

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет» (ФГБОУ ВО «КубГУ»)

Факультет компьютерных технологий и прикладной математики
Кафедра вычислительных технологий

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор

Иванов А.Г.



2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.02.02 «ПРИКЛАДНАЯ АЛГЕБРА»

Направление подготовки 02.03.02 Фундаментальная информатика и информационные технологии

(код и наименование направления подготовки/специальности)

Направленность (профиль) "Вычислительные технологии"

(наименование направленности (профиля) специализации)

Программа подготовки академическая

(академическая /прикладная)

Форма обучения очная

(очная, очно-заочная, заочная)

Квалификация (степень) выпускника бакалавр

(бакалавр, магистр, специалист)

Краснодар 2015

Рабочая программа Б1.В.ДВ.02.02 «ПРИКЛАДНАЯ АЛГЕБРА» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.02 «Фундаментальная информатика и информационные технологии» Программу составил(и):

А.И.Миков, заведующий кафедрой вычислительных технологий, д.ф.-м.н., профессор



подпись

Рабочая программа дисциплины Б1.В.ДВ.02.02 «ПРИКЛАДНАЯ АЛГЕБРА» утверждена на заседании кафедры вычислительных технологий

протокол № 9 «20» апреля 2015 г.

Заведующий кафедрой (разработчика) Миков А.И.

фамилия, инициалы



подпись

Рабочая программа обсуждена на заседании кафедры вычислительных технологий протокол № 9 «20» апреля 2015 г.



Заведующий кафедрой (выпускающей) Миков А.И.

фамилия, инициалы

подпись

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики протокол № 5 « 29» апреля 2015 г.

Председатель УМК факультета



К.В. Малыхин

Рецензенты:

Гаркуша О.В., доцент кафедры информационных технологий ФБГОУ ВО «Кубанский государственный университет», кандидат физико-математических наук.

Зайков В.П. Ректор НЧОУ ВО «Кубанский институт информзащиты» д.экон. наук, к.т.н., доцент.

1. Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

Целями освоения дисциплины «Прикладная алгебра» являются формирование у студентов высокой алгебраической культуры, готовых и умеющих применять полученные знания в обучении, в научных исследованиях и при решении прикладных задач, активно участвующих в процессе образования и науки, так же дисциплина способствует формированию и развитию личности студентов, способностей к алгоритмическому и логическому мышлению. Фундаментальная подготовка студентов в области математических дисциплин, овладение современным математическим аппаратом для дальнейшего использования в других областях и дисциплинах естественнонаучного цикла. При освоении дисциплины «Прикладная алгебра» вырабатывается: умение логически мыслить, проводить доказательство основных утверждений, устанавливать логические связи между понятиями.

Целью освоения прикладных разделов дисциплины является освоение студентами методов решения практически ориентированных задач в различных отраслях жизнедеятельности с использованием: кольца и поля, линейных кодов, циклических кодов, алгебраической полиграфии, элементов теории групп, блок-схем, систем Штейнера и так называемых латинских квадратов.

1.2 Задачи дисциплины

Задачи изучения дисциплины. Задачами изучения дисциплины «Прикладная алгебра» является реализация требований, установленных федеральными государственными образовательными стандартами высшего профессионального образования к уровню подготовки бакалавров по направлению «Фундаментальные информатика и информационные технологии (информатика и компьютерные науки)». Следует различать следующие задачи изучения дисциплины:

1. Дать студентам основы знаний по прикладной алгебре;
2. Научить применять алгебру в прикладных областях;
3. Показать связь прикладной алгебры с информатикой;
4. Подготовить будущих преподавателей к использованию полученных знаний в процессе образования.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Прикладная алгебра» относится к дисциплинам по выбору базовой части ООП. Для изучения дисциплины необходимо знание курсов дискретной математики, основ программирования, курса распределенных задач и алгоритмов. Знания, получаемые при изучении курса, используются при изучении программистских дисциплин профессионального цикла учебного плана бакалавра.

Место курса в профессиональной подготовке бакалавра определяется ролью алгебры в формировании высококвалифицированного специалиста по направлению «Фундаментальные информатика и информационные технологии (вычислительные технологии)».

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Компетенции обучающегося, формируемые в результате освоения дисциплины «Фундаментальная информатика и информационные технологии (информатика и компьютерные науки)»:

ПК-6: Способность эффективно применять базовые математические знания и информационные технологии при решении проектно-технических и прикладных задач, связанных с развитием и использованием информационных технологий.

