

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук

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

_____ Т.А. Хагуров
подпись
«31» мая 2024г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.10 АЛГЕБРАИЧЕСКАЯ АЛГОРИТМИКА

Направление подготовки 01.04.01 Математика

Направленность (профиль) Алгебраические методы защиты информации

Форма обучения очная

Квалификация магистр

Краснодар 2024

Рабочая программа дисциплины Алгебраическая алгоритмика
составлена в соответствии с федеральным государственным
образовательным стандартом высшего образования (ФГОС ВО) по
направлению подготовки

01.04.01 Математика Алгебраические методы защиты информации

код и наименование направления подготовки

Программу составил(и):

А.В. Рожков, профессор, д.ф.-м.н., профессор

И.О. Фамилия, должность, ученая степень, ученое звание



Рабочая программа дисциплины Алгебраическая алгоритмика
утверждена на заседании кафедры функционального анализа и алгебры
протокол № 12 «07» мая 2024 г.

Заведующий кафедрой функционального анализа и алгебры

Барсукова В.Ю.

фамилия, инициалы



Утверждена на заседании учебно-методической комиссии факультета
математики и компьютерных наук
протокол № 3 «14» мая 2024 г.

Председатель УМК факультета Шмалько С.П.

фамилия, инициалы



подпись

Рецензенты:

Ганижева Л.Л. к.т.н., доцент кафедры наземного транспорта и механики
КубГТУ

Лазарев В.А. д.п.н., зав. кафедрой теории функций КубГУ

Рецензенты:

Ганижева Л.Л. к.т.н., доцент кафедры наземного транспорта и механики
КубГТУ

Лежнев А.В. к.ф.-м.н., зав. кафедрой математических и компьютерных
методов КубГУ

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Цель освоения дисциплины – рассматривает задачи информатизации и научного программирования. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

Получение базовых теоретических и практических сведений и навыков о структуре и алгоритмах символьных математических вычислений. Прежде всего, алгебраических, связанных с вычислительными и числовыми вопросами алгебры и криптографии.

1.2 Задачи дисциплины.

Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли вычислительных приемов и методов, при решении вопросов защиты информации. А также при анализе структур информационных систем и математических методов построения защищенных информационных систем.

Изучение теоретических основ предмета: Информационные объекты. Компьютерная алгебра и численный анализ. Элементы теории сложности алгоритмов. Числовые функции, основные теоремы о евклидовых кольцах, алгоритмы решения линейных и квадратных уравнений в конечных полях, кольцах вычетов, алгоритмы нахождения наибольших общих делителей, алгоритмов проверки простоты чисел.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «алгебраическая алгоритмика» относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана Б1.В.10.

Алгебраической алгоритмике предшествует алгебра и теория алгоритмов. Данная дисциплина, как алгоритмическая основа криптографии, криптоанализа, теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров. А также развитию навыков применения современных компьютерных средств для решения естественно-научных проблем.

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

| Код и наименование индикатора* достижения компетенции | Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности)) |
|--|--|
| ПК-1 Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики | |
| ПК-1.1 Знает основные понятия, идеи и методы фундаментальных математических дисциплин для решения базовых задач | Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа |
| ПК-1.2 Умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области | Уметь: Применять основные математические методы, используемые в анализе типовых алгоритмов |
| ПК-1.3 Самостоятельно и корректно решает стандартные задачи фундаментальной и прикладной математики | Владеть навыками: использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в |

| Код и наименование индикатора* достижения компетенции | Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности)) |
|---|---|
| ПК-1.4 Имеет навыки решения математических задач, соответствующих квалификации, возникающих при проведении научных и прикладных исследований | области символьных вычислений. |
| ПК-4 Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах | |
| ПК-4.1 Умеет применять и реализовывать математически сложные алгоритмы в современных программных комплексах ПК-4.2 Применяет в профессиональной деятельности методику исследования и создания новых моделей, методов и технологий в математике и естественных науках ПК-4.3 Демонстрирует умение отбора среди существующих методов наиболее подходящие для решения конкретной прикладной задачи | Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа. Элементы теории сложности алгоритмов. Уметь: Определять структуры данных в компьютерной алгебре. Использовать технику символьных вычислений. Применять основные математические методы, используемые в анализе типовых криптографических алгоритмов. Владеть навыками: классификации систем компьютерной алгебры; ориентироваться в типовых архитектурах вычислительных процессов; использования библиотеки алгоритмов и пакетов расширения; |

