Фонд оценочных средств
для промежуточной аттестации
по дисциплине
Теоретико-числовые методы в криптографии

Направление подготовки (специальность)
10.05.01 Компьютерная безопасность

Направленность (профиль)
специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Присваиваемая квалификация
специалист по защите информации

Форма обучения
очная

Челябинск 2025 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность 10.05.01 Компьютерная безопасность.
Специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем».
Дисциплина: **Теоретико-числовые методы в криптографии**.
Семестр (семестры) изучения: 6 семестр.
Форма (формы) промежуточной аттестации: зачёт 6 семестр.
Используется балльно-рейтинговая система для оценивания результатов.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Теоретико-числовые методы в криптографии» направлено на формирование следующих компетенций:

Коды компетенции согласно ФГОС (ОПОП ВО)	Содержание компетенций согласно ФГОС (ОПОП ВО)	Индикаторы достижения компетенции согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
1	2	3	4
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Критически анализирует проблемную ситуацию с целью выработки стратегии действий, аргументировано формулирует собственные суждения и оценки. УК-1.2. Использует критический анализ, систематизацию и обобщение информации для решения проблемной ситуации.	Знать: – основы выполнения эффективного поиска информации. Уметь: – определять критерии системного анализа для поставленных задач. Владеть: – навыками системного анализа и поиска информации.
ОПК-10	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства	ОПК-10.1 Знает основные методы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах; базовые понятия теории эллиптических кривых. ОПК-10.2 Умеет эффективно производить операции с большими	Знать: – точные и асимптотические оценки сложности основных теоретико-числовых алгоритмов; – основные теоретико-числовые методы и подходы для решения прикладных задач. Уметь: – применять основные теоретико-числовые результаты, изучаемые в курсе, для решения задач в

	криптографической защиты информации при решении задач профессиональной деятельности	числами, а также в кольцах вычетов, кольцах многочленов и конечных полях; исследовать и решать сравнения в кольцах вычетов; использовать достаточные условия простоты для построения больших простых чисел; оценивать теоретическую сложность применяемых алгоритмов. ОПК-10.3 Владеет навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов; методами построения быстрых вычислительных алгоритмов алгебры и теории чисел.	криптографии. Владеть: – основными теоретико-числовыми методами, которые используются или могут использоваться в криптографии.

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1 Виды оценочных средств

№ п/п	Код компетенции / планируемые результаты обучения	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1.	ОПК-10 УК-1	1. Оценка сложности арифметических операций	Контрольная работа. Решение задач. Максимальное количество баллов за работу -- 20 баллов.	Задача на зачёте.
2.	ОПК-10 УК-1	2. Тестирование чисел на простоту и построение больших простых чисел	Коллоквиум. Максимальное количество баллов за коллоквиум -- 20 баллов	Вопросы к зачету 1—5,9,15
3.	ОПК-10 УК-1	3. Факторизация целых чисел	Домашняя самостоятельная работа. Изучение алгоритма. Максимальное количество баллов за работу -- 20 баллов	Вопросы к зачету 10,11,12,16,17,18,19

Типовые задания, критерии и показатели оценивания в рамках текущего контроля представлены в рабочей программе дисциплины (модуля). Полные комплекты оценочных средств и контрольно-измерительных материалов хранятся на кафедре.

3.2. Содержание оценочных средств

3.2.1. Домашняя самостоятельная работа

1. Изучить алгоритм факторизации и сделать доклад.
2. Реализовать алгоритм. Написать программу для работы с большими числами.
3. Вычислить сложность алгоритма.
4. Привести числовой пример для маленького числа, иллюстрирующий работу алгоритма.

3.2.2. Пример контрольной работы

Контрольная работа

Для суммы квадратов первых n натуральных чисел справедлива формула

$$\sum_{j=1}^{n} = \frac{n(n+1)(2n+1)}{6}.$$

1. Используя обозначение O -большое, оценить в терминах n число двоичных операций , требующихся для вычисления левой части равенства.
2. Используя обозначение O -большое, оценить в терминах n число двоичных операций , требующихся для вычисления правой части равенства.
3. Используя обозначение O -большое, оценить в терминах простой функции от n число двоичных операций при вычислении n^n.
4. Оценить время, необходимое для проверки того, имеет ли число n простой делитель, не превосходящий m. Предположить, что имеется список всех простых чисел не превосходящих m. Воспользоваться теоремой о распределении простых чисел.