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1	ПК-6	Способностью эффективно применять базовые математические знания и информационные технологии при решении проектно-технических и прикладных задач, связанных с развитием и использованием информационных технологий;	методы основные понятия, определения и свойства объектов прикладной алгебры, формулировки и доказательства утверждений, методы их доказательства, возможные сферы их связи и приложения в других областях математического знания и дисциплинах естественнонаучного цикла;	доказывать утверждения математики, решать задачи математики, применять полученные навыки в других областях и дисциплинах естественнонаучного цикла;	аппаратом математики, методами доказательства утверждений, навыками применения этого в других областях и дисциплинах естественнонаучного цикла.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 3 зач.ед. (108 часов), их распределение по видам работ представлено в таблице:

Вид учебной работы	Всего часов	Семестры (часы)	
		6	
Контактная работа в том числе:			
Аудиторные занятия (всего):	68	68	
В том числе:			
Занятия лекционного типа	34	34	
Занятия семинарского типа (семинары, практ. занятия)			
Лабораторные занятия	34	34	
Иная контрольная работа			

Контроль самостоятельной работы	4	4	
Промежуточная аттестация (ИКР)	0,2	0,2	
Самостоятельная работа, в том числе			
В том числе:			
Курсовая работа			
<i>Проработка учебного (теоретического) материала</i>	20	20	
<i>Выполнение индивидуальных заданий (РГЗ)</i>	10	10	
<i>Подготовка к текущему контролю</i>	5,8	5,8	
Контроль:			
Подготовка к экзамену:			
Общая трудоемкость	час	108	108
	в т.ч. контактная работа	72,2	72,2
	зач. ед.	3	3

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в 6 семестре (очная форма)

№ раздела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	КСР	ЛР	
1	2	3	4	5	6	7
1	Кольца и поля	18	6		6	6
2	Линейные коды	26	8	2	8	8
3	Циклические коды	18	6	2	6	4
4	Алгебраическая полиграфия	20	6		6	8
5	Элементы теории групп	12	4		4	4
6	Блок-схемы	13,8	4		4	5,8
	Итого по разделам	107,8	34	4	34	35,8
	ИКР	0,2				
	Итого:	108				

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Кольца и поля	Кольца, идеалы, гомоморфизмы, фактор-кольца, многочлены, поля, поля разложения, конечные поля, теорема о цикличности	ЛР
		группы ненулевых элементов конечного поля, неприводимые многочлены над конечными полями, автоморфизмы конечных полей, алгоритм Берлекэмп разложения многочлена на неприводимые многочлены.	
2.	Линейные коды	Определение, примеры, расстояние Хэмминга, связь минимального расстояния с числом исправляемых ошибок, граница Хэмминга кода, исправляющего t ошибок, граница Гилберта-Варшамова, декодирование вектора по лидеру смежного класса, бинарный код Хэмминга, дуальный линейный код.	ЛР, РГЗ
3.	Циклические коды	Определение, характеристика, примеры (код Хэмминга), БЧХ – код, код Рида-Соломона, алгоритмы кодирования и декодирования БЧХ-кода.	ЛР, РГЗ
4.	Алгебраическая полиграфия	Криптосистемы с единым ключом (шифры Цезаря, Виженера, Хилла), криптосистемы с публичными ключами (РША – криптосистема, метод рюкзака-ловушки), линейные рекуррентные последовательности (их свойства) и их связь с криптосистемами с бегущим ключом.	ЛР, РГЗ
5.	Элементы теории групп	Теорема Кэли, строение группы подстановок, стабилизаторы и орбиты элементов, теорема Бернсайда, цикловой индекс подстановки, многочлены цикловых индексов, теорема Пойа, примеры.	ЛР, РГЗ
6.	Блок-схемы	Блок-схемы, системы Штейнера, латинские квадраты.	ЛР

2.3.2 Лабораторные занятия

№ работы	№ раздела дисциплины	Наименование лабораторных работ	Форма текущего контроля
1	2	3	4
1	1	Основные алгебраические структуры: группы, кольца, поля	Решение задач
2	1	Конечные поля	Решение задач
3	1	Линейные коды, границы параметров	Решение задач
4	1	Коды Рида-Соломона и код Хемминга	Решение задач
5	2	Коды Рида-Маллера	Решение задач

6	2	Алгоритм Берлекампа Криптосистемы с открытым ключом	Решение задач
7	2	Группа точек эллиптической кривой	Решение задач
8	2	Алгоритм Гольдвассера-Килиана проверки числа на простоту	Решение задач
9	3	Алгоритм Ленстры разложения чисел на множители	Решение задач

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Раздел 1. Кольца и поля.	Основная литература [1] Дополнительная литература [1]
2	Линейные коды	Основная литература [2] Дополнительная литература [2]
3	Циклические коды	Основная литература [3] Дополнительная литература [1-2]
4	Алгебраическая полиграфия	Основная литература [1] Дополнительная литература [1-3]
5	Элементы теории групп	Основная литература [2] Дополнительная литература [2]
6	Блок-схемы	Основная литература [3-4] Дополнительная литература [2-3]

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

При изучении данного курса используются традиционные лекции и практические занятия.

Цель практических занятий – научить студента применять полученные на лекциях теоретические знания к решению и исследованию конкретных задач.

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
3	Л	Компьютерные презентации и обсуждение	34
	ЛР	Разбор конкретных ситуаций (задач),	34
		тренинги по решению задач, компьютерные симуляции (программирование алгоритмов)	
Итого:			68

4. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1 Фонд оценочных средств для проведения текущего контроля

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий, лабораторных работ и итоговой аттестации (зачет в 6 семестре).