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 2 зач. ед. (72 часа), их распределение по видам работ представлено в таблице
(для магистров ОФО).

| Вид учебной работы | Всего часов | Семестры (часы) | | | |
|--|-------------|-----------------|---|---|---|
| | | 3 | | | |
| Контактная работа, в том числе: | | | | | |
| Аудиторные занятия (всего): | 16 | 16 | | | |
| Занятия лекционного типа | 8 | 8 | - | - | - |
| Лабораторные занятия | 8 | 8 | - | - | - |
| Занятия семинарского типа (семинары, практические занятия) | - | - | - | - | - |
| | - | - | - | - | - |
| Иная контактная работа: | | | | | |
| Контроль самостоятельной работы (КСР) | | | | | |

| | | | | | |
|---|--------------------------------------|-------------|-------------|----------|----------|
| Промежуточная аттестация (ИКР) | 0,2 | 0,2 | | | |
| Самостоятельная работа, в том числе: | 55,8 | 55,8 | | | |
| Курсовая работа | - | - | - | - | - |
| Проработка учебного (теоретического) материала | 10 | 10 | - | - | - |
| Выполнение индивидуальных заданий (подготовка сообщений, презентаций) | 10 | 10 | - | - | - |
| Реферат | 10 | 10 | - | - | - |
| | | | | | |
| Подготовка к текущему контролю | 21,8 | 21,8 | - | - | - |
| Контроль: | | | | | |
| Подготовка к зачету | - | - | | | |
| Общая трудоемкость | час. | 72 | 72 | - | - |
| | в том числе контактная работа | 20,2 | 20,2 | | |
| | зач. ед | 2 | 2 | | |

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в 3 семестре (очная форма)

| № | Наименование разделов | Количество часов | | | | |
|---|--|------------------|-------------------|----|----------|----------------------|
| | | Всего | Аудиторная работа | | | Внеаудиторная работа |
| | | | Л | ПЗ | ЛР | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Присваивание. Последовательность. Цикл. Альтернатива. Рекурсия. Быстрый алгоритм возведения в степень. Работа с матрицами. | 19,8 | 2 | | 2 | 15,8 |
| 2 | Арифметика целых чисел. Работа с большими числами. Наибольший общий делитель. Алгоритмы факторизации. | 18 | 2 | | 2 | 14 |
| 3 | Евклидовы кольца. Неприводимые многочлены. Конечные кольца. | 18 | 2 | | 2 | 14 |
| 4 | Китайская теорема об остатках. Вычисления в кольцах вычетов. Функция Эйлера. Дискретное преобразование Фурье. | 16 | 2 | | 2 | 12 |
| | Итого по дисциплине: | | 8 | | 8 | 55,8 |

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

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

| № | Наименование раздела | Содержание раздела | Форма текущего контроля |
|---|--|--|-------------------------|
| 1 | 2 | 3 | 4 |
| 1 | Присваивание. Последовательность. Цикл. Альтернатива | Структура данных для представления объектов вычислений в целочисленной. Язык реализации – C++. Полиномиальная арифметика | Р |
| 2 | Арифметика целых | Расширение состава встроенных и | Э |

