Фонд оценочных средств для промежуточной аттестации

по дисциплине

Теория чисел

Направление подготовки (специальность)
10.05.01 Компьютерная безопасность

Направленность (профиль)
специализация № 1 «Анализ безопасности 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 № 1 «Анализ безопасности компьютерных систем».
Дисциплина: **Теория чисел**.
Семестр (семестры) изучения: 2 семестр.
Форма (формы) промежуточной аттестации: экзамен 2 семестр.
Используется балльно-рейтинговая система для оценивания результатов.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Теория чисел» 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**
ОПК-3	Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ОПК-3.1. Знает основные понятия теории чисел. ОПК-3.2. Умеет решать основные типы задач теории чисел. ОПК-3.3. Владеет навыками решения типовых линейных уравнений над полем и кольцом вычетов.	Знать: – основные понятия, связанные с теорией делимости, сравнениями и кольцами классов вычетов и их свойства; – формулировку основных результатов по этим темам. Уметь: – ориентироваться в соотношении между собой понятий теории чисел; – доказать свойства основных понятий курса; – доказать основные теоретические результаты, приводимые в курсе теории чисел. Владеть: – основами теории чисел; – теоретической базой, связанной с теорией делимости, сравнениями и кольцами классов вычетов; – теоретической базой, связанной с базовыми приложениями теории чисел 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-3	Раздел 1. Простые и составные числа. Делимость чисел. Раздел 2. Цепные дроби Раздел 3. Числовые сравнения Раздел 4. Сравнения с одним неизвестным	Контрольная работа №1	Вопрос в экзаменационном билете № 1–22
2.	ОПК-3	Раздел 5. Сравнения второй степени Раздел 6. Первообразные корни и индексы	Контрольная работа №2	Вопрос в экзаменационном билете № 23–32

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. Пример контрольных работ

Контрольная работа №1.

Вариант 1.

1. Найти наибольший общий делитель пары чисел 10920, 6600. Представить его в виде линейной комбинации исходных чисел.

2. Решить сравнение первой степени a) $441x \equiv 3(mod\ 557)$, b) $15x \equiv 321(mod\ 444)$.

3. Решить систему сравнений первой степени

$$\begin{cases} x \equiv 2(mod\ 4) \\ x \equiv 3(mod\ 5) \\ x \equiv 3(mod\ 7) \\ x \equiv 11(mod\ 13) \end{cases}$$

4. Решить систему сравнений первой степени

$$\begin{cases} 8x \equiv 6(mod\ 26) \\ 4x \equiv 7(mod\ 15) \\ 11x \equiv 23(mod\ 27) \end{cases}$$

5. Решить сравнение по составному модулю

$13x^4 + 11x^3 + 4x^2 + 7x + 20 \equiv 0(mod\ 100)$.

Вариант 2.

1. Найти наибольший общий делитель пары чисел 3492, 13392. Представить его в виде линейной комбинации исходных чисел.

2. Решить сравнение первой степени a) $352x \equiv 5(mod\ 599)$, b) $44x \equiv 548(mod\ 668)$.

3. Решить систему сравнений первой степени

$$\begin{cases} x \equiv 2(mod\ 5) \\ x \equiv 3(mod\ 6) \\ x \equiv 5(mod\ 11) \\ x \equiv 2(mod\ 13) \end{cases}$$

4. Решить систему сравнений первой степени

$$\begin{cases} 2x \equiv 6(mod\ 10) \\ 3x \equiv 7(mod\ 11) \\ 4x \equiv 8(mod\ 12) \end{cases}$$

5. Решить сравнение по составному модулю

$7x^4 + 10x^3 + 5x^2 + 13x + 35 \equiv 0(mod\ 144)$.

Контрольная работа №2

Вариант 1.

1. Разрешимо ли сравнение второй степени?

$x^2 \equiv 3(47)$; $x^2 \equiv 397(599)$.

2. Решить сравнения второй степени

$x^2 \equiv 2251(4721)$; $x^2 \equiv 1987(6277)$.

3. Найти наименьший первообразный корень. Построить таблицу индексов, и решить сравнение с ее помощью.

$m = 71;\ x^{10} \equiv 30$

Вариант 2.

1. Разрешимо ли сравнение второй степени?

   $x^2 \equiv 26(53)$; $x^2 \equiv 345(631)$.

2. Решить сравнения второй степени

   $x^2 \equiv 677(6743)$; $x^2 \equiv 3344(4273)$.

3. Найти наименьший первообразный корень. Построить таблицу индексов, и решить сравнение с ее помощью.

   $m = 83;\ x^{14} \equiv 65$.