Оценка успеваемости осуществляется по результатам:

- выполнения лабораторных работ;
- ответа на зачете (для выявления знания и понимания теоретического материала дисциплины).

Учебная деятельность проходит в соответствии с графиком учебного процесса. Процесс самостоятельной работы контролируется во время аудиторных занятий, индивидуальных консультаций.

Оценочными средствами дисциплины являются средства текущего контроля (устный опрос, выполнение индивидуальных заданий и итоговая аттестация (экзамен)).

Перечень вопросов, выносимых на зачет

1. Кольца, идеалы, определение, примеры;
2. Гомоморфизмы, фактор-кольца;
3. Многочлены, поля, поля разложения, конечные поля;
4. Теорема о цикличности группы ненулевых элементов конечного поля;
5. Неприводимые многочлены над конечными полями;
6. Автоморфизмы конечных полей;
7. Алгоритм Берлекэмп разложения многочлена на неприводимые многочлены;
8. Линейные коды: определение, примеры;
9. Расстояние Хэмминга, связь минимального расстояния с числом исправляемых ошибок;
10. Граница кода Хэмминга, исправляющего t ошибок;
11. Граница Гилберта-Варшавова, декодирование вектора по лидеру смежного класса;
12. Бинарный код Хэмминга;
13. Дуальный линейный код;
14. Циклические коды: определение, характеристика, примеры (код Хэмминга); 15. БЧХ – код, код Рида-Соломона;
16. Алгоритмы кодирования и декодирования БЧХ-кода;
17. Алгебраическая полиграфия, криптосистемы с единым ключом (шифры Цезаря,

Виженера, Хилла);

18. Криптосистемы с публичными ключами (РША – криптосистема, метод рюкзака-ловушки);
19. Линейные рекуррентные последовательности (их свойства) и их связь с криптосистемами с бегущим ключом;
20. Элементы теории групп, теорема Кэли;
21. Строение группы подстановок;
22. Стабилизаторы и орбиты элементов;
23. Теорема Бернсайда;
24. Цикловой индекс подстановки, многочлены цикловых индексов; 25. Теорема Пойа, примеры;
26. Блок-схемы, системы Штейнера;
27. Блок-схемы и связь с латинскими квадратами.

Критерии оценивания:

"Зачет" - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

- наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности.

Практические задания выполнены на 60-100%.

"Не зачет"- баллов (оценка неудовлетворительно) - ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы». **Выполнено менее 60% практических заданий.**

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

- в форме электронного документа. Для лиц с нарушениями слуха:
- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

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

5.1 Основная литература:

- 1.** Огнева Э. Н., Математика: Раздел 1. **Алгебра** и геометрия : учебное пособие / Огнева Э. Н. ; Министерство культуры Российской Федерации, ФГБОУ ВПО «Кемеровский государственный университет культуры и искусств», Кафедра технологии автоматизированной обработки информации. - Кемерово : КемГУКИ, 2011. - 227 с. : табл., схем. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=227759>
- 2.** Математические методы и модели исследования операций : учебник / ред. В.А. Колемаева. - Москва : Юнити-Дана, 2015. - 592 с. : ил., табл., граф. - Библиогр. в кн. - ISBN 978-5-238-01325-1 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=114719>
- 3.** Зайцева, О.Н. Математические методы в приложениях. Дискретная математика : учебное пособие / О.Н. Зайцева, А.Н. Нуриев, П.В. Малов ; Министерство образования и науки России, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Казанский национальный исследовательский технологический университет». - Казань : Издательство КНИТУ, 2014. - 173 с. : табл., ил. - Библиогр. в кн. - ISBN 978-5-7882-1570-9 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=428299>

5.2. Дополнительная литература:

- 1.** Зализняк, В.Е. Теория и практика по вычислительной математике : учебное пособие / В.Е. Зализняк, Г.И. Щепановская ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2012. - 174 с. : табл. - ISBN 978-5-7638-2498-8 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=229271>
- 2.** Мицель, А.А. Вычислительные методы : учебное пособие / А.А. Мицель ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Эль Контент, 2013. - 197 с. : ил. - Библиогр.: с.183-184. - ISBN 978-5-4332-0121-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=480612>

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах

1. ЭБС Издательства «Лань» <http://e.lanbook.com> ,
2. ЭБС «Университетская библиотека онлайн» www.biblioclub.ru ,
3. ЭБС «Юрайт» <http://www.biblio-online.ru> ,
4. ЭБС «ZnaniUM.COM» www.znanium.com,
5. ЭБС «BOOK.ru» <https://www.book.ru>.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

6.1 Перечень необходимого программного обеспечения.

1. Matlab.

7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оборудованная видеопроектором и экраном, ауд. 129, 131.
2.	Лабораторные занятия	Компьютерные классы, лаб. 101 - 104. Классы оснащены компьютерами, объединенными в локальную сеть. Аудитории для лабораторных занятий, оборудованные досками.
3.	Текущий контроль, промежуточная аттестация	Лекционная аудитория.
4.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.