Экзамен по курсу "Теоретико-числовые методы в криптографии специальность 10.05.01 — Компьютерная безопасность
Билет 1

1. Тест Рабина –Миллера, его обоснование.
2. Метод Ферма (факторизация), его обоснование.
3. Показать, что если p и $2p-1$ — простые числа и $n = p(2p-1)$, то n — псевдопростое для 50% возможных оснований b, а именно, для тех b, которые являются квадратичными вычетами по модулю $2p-1$.
4. Пусть надо проверить простоту числа n при помощи последовательного деления на все нечетные числа, не превосходящие $\sqrt{n}$. Оценить число двоичных опереаций.

3.2.3. Вопросы к коллоквиуму

1. Тест на основе теоремы Ферма.
2. Свойства псевдопростых чисел (доказать).

3. Свойства чисел Кармайкла (доказать).
4. Тест Соловея-Штрассена, его обоснование.
5. Тест Рабина –Миллера, его обоснование.
6. Алгоритм Конягина-Померанса.
7. Алгоритм Миллера.
8. Детерминированный полиномиальный алгоритм проверки простоты чисел (AKS).
9. Тест на простоту для чисел специального вида.
10. Современные методы проверки простоты числа.

3.2.4. Вопросы к экзамену

1. Тест на основе теоремы Ферма.
2. Свойства псевдопростых чисел (доказать).
3. Свойства чисел Кармайкла (доказать).
4. Тест Соловея-Штрассена, его обоснование.
5. Тест Рабина –Миллера, его обоснование.
6. Ро-метод Полларда.
7. Вычисление квадратных корней по простому модулю.
8. Алгоритм Ленстры.
9. Алгоритм Конягина-Померанса.
10. Метод Шермана-Лемана.
11. Метод Ферма.
12. Алгоритм Полларда-Штрассена.
13. Алгоритм согласования (дискретное логарифмирование).
14. Индекс метод (дискретное логарифмирование).
15. Детерминированный полиномиальный алгоритм проверки простоты чисел (AKS).
16. Алгоритм Карацубы.
17. Эллиптические кривые над конечным полем. Группа точек.
18. Экспоненциальные алгоритмы.
19. Субэкспоненциальные алгоритмы.

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

В ходе изучения дисциплины «Теоретико-числовые методы в криптографии» студент должен выполнить одну контрольную работу, одну домашнюю самостоятельную работу и сдать один коллоквиум. В конце семестра сдаётся зачет.

Каждая из работ, коллоквиум оцениваются в 20 баллов, зачет оценивается в 40 баллов. Нарушение сроков без уважительной причины ведет за собой снижение баллов за контрольную работу и коллоквиум на 2 балла за каждую неделю задержки.

Билеты для зачета содержат 4 задания (2 практических задачи и 2 теоретических вопроса). За каждое выполненное задание билета студент может получить от 2 до 5 баллов. Если задание выполнено правильно, то оно оценивается 5 баллами. Если задание выполнено с ошибками, то баллы снижаются в зависимости от количества допущенных ошибок. Если допущена одна ошибка, то здание оценивается 4 баллами, допущены две ошибки – 3 баллами, допущены три ошибки – 2 баллами. Если задание выполнено частично, и выполненная часть задания не содержит ошибок, то оно оценивается 2 баллами. Если допущено более трех ошибок в задании или студент выполнил менее половины задания из билета, то за него он получает 0 баллов.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Контрольная работа	20
2	Домашняя самостоятельная работа	20
3	Коллоквиум	20
4	Зачет	40
	Итого	100

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств.

4.2.1 Критерии оценивания домашней самостоятельной работы, ответа на коллоквиуме

Критерии оценивания одного вопроса/задания

Показатели	Отлично/зачтено/ 5 баллов	Хорошо/зачтено/ 4 балла	Удовлетворительно /зачтено/ 3 балла	Неудовлетворительно/не зачтено/ 0-2 балла
1. Полнота изложения теоретического материала; 2. Правильность	Студентом дан полный, в логической последовательности развернутый ответ	Студентом дан развернутый ответ на поставленный вопрос, где студент демонстрирует	Студентом дан ответ, свидетельствующий, в основном, о знании процессов	Студентом дан ответ, который содержит ряд серьезных неточностей,

