежащие в основе построения всей математики; современные приложения теории чисел в области защиты информации. <p>Умений:</p> <ul style="list-style-type: none"> - реализовывать основные методы математических рассуждений в символьной записи; - пользоваться построением математических моделей для решения практических проблем; - применять интегрированные системы вычислений в математическом модели- 	<p>Вопросы к экзамену; Собеседование: Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.</p>

		<p>ровании;</p> <ul style="list-style-type: none"> - применять полученные знания при решении конкретных задач математического моделирования <p>Навыков:</p> <ul style="list-style-type: none"> - культуры математического мышления; логической и алгоритмической культурой; - математики как универсальным языком науки, средством моделирования явлений и процессов; - работы с пакетами символьной математики Maxima, Derive и численных вычислений Octave; - разработки основных алгоритмов на основе символьных вычислений. 	
2	Среда Maxima	<p>ОК-4 Способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять свое научное мировоззрение.</p> <p>ПК-3 Способность углубленного анализа проблем, постановки и обоснования задач научной и проектно-технологической деятельности.</p> <p>Знаний:</p> <ul style="list-style-type: none"> - особенностей символьных вычислений как методологии точного решения вычислительных задач; - критериев качества математических исследований, принципы экспериментальной и эмпирической проверки научных теорий; - тенденций и перспектив развития инструментальных средств компьютерной алгебры и символьных вычислений; - основополагающих фактов элементарной теории чисел, лежащие в основе построения всей математики; современные приложения теории чисел в области защиты информации. <p>Умений:</p> <ul style="list-style-type: none"> - реализовывать основные методы математических рассуждений в символьной записи; - пользоваться построением математических моделей для решения практических проблем; 	<p>Вопросы к экзамену;</p> <p>Собеседование:</p> <p>Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.</p>

		<ul style="list-style-type: none"> - применять интегрированные системы вычислений в математическом моделировании; - применять полученные знания при решении конкретных задач математического моделирования <p>Навыков:</p> <ul style="list-style-type: none"> -культуры математического мышления; логической и алгоритмической культурой; - математики как универсальным языком науки, средством моделирования явлений и процессов; - работы с пакетами символьной математики Maxima, Derive и численных вычислений Octave; -разработки основных алгоритмов на основе символьных вычислений. 	
3	Среда Derive	<p>ОК-4 Способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять свое научное мировоззрение.</p> <p>ПК-3 Способность углубленного анализа проблем, постановки и обоснования задач научной и проектно-технологической деятельности.</p> <p>Знаний:</p> <ul style="list-style-type: none"> - особенностей символьных вычислений как методологии точного решения вычислительных задач; - критериев качества математических исследований, принципы экспериментальной и эмпирической проверки научных теорий; - тенденций и перспектив развития инструментальных средств компьютерной алгебры и символьных вычислений; - основополагающих фактов элементарной теории чисел, лежащие в основе построения всей математики; современные приложения теории чисел в области защиты информации. <p>Умений:</p> <ul style="list-style-type: none"> - реализовывать основные методы математических рассуждений в символьной записи; - пользоваться построением математиче- 	<p>Вопросы к экзамену;</p> <p>Собеседование:</p> <p>Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.</p>

		<p>ских моделей для решения практических проблем;</p> <ul style="list-style-type: none"> - применять интегрированные системы вычислений в математическом моделировании; - применять полученные знания при решении конкретных задач математического моделирования <p>Навыков:</p> <ul style="list-style-type: none"> - культуры математического мышления; логической и алгоритмической культурой; - математики как универсальным языком науки, средством моделирования явлений и процессов; - работы с пакетами символьной математики Maxima, Derive и численных вычислений Octave; - разработки основных алгоритмов на основе символьных вычислений. 	
4	<p>«Альтернативные» пакеты Maple и Mathematica, MathCad</p>	<p>ОК-4 Способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять свое научное мировоззрение.</p> <p>ПК-3 Способность углубленного анализа проблем, постановки и обоснования задач научной и проектно-технологической деятельности.</p> <p>Знаний:</p> <ul style="list-style-type: none"> - особенностей символьных вычислений как методологии точного решения вычислительных задач; - критериев качества математических исследований, принципы экспериментальной и эмпирической проверки научных теорий; - тенденций и перспектив развития инструментальных средств компьютерной алгебры и символьных вычислений; - основополагающих фактов элементарной теории чисел, лежащие в основе построения всей математики; современные приложения теории чисел в области защиты информации. <p>Умений:</p> <ul style="list-style-type: none"> - реализовывать основные методы математических рассуждений в символьной 	<p>Вопросы к экзамену; Собеседование: Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.</p>

