Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)
Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ
Первый проректор
(должность)
_____ /Т.Р. Змызгова/
(подпись, Ф.И.О.)
«01» августа 2022 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

(наименование дисциплины)

образовательной программы высшего образования –

программы специалитета

«10.05.03 - Информационная безопасность автоматизированных систем»

Специализация (Специализация №5): **«Безопасность открытых информационных систем»**

Форма обучения: очная

Курган 2022

Рабочая программа дисциплины «Математическая логика и теория алгоритмов» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» («Безопасность открытых информационных систем»), утвержденным для очной формы обучения 30 августа 2022 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 29 августа 2022 года, протокол № 1.

Рабочую программу составил:
канд. пед. наук, доцент _____ /Т.А. Никифорова/

Согласовано:

Зав. кафедрой «БИАС»
канд. тех. наук, доцент _____ /Д.И. Дик/

Начальник Управления
образовательной деятельности _____ /И.В. Григоренко/

Специалист по учебно-методической
работе учебно-методического отдела _____ /Г.В. Казанкова/

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: **3** зачетных единиц трудоемкости (**108** академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		5
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**64**	**64**
Лекции	32	32
Лабораторные работы	-	-
Практические занятия	32	32
Самостоятельная работа, всего часов в том числе:	**44**	**44**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (подготовка к практическим, лабораторным занятиям и рубежному контролю)	26	26
Вид промежуточной аттестации	**Зачет**	**Зачет**
	108	**108**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Математическая логика и теория алгоритмов» относится к бязательным дисциплинам блока дисциплин модуля «Математические и естественно-научные дисциплины».

Краткое содержание. Математическая логика. Логические высказывания. Алгебра логики. Логические функции. Минимизация логических функций в классе ДНФ. Предикаты. Формулы логики предикатов. Приложение логики предикатов в теории практики информационной безопасности и основ искусственного интеллекта. Теория алгоритмов как наука. Понятие "алгоритм". Свойства алгоритма. Формализация понятия алгоритма. Абстрактная машина А. Тьюринга. Абстрактная машина Э. Поста. Нормальные алгорифмы А.А. Маркова. Сложность алгоритма.

Изучение дисциплины «Математическая логика и теория алгоритмов» основывается на базе таких дисциплин как «Математический анализ», «Алгебра и геометрия», «Дискретная математика», «Языки программирования» и «Технологии и методы программирования». Знания и навыки, полученные при изучении дисциплины «Математическая логика и теория алгоритмов», широко используются студентами при изучении общепрофессиональных и специальных дисциплин, связанных с вопросами проектирования, разработки, эксплуатации и внедрения систем защиты информации.

Результаты обучения по дисциплине необходимы для выполнения выпускной квалификационной работы в части проектирования систем или модулей защиты информации криптографическими методами.

Освоение следующих компетенций на уровне не ниже порогового: способен использовать математические методы, необходимые для решения задач профессиональной деятельности (ОПК-3).

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины «Математическая логика и теория алгоритмов» является формирование общепрофессиональных и специальных компетентностей посредством знакомства студентов с базовыми понятиями математической логики и теория алгоритмов, с математическими основами защиты информации, с методами разработки алгоритмов посредством рассмотрения примеров реализации абстрактных машин теории алгоритмов на практике, а также ознакомление с основными понятиями и методами математической логики и теории алгоритмов с ориентацией на их использование в практической информатике и вычислительной технике, формирование устойчивого алгоритмического мышления у студентов, изучение фундаментальных свойств алгоритмов и приобретение практических навыков использования и анализа алгоритмов ИБ при создании программных систем.

Задачами освоения дисциплины «Математическая логика и теория алгоритмов» являются:

- заложить базовые знания для восприятия последующих математических дисциплин;

- сформировать навыки математического моделирования мыслительного процесса в различных предметных областях;

- сформировать умение выполнять оценку сложности алгоритмов;

- изучить формализацию понятия алгоритм на примере машины А. Тьюринга, машины Э. Поста, нормального алгоритма А.А. Маркова, иметь представление об алгоритмически неразрешимых проблемах;

- изучить основные понятия, связанные с оценкой сложности алгоритмов и вычислений, освоить проблематику NP-полноты.