| | | | |
|---|---|---|---|
| | чисел. Работа с большими числами | программируемых типов математических объектов. Интеграция СКА с другими компьютерными системами. Унификация и объектная ориентация интерфейса пользователя. | |
| 3 | Наибольший общий делитель. Алгоритмы факторизации | Алгоритм проверки на простоту. Алгоритм тестирования. Тест Эдуарда Люка (1878) – Дерика Генри Лемера (1930). Тест Адлемана-Померанца-Рюмли. | Т |
| 4 | Китайская теорема об остатках. Вычисления в кольцах вычетов | Тесты псевдопростоты. Числа Кармайкла. Разложение чисел на простые числа. Метод Адриена Мари Лежандра. Метод Ферма. Метод цепных дробей. | Р |
| 5 | Дискретное преобразование Фурье. | Алгоритмы вычисления НОД в кольцах полиномов. Бинарный алгоритм вычисления НОД. Расширенный алгоритм Евклида. Расширенный алгоритм Евклида для полиномов над полем. | Т |

2.3.2 Занятия лабораторного типа.

Не предусмотрены

2.3.3 Практические занятия.

| № | Наименование лабораторных работ | Форма текущего контроля |
|---|--|------------------------------|
| 1 | 3 | 4 |
| 1 | Пакеты компьютерной алгебры на открытом коде. | ЛР |
| 2 | Алгоритмы факторизации целых чисел. | РГЗ |
| 3 | Редукция алгебраических выражений. Метод локализации. Алгоритм пополнения. | Отчет по лабораторной работе |
| 4 | Базисы Грёбнера. Решение системы полиномиальных уравнений. | РГЗ |

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т).

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

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

| № | Вид СРС | Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы |
|---|--|---|
| 1 | 2 | 3 |
| 1 | Подготовка рефератов и научных сообщений | Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017 г. |
| 2 | Самостоятельное решение задач | Рожков А.В. «Алгебраические методы криптографии. Методические указания», утвержденные кафедрой |

| | | |
|---|---------------------------------|--|
| | | функционального анализа и алгебры, протокол № 12 от 7 мая 2024. |
| 3 | Самостоятельное освоение теории | Рожков А.В. «Алгебра и теория чисел. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 12 от 7 мая 2024 г. |

1. Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

2. Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

3. Методические указания по использованию интерактивных методов обучения. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

4. Методические указания по подготовке эссе, рефератов, курсовых работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

5. Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

6. Методические указания по выполнению расчетно-графических заданий. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

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 с 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,

3. Образовательные технологии.

Активные и интерактивные формы, лекции, лабораторные занятия, контрольные работы, реферативные доклады (по некоторым темам в виде презентации) и зачет. В течение семестра магистры решают задачи, указанные преподавателем, к каждому лабораторному занятию. Каждый магистр готовит реферативный доклад по одной из ниже научных тем. Зачет выставляется после выполнения определенного количества (практических и теоретических) заданий контрольных работ и отчета по реферативному докладу. В случае невыполнения какого-то из приведенных требований, магистру для сдачи зачета предлагаются по усмотрению преподавателя некоторые практические и теоретические задания, подобные предложенным ниже.

К образовательным технологиям также относятся интерактивные методы обучения. Интерактивность подачи материала по дисциплине «Алгебраическая алгоритмика» предполагает не только взаимодействия вида «преподаватель - магистр» и «магистр - преподаватель», но и «магистр - магистр». Все эти виды взаимодействия хорошо достигаются при изложении материала на занятиях в ходе дискуссий, а также на

лабораторных занятиях в ходе изложения магистрами реферативных докладов (возможно в виде презентации).

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1 Фонд оценочных средств для проведения текущего контроля.