		<p>записи;</p> <ul style="list-style-type: none"> - пользоваться построением математических моделей для решения практических проблем; - применять интегрированные системы вычислений в математическом моделировании; - применять полученные знания при решении конкретных задач математического моделирования <p>Навыков:</p> <ul style="list-style-type: none"> - культуры математического мышления; логической и алгоритмической культуры; - математики как универсальным языком науки, средством моделирования явлений и процессов; - работы с пакетами символьной математики Maxima, Derive и численных вычислений Octave; - разработки основных алгоритмов на основе символьных вычислений. 	
5	<p>Интегрированные системы численных вычислений (SciLab, Octave, MatLab)</p>	<p>ОК-4 Способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять свое научное мировоззрение.</p> <p>ПК-3 Способность углубленного анализа проблем, постановки и обоснования задач научной и проектно-технологической деятельности.</p> <p>Знаний:</p> <ul style="list-style-type: none"> - особенностей символьных вычислений как методологии точного решения вычислительных задач; - критериев качества математических исследований, принципы экспериментальной и эмпирической проверки научных теорий; - тенденций и перспектив развития инструментальных средств компьютерной алгебры и символьных вычислений; - основополагающих фактов элементарной теории чисел, лежащие в основе построения всей математики; современные приложения теории чисел в области защиты информации. <p>Умений:</p>	<p>Вопросы к экзамену; Собеседование: Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.</p>

		<ul style="list-style-type: none">- реализовывать основные методы математических рассуждений в символьной записи;- пользоваться построением математических моделей для решения практических проблем;- применять интегрированные системы вычислений в математическом моделировании;- применять полученные знания при решении конкретных задач математического моделирования <p>Навыков:</p> <ul style="list-style-type: none">-культуры математического мышления; логической и алгоритмической культурой;- математики как универсальным языком науки, средством моделирования явлений и процессов;- работы с пакетами символьной математики Maxima, Derive и численных вычислений Octave;-разработки основных алгоритмов на основе символьных вычислений.	
--	--	---	--

Перечень вопросов для промежуточной аттестации (экзамен)

1. Операция деления, деление с остатком.
2. Наибольший общий делитель, его свойства.
3. Алгоритм Евклида.
4. Теорема Ламе.
5. Двоичный алгоритм Евклида.
6. Простые числа.
7. Основная теорема арифметики.
8. Вычеты по модулю целых чисел.
9. Теорема о числе решений сравнения первой степени.
10. Лемма Безу.
11. Расширенный алгоритм Евклида.
12. Китайская теорема об остатках.
13. Алгоритм Гарнера.
14. Функция Эйлера.
15. Теоремы Эйлера и Ферма.
16. Первообразные корни.
17. Теорема о существовании первообразного корня по модулю простого числа.
18. Определение элементарных операций над многочленами.
19. Алгоритмы умножения многочленов.
20. Операция деления с остатком для многочленов.
21. Алгоритм Евклида для многочленов.
22. Лемма Безу для многочленов.
23. Основная теорема арифметики для многочленов.
24. Теорема о числе корней многочленов.
25. Теоремы о подъеме решений.
26. Определение квадратичного вычета.
27. Символ Лежандра.
28. Теорема о числе решений.
29. Свойства символа Лежандра.
30. Определение символа Якоби, его свойства.
31. Алгоритм вычисления символа Якоби.
32. Вычисление квадратного корня: частные случаи.
33. Алгоритм Тонелли-Шенкса.
34. Общее квадратное уравнение.
35. Вероятностный алгоритм вычисления корней многочлена.
36. Построение таблицы простых чисел.
37. Вероятностные алгоритмы проверки на простоту.
38. Тест Соловея–Штрассена.
39. Тест Миллера–Рабина.
40. Теорема Поклингтона и ее дополнения.
41. Алгоритмы построения простых чисел.
42. Рекуррентные последовательности Люка.
43. Теорема Моррисона.
44. Рекурсивный алгоритм построения простого числа с известным разложением $p-1$.
45. Алгоритм построения сильно простого числа.
46. Определение непрерывной дроби.
47. Понятие подходящей дроби.
48. Теорема о наилучшем приближении.
49. Квадратичные иррациональности и их свойства.
50. Подходящие дроби и наилучшие приближения.

