Фонд оценочных средств
для промежуточной аттестации
по дисциплине
Линейные рекуррентные последовательности

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
2. Перечень формируемых компетенций
   2.1. Компетенции, закреплённые за дисциплиной
3. Содержание оценочных средств по дисциплине
   3.1. Виды оценочных средств
   3.2. Содержание оценочных средств
4. Порядок проведения и критерии оценивания промежуточной аттестации
   4.1. Порядок проведения промежуточной аттестации
   4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств
   4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность 10.05.01 Компьютерная безопасность.
Специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем».
Дисциплина: **Линейные рекуррентные последовательности**.
Семестр (семестры) изучения: 10 семестр.
Форма (формы) промежуточной аттестации: зачёт 10 семестр.
Используется балльно-рейтинговая система для оценивания результатов.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Линейные рекуррентные последовательности» 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 свойства основных дискретных структур: линейных рекуррентных последовательностей, графов, конечных автоматов, комбинаторных структур. ОПК-3.2 Умеет решать задачи периодичности и эквивалентности для линейных рекуррентных последовательностей и конечных автоматов. ОПК-3.2 Умеет применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач.	Знать: – понятие ценности информации, защиты информации, системы защиты и данных; – понятие информации по уровню доступа; – конфиденциальность информации; – понятие конфиденциальной информации; – требования к криптографическим системам защиты информации; – способы реализации криптографических методов; – понятие и виды криптографических атак; – криптографический протокол; – криптографические методы защиты информации; – методы стеганографии; – классификация методов шифрования; – требования к современным шифрам; – цели и концептуальные основы защиты информации; – требования к криптографическим

			системам защиты информации; – понятие и виды криптографических атак. Уметь: – производить анализ типов информации в зависимости от порядка ее предоставления; – делать разбор методов обеспечения информационной безопасности; – подразделять основные средства защиты по видам деятельности. Владеть: – разработкой поточного симметрического шифрования.
ОПК-10	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Знает основные типы криптографических методов защиты информации. ОПК-10.2 Умеет проводить анализ криптографической стойкости хеш-функции, в том числе с использованием автоматизированных средств. ОПК-10.3 Владеет подходами к разработке и анализу безопасности криптографических хеш-функции.	Знать: – различия между стеганографией и криптографией; – основные актуальные модели атак на алгоритмы цифровой подписи и их возможные результаты. Уметь: – использовать блочные алгоритмы шифрования для формирования хеш-функции; – использовать криптографические методы защиты информации для обеспечения безопасности как локальных, так и распределенных систем; – использовать односторонние функции в целях построения криптосистем; – использовать алгоритмы генерации, хранения и распределения ключей; – проектировать и использовать системы электронной цифровой подписи; – применять на практике алгоритмы управления открытыми ключами. Владеть: – основными методами симметричного шифрования; алгоритмами формирования хеш-функций; – инструментами обеспечения безопасной работы в сети Интернет; – методологией применения асимметричных криптосистем; методами управления ключами в системах с открытым ключом; – технологиями электронной цифровой подписи, инструментами обеспечения безопасной работы в сети Интернет.

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 ОПК-10	Раздел 1. Конечные поля	Лабораторная работа №1	Теоретические вопросы для зачета
2.	ОПК-3 ОПК-10	Раздел 2. Характеристический многочлен линейной рекуррентной последовательности	Лабораторная работа №2	Теоретические вопросы для зачета
3.	ОПК-3 ОПК-10	Раздел 3. Матрица линейной рекуррентной последовательности	Лабораторная работа №3	Теоретические вопросы для зачета
4.	ОПК-3 ОПК-10	Раздел 4. Период линейной рекуррентной последовательности	Лабораторная работа №4	Теоретические вопросы для зачета
5.	ОПК-3 ОПК-10	Раздел 5. Поточное шифрование на основе линейной рекуррентной последовательности	Лабораторная работы №5-6	Теоретические вопросы для зачета

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. Список лабораторных работ

1. Написать программу, реализующую разложение многочлена на неприводимые множители над полем с помощью алгоритма Берлекэмпа.
2. Написать программу для поиска минимального многочлен данной линейной рекуррентной последовательности.
3. Написать программу, вычисляющую порядок матрицы рекуррентной последовательности, используя нормальную жорданову форму.
4. Написать программу, вычисляющую минимальный период импульсной функции рекуррентной последовательности.
5. Написать программу для проверки того, является ли характеристический многочлен f(x) примитивным многочленом и линейная рекуррентная последовательность — последовательностью максимального периода.
6. Написать программу, реализующую поточное шифрование на основе комбинированной линейной рекуррентной последовательности со сложностью перебора ключа порядка w.

3.2.2. Перечень вопросов для зачета

Для данной линейной рекуррентной последовательности над полем F2 необходимо:

1. Разложить характеристический многочлен f(x) рекуррентной последовательности на неприводимые множители над полем F2 с помощью алгоритма Берлекэмпа.
2. Построить поле разложения многочлена f(x). Найти количество примитивных элементов и указать примитивный элемент поля разложения. Построить таблицу логарифма Якоби.
3. Вычислить порядок матрицы рекуррентной последовательности, используя нормальную жорданову форму.
4. Вычислить порядок характеристического многочлена f(x), используя разложение f(x) на неприводимые множители над полем F2.
5. Найти минимальный период импульсной функции рекуррентной последовательности.
6. Проверить, является ли характеристический многочлен f(x) примитивным многочленом и линейная рекуррентная последовательность — последовательностью максимального периода.
7. Найти минимальный многочлен линейной рекуррентной последовательности.
8. Разложить многочлены на неприводимые множители над полем Fpc
9. помощью алгоритма Кантора-Цассенхауза.
10. Вычислить порядки многочленов, используя их разложения на неприводимые множители над полем Fp
11. Реализовать поточное шифрование на основе комбинированной линейной рекуррентной последовательности над полем Fpco сложностью перебора ключа порядка w, вычислить максимальный период линейной рекуррентной последовательности.

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

В течение семестра студентам необходимо выполнить 6 лабораторных работ, каждая из которых в случае безупречного выполнения оценивается в 10 баллов.

Кроме того, в рамках зачета студентам предлагается 3 вопроса, каждый из которых оценивается в 10 баллов.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Лабораторная работа (№1-6)	6x10=50
2	Зачет	3x10=30
	Итого	80

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств.

4.2.1 Критерии оценивания теоретического вопроса

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 балла
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.
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 лабораторной работы

Лабораторная работа выполняется на любом доступной студенту языке программирования.

Максимальный балл за лабораторную работу – 10 баллов.

Отлично/зачтено /9-10 баллов	**Хорошо/зачтено/ 7-8 баллов**	**Удовлетворительно/зачтено/ 5-6 баллов**	**Неудовлетворительно/не зачтено /0-4 балла**
Работа выполнена в срок, обучающийся отлично знает материал, умеет анализировать проблему и может грамотно сформулировать доказательство.	Работа выполнена в срок, обучающийся хорошо знает материал, умеет анализировать проблему, но допускает ошибки в доказательствах.	Работа выполнена и сдана позднее, чем предполагалось, либо обучающийся допускает фактические 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

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

0-50 баллов - не зачтено;

51-80 баллов - 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 «Линейные рекуррентные последовательности»
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)		А. Н. Ручай

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