Список теоретических вопросов (для самостоятельных работ)

1. Константы и операторы в GAP и Sage.
2. Переменные и присваивания.
3. Функции.
4. Списки - тождественность и равенство списков.
5. Множества, Векторы и матрицы.
6. Записи.
7. Использование циклов.
8. Алгоритм пополнения.
9. Задача полиномиального упрощения.
10. Базисы Грёбнера. Решение системы полиномиальных уравнений.
11. Алгоритм Бухбергера.
12. Алгоритмы вычисления НОД в кольце целых чисел.
13. Алгоритмы вычисления НОД в кольцах полиномов.
14. Бинарный алгоритм вычисления НОД.
15. Расширенный алгоритм Евклида для полиномов над полем.
16. Алгоритм проверки на простоту.
17. Алгоритм тестирования.
18. Тест Эдуарда Люка – Лемера.
19. Тест Адлемана- Померанца-Рюмли.
20. Тесты псевдопростоты. Числа Кармайкла.
21. Разложение чисел на простые числа.
22. Метод Ферма.
23. Метод цепных дробей.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Список типовых алгоритмов (для самостоятельных занятий и зачета)

1. Нахождение примитивного элемента конечного поля.
2. Построение таблицы логарифма Якоби конечного поля.
3. Решение систем линейных уравнений над конечным полем.
4. Алгоритм быстрого возведения в степень.
5. Нахождение обратных элементов в конечном поле.
6. Расширения конечных полей.
7. Алгоритм шифрования AES: структура поля $GF(2^8)$, нахождение обратных элементов.
8. Алгоритм RSA – выбор секретных параметров p, q, d , вычисление открытого ключа n, e .
9. Рюкзачная система шифрования. Быстрорастущий вектор. Скрытие быстрорастущего вектора после преобразования умножения по модулю.
10. Решение систем линейных уравнений по разным модулям.
11. Решение систем линейных уравнений в кольце целых чисел.
12. Линейный регистр сдвига с обратной связью
$$S_{n+k} = a_{k-1}S_{n+k-1} + a_{k-2}S_{n+k-2} + \dots + a_1S_{n+1} + a_0S_n + a, n = 0, 1, 2, \dots$$

Критерии оценивания результатов обучения

| Оценка | Критерии оценивания по экзамену |
|---|--|
| Высокий уровень «5» (отлично) | оценку «отлично» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы. |
| Средний уровень «4» (хорошо) | оценку «хорошо» заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки. |
| Пороговый уровень «3» (удовлетворительно) | оценку «удовлетворительно» заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы. |
| Минимальный уровень «2» (неудовлетворительно) | оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы. |

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает формы допускает незначительные ошибки; студент умеет правильно объяснять материал, иллюстрируя его примерами

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры, довольно ограниченный объем знаний программного материала.

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 (модулю) 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 (модуля).

5.1 Основная литература:

1. Шевелев Ю.П. Дискретная математика, 5-е изд. [Электронный ресурс]. – СПб.: Лань, 2024. – URL: <https://reader.lanbook.com/book/399194>
2. Ерусалимский Я.М. Дискретная математика. Теория и практикум 2-е изд. [Электронный ресурс]. – СПб.: Лань, 2023. – URL: <https://e.lanbook.com/reader/book/319427/>

5.2 Дополнительная литература:

1. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 5-е изд. [Электронный ресурс]. - СПб.: Лань, 2024. - URL: <https://reader.lanbook.com/book/379334>
2. Шевелев Ю.П., Писаренко Л.А., Шевелев М.Ю. Сборник задач по дискретной математике (для занятий в группах) [Электронный ресурс]. – СПб.: Лань, 2022. – <https://reader.lanbook.com/book/211148>

5.3 Периодические издания:

Не предусмотрены

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» <https://urait.ru/>
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» <https://www.book.ru>
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» <https://e.lanbook.com>

Профессиональные базы данных:

1. Web of Science (WoS) <http://webofscience.com/>
2. Scopus <http://www.scopus.com/>
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley <https://onlinelibrary.wiley.com/>
5. Научная электронная библиотека (НЭБ) <http://www.elibrary.ru/>
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН <http://archive.neicon.ru>
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) <https://rusneb.ru/>
8. Президентская библиотека им. Б.Н. Ельцина <https://www.prilib.ru/>
9. Электронная коллекция Оксфордского Российского Фонда <https://ebookcentral.proquest.com/lib/kubanstate/home.action>
10. Springer Journals <https://link.springer.com/>
11. Nature Journals <https://www.nature.com/siteindex/index.html>
12. Springer Nature Protocols and Methods <https://experiments.springernature.com/sources/springer-protocols>
13. Springer Materials <http://materials.springer.com/>
14. zbMath <https://zbmath.org/>
15. Nano Database <https://nano.nature.com/>
16. Springer eBooks: <https://link.springer.com/>
17. "Лекториум ТВ" <http://www.lektorium.tv/>
18. Университетская информационная система РОССИЯ <http://uisrussia.msu.ru>

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. Американская патентная база данных <http://www.uspto.gov/patft/>

2. Полные тексты канадских диссертаций <http://www.nlc-bnc.ca/thesescanada/>
3. КиберЛенинка (<http://cyberleninka.ru/>);
4. Министерство науки и высшего образования Российской Федерации <https://www.minobrnauki.gov.ru/>;
5. Федеральный портал "Российское образование" <http://www.edu.ru/>;
6. Информационная система "Единое окно доступа к образовательным ресурсам" <http://window.edu.ru/>;
7. Единая коллекция цифровых образовательных ресурсов <http://school-collection.edu.ru/>.
8. Федеральный центр информационно-образовательных ресурсов (<http://fcior.edu.ru/>);
9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" <https://pushkininstitute.ru/>;
10. Справочно-информационный портал "Русский язык" <http://gramota.ru/>;
11. Служба тематических толковых словарей <http://www.glossary.ru/>;
12. Словари и энциклопедии <http://dic.academic.ru/>;
13. Образовательный портал "Учеба" <http://www.uceba.com/>;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--plai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы

КубГУ:

1. Среда модульного динамического обучения <http://moodle.kubsu.ru>
2. База учебных планов, учебно-методических комплексов, публикаций и конференций <http://mschool.kubsu.ru/>
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий <http://mschool.kubsu.ru;>
4. Электронный архив документов КубГУ <http://docspace.kubsu.ru/>
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" <http://icdau.kubsu.ru/>

6. Методические указания для обучающихся по освоению дисциплины (модуля).

Согласно учебному плану дисциплины «Информационная безопасность» итоговой формой контроля является зачет. Для сдачи зачета студент должен научиться на лабораторных занятиях решать практические задания по темам разделов 1-3, выполнять домашние задания. Типы практических заданий на зачет соответствуют заданиям. Также на зачете студентам предлагаются и теоретические задания, состоящие в письменном ответе на один из вопросов. Количество практических и теоретических заданий зависит от активности и результативности работы студента в течение семестра.

Важнейшим этапом курса является самостоятельная работа по дисциплине (модулю).

Для подготовки к ответам на теоретические вопросы в ходе контрольных работ и на зачете студентам достаточно использовать материал лекций. Весь этот теоретический материал содержится в учебных пособиях из списка основной литературы. Для изучения теоретического материала, необходимого для подготовки реферативного доклада, кроме основных источников литературы возможно использование дополнительных источников и Интернет-ресурса. В случае затруднений, возникающих у студентов в процессе самостоятельного изучения теории, преподаватель разъясняет сложные моменты на консультациях.

7. 7. Материально-техническое обеспечение по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

При заполнении таблицы учитывать все виды занятий, предусмотренные учебным планом по данной дисциплине: лекции, занятия семинарского типа (практические занятия, лабораторные работы), а также курсовое проектирование, консультации, текущий контроль и промежуточную аттестацию.