Компетенции, формируемые в результате освоения дисциплины «Математическая логика и теория алгоритмов»:

- способен использовать математические методы, необходимые для решения задач профессиональной деятельности (ОПК-3).

В результате изучения дисциплины «Математическая логика и теория алгоритмов» обучающийся должен:

знать:

- соответствующий математический аппарат математической логики (высказывания, логические операции и функции, минимизация логических функций, предикаты, формулы логики предикатов и др.) и теории алгоритмов (абстрактные машины и теории алгоритмов для формализации понятия алгоритма, оценка сложности алгоритмов и др.) (для ОПК-3);
- основные методы применения математического аппарата математической логики и теории алгоритмов для формализации и решения профессиональных задач (для ОПК-3);
- новые образцы программных, технических средств и возможности информационных технологий, направленных на защиту информации (для ОПК-3);
- критерии оценки эффективности применяемых криптографических средств защиты информации (для ОПК-3).

уметь:

- корректно применять при решении профессиональных задач соответствующий математический аппарат математической логики и теории алгоритмов, в том числе с использованием вычислительной техники (ОПК-3).
- проводить оценки сложности криптоалгоритмов и эффективности применяемых криптографических средств защиты информации (для ОПК-3);

владеть:

- способностью использовать математические методы, необходимые для решения задач профессиональной деятельности, а именно: соответствующий математический аппарат математической логики и теории алгоритмов, в том числе с использованием вычислительной техники (для ОПК-3).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем		
			Лекции	Лаборатор. работы	Практич. занятия
семестр 5					
Модуль 1. **Математическая логика**					
Рубеж 1	Тема 1.	Математическая логика	2		
	Тема 2.	Логика высказываний	4		4
	Тема 3.	Алгебра логики	4		2
	Тема 4.	Логика предикатов	2		2
	Тема 5.	Логические схемы	2		1
	Рубежный контроль 1 (*решение задач*)				1
Модуль 2. **Логика предикатов и основы искусственного интеллекта**					
Рубеж 2	Тема 6.	Основы языка логического программирования	2		6
	Тема 7.	Рекурсия	2		
Модуль 3. **Теория алгоритмов**					
Рубеж 2	Тема 8.	Теория алгоритмов как наука.	2		
	Тема 9.	Алгоритм и свойства алгоритма	2		
	Тема 10.	Формализация понятия алгоритм. Теория рекурсивных функций.	2		
	Тема 11.	Абстрактная машина А.Тьюринга	2		4
	Тема 12.	Абстрактная машина Э. Поста	2		2
	Тема 13.	Нормальные алгоритмы Маркова	2		4
	Тема 14.	Сложность алгоритмов	2		4
	Рубежный контроль 2 (*решение задач по теории алгоритмов*)				2
		Всего за семестр:	**32**		**32**

4.2. Содержание лекционных занятий

Модуль 1. Математическая логика

Тема 1. **Математическая логика**

Математическая логика как учебная дисциплина и как наука. История развития. Дискретность и непрерывность в природе и в теории. Основные понятия математической логики.

Проблемы логических систем. Формализация. Исчисление высказываний и предикатов. Критика классической логики. Многозначная логика. Элементы нечеткой логики. Логика и информационные технологии.

Тема 2. **Логика высказываний**

Понятие логического высказывания и его свойства. Мера истинности логического высказывания. Семантика. Простое и сложное (составное) логическое высказывание. Логические операции (связки) и их интерпретация в естественном языке: логическое сложение, логическое умножение, отрицание, импликация, сложение Жегалкина, эквивалентность. Вычисление истинности сложных логических высказываний. Старшинство операций. Формализация суждений. Высказывательные функции и их

интерпретация. Таблица истинности. Вычисление истинности высказывательных функций.