51. Метод пробного деления (факторизации).
52. Метод факторизации Ферма.
53. Метод факторизации Лемана.
54. Метод факторизации Полларда.
55. Метод факторизации Брента.
56. $p-1$ метод факторизации Полларда.
57. $p+1$ метод факторизации Вильямса.
58. Оптимизация методов факторизации Полларда и Вильямса.
59. Метод факторизации Женга.
60. Метод факторизации Макки.
61. Основная лемма факторизации.
62. Решето (метод факторизации) Крайчика.
63. Метод непрерывных дробей (факторизация).
64. Метод факторизации Моррисона–Брилхарда.
65. Линейное решето Шреппеля (факторизация).
66. Квадратичное решето (факторизация).
67. Основные понятия криптографии.
 1. Шифры потока и блочные шифры.
 2. Полноразмерные ключевые шифры.
 3. Шифры ключа частичного размера.
 4. Шифры без ключа. Шифры Файстеля. Шифры не-Файстеля.
 5. Атаки на блочные шифры.
 6. Синхронные шифры потока.
 7. Общие положения шифра DES.
 8. Структура и алгоритмы DES.
 9. Анализ шифра DES.
 10. Многократное применение шифра DES.
 11. Безопасность шифра DES.
 12. Общие положения шифра AES.
 13. Преобразования в шифре AES.
 14. Расширение шифра AES (AES-128, AES-192 и AES-256).
 15. Алгоритмы шифра и обратного шифра AES.
 16. Анализ шифра AES.
 17. Применение современных блочных шифров.
 18. Использование шифров потока.
 19. Проблемы управлением и генерацией ключей.
 20. Основные идеи и положения асимметрично-ключевой криптографии.
 21. Криптографическая система RSA.
 22. Атаки на RSA.

Контролируемые компетенции:

ОК-4 Способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять свое научное мировоззрение.

ПК-3 Способность углубленного анализа проблем, постановки и обоснования задач научной и проектно-технологической деятельности.

Разработчик Саушкин М.Н. _____ Ф. И. О.

(подпись)

«__» _____ 20__ г.

Протокол экспертизы соответствия уровня достижения студентом _____ (Ф.И.О.) _____ запланированных результатов обучения по дисциплине Интегрированные системы в символьной математике

Перечень компетенций по дисциплине	Структурные элементы заданий по дисциплине												
	Выполнение домашнего задания	Реферат	Расчетно-графические работы	Типовые расчеты	Подготовка и выступление с докладом	Написание эссе	Формирование отчета по лабораторным работам	Курсовой проект/работа	Вопросы 1	Вопрос 2	Вопрос 3	Вопрос 4
	Виды СРС, предусмотренные рабочей программой дисциплины*							Вопросы к экзамену					
ОК-4 Способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять свое научное мировоззрение.													
ПК-3 Способность углубленного анализа проблем, постановки и обоснования задач научной и проектно-технологической деятельности.													
				<i>Оценки по пятибалльной шкале выставляются в ячейках, соответствующих компетенциям (по строке), подлежащим оцениванию по результатам конкретного элемента задания по дисциплине (по столбцам) в соответствии с запланированными в рабочей программе видами СРС и ответами на экзаменационные вопросы.</i>									
				<i>Остальные ячейки заполняются символом X.</i>									
				<i>Критерии выставления оценки устанавливаются настоящим фондом оценочных средств ОПОП.</i>									

*перечень прилагается

Шкала оценивания:

Виды СРС оцениваются по своевременности и качеству выполнения (до 50 баллов). Ответы на вопросы при сдаче зачета (до 50 баллов) Оценка студента за промежуточную аттестацию по учебной дисциплине, проставляемая в ведомость и зачетную книжку, определяется по сумме баллов, набранной по приведенным оцениваемым элементам. Формирование оценки: от 80-100 баллов – «отлично»; от 65-80 баллов – «хорошо»; от 50-65 баллов – «удовлетворительно».

Экзамен проходит в форме собеседования по билету. Каждый билет включает два теоретических вопроса и два практикоориентированных задания. При выставлении оценок учитывается уровень приобретенных компетенций студента. Компонент «знать» оценивается теоретическими вопросами по содержанию дисциплины, компоненты «уметь» и «владеть» - практикоориентированными заданиями. Аудиторное время, отведенное студенту, на подготовку — 30 минут.

Экзамен проходит в форме собеседования по билету. Каждый билет включает два вопроса из списка вопросов к экзамену, и вопрос по реферату. При выставлении оценки учитывается уровень приобретенных компетенций студента, оценивается сданный реферат и ответы на вопросы по билету и работа на практических занятиях.

Преподаватель Саушкин М.Н. _____ «__» _____ 20__ г

Уровень освоения дисциплины «Интегрированные системы в символической математике» магистрантами определяется следующими оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

- оценки «отлично» заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка «отлично» выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой специальности.
- оценки «хорошо» заслуживает студент, обнаруживший полное знание учебно-программного материала, успешно выполняющий предусмотренные программой задания, усвоивший основную литературу. Как правило, оценка «хорошо» выставляется студентам, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшего обучения в вузе и в будущей профессиональной деятельности.
- оценки «удовлетворительно» заслуживает студент, обнаруживший знание основного учебно-программного материала в объеме, необходимом для дальнейшего обучения, выполняющего задания, предусмотренные программой, знакомый с основной литературой, рекомендованной программой. Как правило, оценка «удовлетворительно» выставляется студентам, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя.
- оценка «неудовлетворительно» выставляется студенту, имеющему пробелы в знаниях основного учебно-программного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий. Как правило, оценка «неудовлетворительно» выставляется студентам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных знаний по дисциплине.