и/или аргументированность изложения (последовательность действий)	на поставленный вопрос, где он продемонстрировал знания предмета.	знания, однако допускает неточность в ответе.	изучаемой дисциплины, но отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, недостаточным умением давать аргументированные ответы и приводить примеры. Допускает несколько ошибок в содержании ответа.	обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, отсутствием логичности и последовательности. Студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.
	Высокий уровень освоения проверяемых компетенций	Средний уровень освоения проверяемых компетенций	Базовый уровень освоения проверяемых компетенций	Недостаточный уровень освоения проверяемых компетенций

4.2.2 Критерии оценивания контрольной работы

Максимальный балл за контрольную работу – 20 баллов.

Контрольная работа включает 4 задания.

Критерии оценивания каждого задания

Показатели	**Отлично/зачтено/ 5 баллов**	**Хорошо/зачтено/ 4 балла**	**Удовлетворительно /зачтено/ 3 балла**	**Неудовлетворительно/не зачтено/ 2 балла**
1. Полнота изложения теоретического материала; 2. Правильность и/или аргументированность изложения (последовательность действий)	Задание решено правильно, дан полный, развернутый ответ на поставленный вопрос.	Выполнено 3/4 задания, дан полный, развернутый ответ на поставленный вопрос, однако были допущены неточности в определении понятий, терминов и др.	Выполнено 1/2 задания, дан неполный ответ на поставленный вопрос.	Выполнено менее 1/2 задания, на поставленный вопросы ответ отсутствует или неполный, допущены существенные ошибки в терминах и понятиях.
	Высокий уровень освоения проверяемых компетенций	Средний уровень освоения проверяемых компетенций	Базовый уровень освоения проверяемых компетенций	Недостаточный уровень освоения проверяемых компетенций

4.2.3 Критерии оценивания теоретического вопроса зачета и практической задачи зачета

Максимальный балл за ответ на теоретический вопрос – 10 баллов.

Отлично/зачтено/ 9-10 баллов	**Хорошо/зачтено/ 7-8 баллов**	**Удовлетворительно/ зачтено/5-6 баллов**	**Неудовлетворительно/ не зачтено/0-4 баллов**
Студентом дан полный, в логической последовательности развернутый ответ на поставленный вопрос, в котором он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса.	Студентом дан развернутый ответ на поставленный вопрос, в котором студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствуют логичность и последовательность., однако допускается неточность.	Студентом дан ответ, свидетельствующий, в основном, о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточной логичностью и последовательностью ответа.	Студентом дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, отсутствием логичности и последовательности. Выводы поверхностны. Студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.
Высокий уровень освоения проверяемых компетенций	Средний уровень освоения проверяемых компетенций	Базовый уровень освоения проверяемых компетенций	Недостаточный уровень освоения проверяемых компетенций

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации:

Критерии оценивания зачета:

менее 60 – не зачтено

61 – 100 – зачтено.

Особенности проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обозначены в рабочей программе дисциплины (модуля).

Уровни сформированности компетенций определяется следующим образом:

1. Высокий уровень сформированности компетенций соответствует оценке «Отлично»:
   - предполагает формирование компетенций на высоком уровне, готовность к самостоятельной профессиональной деятельности,
   - студент способен аргументировать собственную точку зрения по дискуссионным вопросам дисциплины, решать ситуационные задачи, формулировать собственные выводы.
2. Средний уровень соответствует оценке «Хорошо»:
   - предполагает формирование компетенций на достаточном уровне,
   - студент способен давать развернутые ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Хорошо».
3. Базовый уровень соответствует оценке «Удовлетворительно»:
   - предполагает формирование компетенций на начальном уровне,
   - студент способен давать ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Удовлетворительно»,
   - студент способен отвечать на вопросы в закрытой форме. Количество правильных ответов – не менее 50%.
4. Низкий уровень соответствует оценке «Неудовлетворительно».

Специальность 10.05.01 Компьютерная безопасность
Специализация №6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»
Фонд оценочных средств по дисциплине «Теоретико-числовые методы в криптографии»
2025 год набора, очная форма обучения

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:
Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 6 от 20.02.2025

Председатель Ученого совета
математического факультета согласовано Е.А. Сбродова

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 8 от 01.02.2025

Заведующий кафедрой согласовано А. Н. Ручай

Автор (составитель) Кораблева В.В.

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1