Тема 3. **Алгебра логики**

Носитель и сигнатура алгебры логики. Свойства сигнатуры. Эквивалентные преобразования высказывательных функций. Формулы алгебры логики. Классы логических формул.

Полностью и частично определенные логические функции. Существенные и фиктивные переменные. Способы задания логических функций. Задача восстановления аналитического представления функции по табличному заданию. Понятие первичного терма, импликанты и конституенты и их свойства. Нормальные формы представления логических функций (ДНФ, СовДНФ, КНФ, СовКНФ). Примеры.

Понятие сложности логической функции в ДНФ. Постановка задачи нахождения минимальной ДНФ. Свойства алгебры логики, понижающие сложность ДНФ. Геометрическая интерпретация логической функции. Гиперкуб и его свойства. Интервал и его свойства. Максимальный интервал и простая импликанта. Сокращенная и тупиковая ДНФ. Алгоритм Квайна-МакКласки порождения тупиковых и минимальных ДНФ заданной функции.

Минимизация логических функций в классе ДНФ.

Суперпозиция функций. Функционально полные системы функций. Базис. Классы логических функций: К0, К1, Кл, Кс, Км. Критерий Поста-Яблонского. Типовые базисы и их аппаратная реализация.

Тема 4. **Логика предикатов**

Логические высказывания с переменными. Предикат (одноместный и многоместный). Область определения предиката. Область истинности предиката. Тождественно истинные и тождественно ложные предикаты. Выполнимые предикаты. Таблица истинности для предиката. Логические операции над предикатами. Кванторные операции.

Алфавит для определения формул логики предикатов. Определение формулы логики предикатов. Интерпретация формулы предиката. Свободные и связанные переменные. Замкнутая формула. Правила эквивалентных преобразований в логике предикатов.

Нормальная и предварённая форма. Выполнимые и общезначимые формулы. Тождественно истинные формулы. Проблема разрешимости в логике предикатов.

Элементы доказательства в логике. Доказательства, основанные на эквивалентности. Объект и субъект доказательства. Клауза. Причина и следствие. Доказательства в логике предикатов. Логика предикатов в математическом анализе. Формулировка определений и утверждений.

Тема 5. **Логические схемы**

Понятие логической схемы. Задача анализа и задача синтеза логической схемы. Решение задачи анализа логической схемы. Метод синтеза логической схемы посредством моделирования элементов классического базиса.

Модуль 2. **Логика предикатов и основы искусственного интеллекта**

Тема 6. **Основы логического программирования**

Парадигма логического программирования. Основы логики предикатов в логическом программировании.

Основы языка логического программирования: утверждение: факт, правило; предикат, термы, внутренняя или внешняя цель, и др. Стандартные домены. Классификация

доменов. Полное объявление типов доменов на Prolog: простое имя, список, структура, файлы. Программа с точки зрения логического программирования. Структура программы на Prolog. Основные операции в Prolog: арифметические, логические, операции отношения. Примеры. Согласование переменных. Основные функции Prolog.
Стандартные предикаты ввода данных Prolog. Режимы передачи. Примеры.
Стандартные предикаты вывода данных Prolog. Форматный вывод данных. Режимы передачи. Примеры.
Предикат cut (или !) языка Prolog. "Зеленые" и "красные" отсечения. Примеры.

Тема 7. **Рекурсия**

Повторение на языке Prolog. Примеры правил. Рекурсия и откат в логическом программировании. Рекурсия (нисходящая или концевая) языка логического программирования Prolog. Примеры предикатов.

Модуль 3. **Теория алгоритмов**

Тема 8. **Теория алгоритмов как наука**

Теория алгоритмов как наука. Задачи теории алгоритмов. Персоналии в теории алгоритмов. Возникновение теории алгоритмов. Направления в теории алгоритмов. Дескриптивная и метрическая теория алгоритмов. Качественная и количественная теория алгоритмов.