3.2.2 *Вопросы к экзамену*

1. Кольцо целых чисел. Делимость. Свойства делимости.
2. Общий делитель. НОД. свойства НОД. Взаимная простота. Алгоритм Евклида.
3. Простые числа. Свойства простых чисел. Основная теорема арифметики.
4. Цепные дроби. Подходящие дроби. Свойства цепных дробей. Теорема о единственности представления рационального числа в виде цепной дроби.
5. Цепные дроби. Подходящие дроби. Свойства цепных дробей. Теорема о единственности представления действительного числа в виде цепной дроби.
6. Наилучшее приближение действительного числа. Теорема о наилучшем приближении.
7. Совершенные числа. Теорема Евклида (достаточное условие для четных чисел).
8. Совершенные числа. Теорема Эйлера (необходимое условие для четных чисел).
9. Простые числа Мерсенна. Простые числа Ферма. Свойства чисел Ферма. Открытые вопросы.
10. Мультипликативные функции. Лемма. Формула суммы распространенной на делители числа.
11. Сумма и число делителей числа.
12. Функция Мёбиуса. Леммы. Формула обращения Мёбиуса.
13. Функция Эйлера. Теорема о представлении числа суммой функций Эйлера. Теорема о вычислении функции Эйлера.
14. Сравнения. Свойства сравнения как бинарного отношения. Классы вычетов. Различные системы вычетов(полная, наименьшая, приведенная).
15. Свойства сравнений (леммы). Кольцо классов вычетов (теорема).
16. Деление в кольце классов вычетов. Две теоремы о делении.
17. Группа классов вычетов. Условие того, что кольцо классов вычетов образует поле.
18. Малая теорема Ферма. Теорема Эйлера.
19. Системы сравнений первой степени. Китайская теорема об остатках.
20. Линейные системы сравнений. Метод решения.
21. Сравнения по простому модулю. Две теоремы о сравнениях по простому модулю. Критерий Вильсона.
22. Сравнения по составному модулю. Теорема о равносильности сравнения по составному модулю системе сравнений по взаимно простым модулям. Теорема о сравнении по модулю p^k.
23. Вычеты и невычеты степени n. Леммы и теорема о квадратичном вычете по простому модулю.
24. Символ Лежандра. Теорема о свойствах символа Лежандра. Квадратичный закон взаимности.
25. Символ Якоби. Теорема о свойствах символа Якоби.
26. Сравнения по составному модулю. Теоремы о решении сравнений второй степени по модулям p^k и 2^k.
27. Показатель. Три теоремы о показателе. Первообразные корни.
28. Первообразные корни по простому модулю. Леммы. Теорема о существовании.
29. Первообразные корни по модулям p^k и 2p^k. Теоремы о существовании. Теорема об отыскании первообразных корней.
30. Индексы по модулям p^k и 2p^k. Теорема о степенях первообразного корня. Теорема(свойство индексов).
31. Критерий существования первообразных корней. Теорема (следствия).
32. Индексы по модулю 2^k.

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

На экзамене студент получает билет. В билете два теоретических вопроса и две задачи. На написание ответа дается 1,5 часа. После этого происходит оценка ответа. Преподаватель может задавать вопросы по тексту ответа. Студент должен на них ответить.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Контрольная работа № 1, 2	2x20=40
2	Экзамен (теоретический вопрос)	2x10=20
3	Экзамен (задача)	2x20=40
	Итого	100

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств.

4.2.1 Критерии оценивания теоретического вопроса экзамена

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 присутствует логичность и последовательность. Однако допускается неточность в ответе.	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	Средний уровень	Базовый уровень	Недостаточный уровень

освоения проверяемых компетенций	освоения проверяемых компетенций	освоения проверяемых компетенций	освоения проверяемых компетенций

4.2.2 Критерии оценивания практической задачи экзамена

Максимальный балл за практическую часть экзамена – 20 баллов.

Показатели	**Отлично/зачтено/15-20 баллов**	**Хорошо/зачтено/11-14 баллов**	**Удовлетворительно/зачтено/7-10 баллов**	**Неудовлетворительно/не зачтено/0-6 баллов**
1. Полнота изложения теоретического материала; 2. Правильность и/или аргументированность изложения (последовательность действий); 3. Самостоятельность ответа.	Обучающийся отлично знает материал, умеет грамотно сформулировать алгоритм решения задачи и не допускает ошибок.	Обучающийся хорошо знает материал, умеет грамотно сформулировать алгоритм решения задачи, но допускает незначительные ошибки.	Обучающийся знаком с материалом, но допускает фактические ошибки.	Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.
Уровень освоения проверяемых компетенций	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 выполнения контрольной работы

Максимальный балл за контрольную работу – 20 баллов.

Отлично/зачтено/17-20 баллов	**Хорошо/зачтено/13-16 баллов**	**Удовлетворительно/зачтено/10-12 баллов**	**Неудовлетворительно/не зачтено/0-9 баллов**
Работа выполнена в срок, обучающийся отлично знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу.	Работа выполнена в срок, обучающийся хорошо знает материал, умеет анализировать проблему и может грамотно прокомментировать выполненную работу. Обучающийся допускает незначительные ошибки.	Работа выполнена и сдана позднее, чем предполагалось. Обучающийся допускает незначительные ошибки.	Работа не выполнена, либо обучающийся не может ответить на контрольные вопросы, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.
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

Промежуточная аттестация в целом выставляется по результатам контрольных работ и ответа на экзаменационный билет.. Если какая-то часть не сдана, то студенту предлагаются дополнительные вопросы по этой части.

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

Для экзамена:

0-54 баллов - неудовлетворительно (2);
64-74 баллов - удовлетворительно (3);
75-90 баллов - хорошо (4);
91-100 баллов - отлично (5).

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 № 1 «Анализ безопасности компьютерных систем»
Фонд оценочных средств по дисциплине «Теория чисел»
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) Л. В. Шалагинов

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