**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФГБОУ ВПО «СГУ имени Н.Г. Чернышевского»**

Механико-математический факультет

|  |  |
| --- | --- |
| СОГЛАСОВАНО  заведующий кафедрой  компьютерной алгебры и теории чисел  В.Н. Кузнецов  "\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ г. | УТВЕРЖДАЮ  председатель НМС факультета  С.В. Тышкевич  "\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ г. |

**Фонд оценочных средств**

Текущего контроля и промежуточной аттестации по дисциплине

**Спецкурс 8.1**

Направление подготовки магистратуры

*020401 – Математика и компьютерные науки*

Профиль подготовки магистратуры

*Математические основы компьютерных наук*

Квалификация (степень) выпускника

*Магистр*

Форма обучения

*очная*

Саратов,

2016 год

1. ***Карта компетенций***

| Контролируемые компетенции  (шифр компетенции) | Планируемые результаты обучения  (знает, умеет, владеет, имеет навык) |
| --- | --- |
| готовностью к саморазвитию, самореализации, использованию творческого потенциала (ОК-3); | ***Знать:*** Основные теории и методы смежных отраслей знаний и особенности видов профессиональной деятельности, методику организации и проведения научной работы и решения практических задач |
| ***Уметь:*** самостоятельно осваивать новые методы исследований и адаптироваться к решению новых практических задач |
| ***Владеть:***навыками быстрой адаптации к изменениям условий среды, решения задач, требованиями должностных обязанностей |
| готовностью руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия (ОПК-5) | ***Знать:*** основные понятия теории чисел и криптографии |
| ***Уметь:*** применять основные разделы теории чисел в криптографии к различным разделам криптографии |
| ***Владеть:***методами решения задач теории чисел и криптографии |
| способность к творческому применению, развитию и реализации математически сложных алгоритмов в современных программных комплексах (ПК-5) | ***Знать:*** содержание ключевых понятий и определений из теории кодирования, используемых в теории и практике применения информационных технологий в науке, информационные ресурсы и базы данных по научно-исследовательской теме, существующие системы, средств и методы управления безопасностью компьютерных сетей с использованием кодов, исправляющих ошибки и декодирования линейными и циклическими кодами |
| ***Уметь:*** применять прикладное программное обеспечение для решения задач в профессиональной деятельности, науке и образовании, самостоятельно расширять и углублять знания в области информационных технологий |
| ***Владеть:*** навыками использования прикладного программного обеспечения для решения задач в профессиональной деятельности, науке и образовании, навыками использования интернет-технологий; навыками компьютерной обработки вычислительных задач с помощью аппарата теории кодирования и декодирования линейными и циклическими кодами |