При использовании лаборатории указать ее наименование «Лаборатория...».

| Наименование специальных помещений | Оснащенность специальных помещений | Перечень лицензионного программного обеспечения |
|---|--|---|
| Учебные аудитории для проведения занятий лекционного типа | Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер | |
| Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации | Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование: | |
| Учебные аудитории для проведения лабораторных работ. Лаборатория... | Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование: | |
| Учебные аудитории для курсового проектирования (выполнения курсовых работ) | Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер Оборудование: | |

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

| Наименование помещений для самостоятельной работы обучающихся | Оснащенность помещений для самостоятельной работы обучающихся | Перечень лицензионного программного обеспечения |
|---|--|---|
| Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки) | Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi) | |
| Помещение для самостоятельной работы обучающихся (ауд. _____) | Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к | |

| | | |
|--|--|--|
| | информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi) | |
|--|--|--|

| № | Вид работ | Материально-техническое обеспечение дисциплины (модуля) и оснащенность |
|----|--|--|
| 1. | Лекционные занятия | Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) Программы, демонстрации видео материалов (проигрыватель «Windows Media Player»). Программы для демонстрации и создания презентаций («Microsoft Power Point»). |
| 2. | Семинарские занятия | Не предусмотрены |
| 3. | Лабораторные занятия | Лаборатория, укомплектованная специализированной мебелью и техническими средствами обучения – компьютерами с предустановленными GAP и Sage |
| 4. | Курсовое проектирование | Не предусмотрено |
| 5. | Групповые (индивидуальные) консультации | Аудитория для групповых занятий |
| 6. | Текущий контроль, промежуточная аттестация | Аудитория для групповых занятий |
| 7. | 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. |

7. Методические указания для обучающихся по освоению дисциплины (модуля).

Согласно учебному плану дисциплины «Алгебраическая алгоритмика» итоговой формой контроля является зачет. Для сдачи зачета магистр должен научиться на лабораторных занятиях решать практические задания по темам разделов 1-3, выполнять домашние задания. Типы практических заданий на зачет соответствуют заданиям. Также на зачете магистрам предлагаются и теоретические задания, состоящие в письменном ответе на один из вопросов. Количество практических и теоретических заданий зависит от активности и результативности работы магистра в течение семестра.

Важнейшим этапом курса является самостоятельная работа по дисциплине (модулю).

Для подготовки к ответам на теоретические вопросы в ходе контрольных работ и на зачете магистрам достаточно использовать материал лекций. Весь этот теоретический

материал содержится в учебных пособиях из списка основной литературы. Для изучения теоретического материала, необходимого для подготовки реферативного доклада, кроме основных источников литературы возможно использование дополнительных источников и Интернет-ресурса.

РЕЦЕНЗИЯ

на рабочую программу дисциплины

АЛГЕБРАИЧЕСКАЯ АЛГОРИТМИКА

Направление подготовки 01.04.01 Математика

Направленность Алгебраические методы защиты информации

Рабочая программа дисциплины Алгебраическая алгоритмика для магистров направленность «Алгебраические методы защиты информации» составлена доктором физико-математических наук, профессором кафедры функционального анализа и алгебры факультета математики и компьютерных наук Кубанского государственного университета Рожковым А.В.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования (ФГОС ВО) по направлению подготовки 01.04.01 Математика. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Содержание рабочей программы – это изучение теоретических основ Алгебраической алгоритмики. Информационные объекты. Компьютерная алгебра и численный анализ. Элементы теории сложности алгоритмов. Числовые функции, основные теоремы о евклидовых кольцах, алгоритмы решения линейных и квадратных уравнений в конечных полях, кольцах вычетов, алгоритмы нахождения наибольших общих делителей, алгоритмов проверки простоты чисел.

Рабочая программа дисциплины Алгебраическая алгоритмика для магистров направленность «Алгебраические методы защиты информации» сочетает теоретическую и практические части, что способствует более глубокому усвоению материала. Предложенные задания научно-исследовательского плана направлены на развитие практических навыков решения задач по направлению защита информации.

Считаю, что рабочая программа дисциплины Алгебраическая алгоритмика для магистров направленность «Алгебраические методы защиты информации» может быть рекомендована для подготовки магистров направления подготовки 01.04.01 Математика.

Кандидат технических наук,
доцент кафедры наземного транспорта и механики
ФГБОУ ВО «КубГТУ»



Л.Л. Ганижева