***2. Показатели оценивания результатов обучения***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Контролируемые  компетенции | Шкала оценивания | | | |
| 2 | 3 | 4 | 5 |
| ОК – 3 | Не владеет  навыками быстрой адаптации к изменениям условий среды, решения задач и требованиями должностных обязанностей  Не знает  методы организации и проведения научной работы и решения практических задач  Не умеет  самостоятельно  осваивать новые методы исследований и адаптироваться к решению новых практических задач | Слабо владеет  навыками адаптации к изменениям условий среды, решения задач и требованиями должностных обязанностей  Знает методы решения практических задач в области своей профессиональной деятельности:  Умеет:  осваивать новые методики, изложенные в должностных инструкциях, методических материалах или учебных курсах | Владеет  навыками адаптации к изменениям условий среды, решения задач, требованиями должностных обязанностей  Знает методы смежных отраслей знаний, методику организации и проведения научной работы и решения практических задач  Умеет:  осваивать новые методы исследований и адаптироваться к решению новых практических задач | Свободно владеет  навыками быстрой адаптации к изменениям условий среды, решения задач, требованиями должностных обязанностей  Знает в полном объеме  основные теории и методологию смежных отраслей знаний и особенности видов профессиональной деятельности, методы организации и проведения научной работы и решения практических задач  Умеет в полной мере  самостоятельно  осваивать новые методы исследований и адаптироваться к решению новых практических задач |
| ОПК – 5 | Фрагментарные представления об основных понятиях теории чисел и криптографии, об  основных понятиях и методах кодирования над конечными полями | Неполные представления об основных понятиях теории чисел и криптографии, об  основных понятиях и методах кодирования над конечными полями | Сформированные, но содержащие отдельные пробелы в представлениях об основных понятиях теории чисел и криптографии, об  основных понятиях и методах кодирования над конечными полями | Сформированные систематические  представления об основных понятиях теории чисел и криптографии, об  основных понятиях и методах кодирования над конечными полями |
| ПК-5 | Не владеет навыками использования прикладного программного обеспечения для решения задач;  не умеет применять прикладное программное обеспечение для решения задач; не умеет самостоятельно углублять знания в области информационных технологий;  не знает основные понятия, не знает существующие системы и методы управления безопасностью компьютерных сетей | Недостаточно владеет навыками использования прикладного программного обеспечения для решения задач;  допускает ошибки в применении прикладного программного обеспечения для решения задач; слабо проявляет самостоятельность в углублении знаний в области информационных технологий;  слабо знает основные понятия, слабо ориентируется в существующих системах и методах управления безопасностью компьютерных сетей | Хорошо владеет навыками использования прикладного программного обеспечения для решения задач;  умеет применять прикладное программное обеспечение для решения задач;  самостоятельно углубляет знания в области информационных технологий;  хорошо знает основные понятия, хорошо ориентируется в существующих системах и методах управления безопасностью компьютерных сетей | Свободно владеет навыками использования прикладного программного обеспечения для решения задач;  свободно  применять прикладное программное обеспечение для решения задач;  самостоятельно расширяет и углубляет знания в области информационных технологий;  отлично знает основные понятия, свободно ориентируется в существующих системах и методах управления безопасностью компьютерных сетей |

***3.Оценочные средства***

* 1. **Задания для текущего контроля**

**Контрольная работа. Критерии оценки**

**Оценка «5»**

* наблюдается глубокое усвоение материала;
* студент свободно справляется с поставленными задачами;
* студент выбирает оптимальный путь решения задач.

**Оценка «4»**

* демонстрируется хорошее знание материала;
* допускает незначительные погрешности при решении задач;
* в основном решены все задачи.

**Оценка «3»**

* наблюдается усвоение основного материала;
* присутствуют неточности;
* не все задания доведены до конца.

**Оценка «2»**

* незнание материала;
* не решена большая часть заданий.

**Примерный вариант контрольной работы.**

1. Определение символа Лежандра, его свойства.

2. Вычислить .

3. Доказать, что сравнение разрешимо тогда и только тогда, когда .



4. Символ Якоби, его свойства.

**3.2 Промежуточная аттестация**

**Методическое обеспечение**

Подготовка к промежуточной аттестации осуществляется в период лекционных и семинарских занятий, а также в рамках самостоятельной работы. Во время самостоятельной подготовки студент пользуется конспектом лекций, основной и дополнительной литературой по дисциплине (см. рабочую программу дисциплины).

**Критерий оценивания**

Во время экзамена студент должен дать развернутый ответ на вопросы, изложенные в билете. Преподаватель вправе задавать дополнительные вопросы по всему изучаемому курсу.

Полнота ответа определяется показателями оценивания планируемых результатов обучения.

**Вопросы для проведения экзамена**

1. Основные задачи теории кодирования.
2. Коды Шеннопа и Гильберта-Мура.
3. Задача о помехоустойчивости.
4. Задача об увеличении скорости передачи информации.
5. Задача о защите информации.
6. Симметрические и асимметрические шифры.
7. Искажение знаков в шифрах простой замены и шифрах Виженера.
8. Метод рюкзака в асимметрических шифрах.
9. Система RSA шифрования с открытым ключом.
10. Криптографические хэш-функции.

ФОС по оцениванию результатов обучения обсуждался на заседании кафедры (протокол № 1 от 29.08.2016г).

Автор:

д.т.н., профессор,

зав. каф. компьютерной

алгебры и теории чисел В.Н.Кузнецов