Тема 9. **Алгоритм и свойства алгоритма**

Алгоритм. Различные подходы к понятию. Возникновение термина "алгоритм". Наивное определение понятия "алгоритм". Различные подходы к понятию «алгоритм».
Неформальное определение алгоритма.
Свойства алгоритма. Основные требования к алгоритмам. Примеры алгоритмов. Роль алгоритмов в информатике. Способы представления алгоритмов.
Алгоритмические проблемы. Проблема разрешимости. Примеры неразрешимых проблем.

Тема 10. **Формализация понятия алгоритм**

Формализация понятия "алгоритм". Понятие вычислимости и вычислительные процедуры. Три основных класса алгоритмических моделей. Эквивалентность математических моделей понятия "алгоритм". Эквивалентность формальных определений алгоритма.

Теория рекурсивных функций. Понятие алгоритма и вычислимой функции. Невычислимые функции. Понятие алгоритмической системы. Сведение общего понятия вычислимой функции к функции, аргументами и значениями которой являются слова конечного алфавита. Базовые функции. Операторы суперпозиции, примитивной рекурсии и минимизации. Свойства операторов суперпозиции, примитивной рекурсии и минимизации (m-операция). Примитивно-рекурсивные функции. Свойства примитивно-рекурсивных функций. Примеры ПРФ. Частично-рекурсивные функции. Определение частично рекурсивных функций. Универсальная частично-рекурсивная функция. Примеры частично-рекурсивных функций. Тезис Черча. Рекурсивные функции. Общерекурсивные функции. Примеры общерекурсивных функций.

Тема 11. **Абстрактная машина А.Тьюринга**

Алгоритм как абстрактная машина. Формализация понятия алгоритма – Машина Тьюринга. Простейшие машины Тьюринга. Тезис Тьюринга. Основная гипотеза теории алгоритмов в форме Тьюринга. Устройство машины Тьюринга. Конфигурация машины Тьюринга.
Описание МТ. Способы представления машины Тьюринга: в виде протокола, в виде таблицы соответствия, в виде графа.

Простейшие машины Тьюринга. Операции на машинах Тьюринга (операция композиции, операция ветвления, операция зацикливания) и их свойства. Базис элементарных машин Тьюринга. Функция, вычислимая по Тьюрингу. Функция, правильно-вычислимая по Тьюрингу. Доказательство существования функций, невычислимых по Тьюрингу.

Многоленточные и многоголовочные машины Тьюринга. Универсальная машина Тьюринга. Недетерминированные машины Тьюринга.

Совпадение класса функций, правильно-вычислимых по Тьюрингу, и класса частично рекурсивных функций.

Муравей Лэнгтона – двумерная МТ

Тема 12. **Абстрактная машина Э. Поста**

Машина Поста. Принцип работы МП. Команды машины Поста. Представление чисел в машине Поста. Машина Поста-Успенского. Универсальная машина Поста.

Тема 13. **Нормальные алгоритмы Маркова**

Нормальный алгорифм Маркова в алфавите и над алфавитом. Нормально-вычислимые функции. Примеры нормальных алгорифмов (тождественный нормальный алгорифм, нормальный алгорифм левого присоединения, нормальный алгорифм правого присоединения, нормальный алгорифм удвоения, некоторые арифметические алгорифмы). Универсальный алгоритм Маркова.

Основная гипотеза теории алгоритмов в форме Маркова.

Эквивалентность определений алгоритма в виде машины Тьюринга и нормального алгоритма Маркова.

Тема 14. **Сложность алгоритмов**

Меры сложности алгоритмов. Понятие сложности алгоритмов и вычислений. Полиномиальная эквивалентность. Экспоненциальная сложность. Недетерминированные алгоритмы. Недетерминированная машина Тьюринга. Псевдополиномиальный алгоритм.

Эффективные алгоритмы. Легко и трудно разрешимые задачи. О-нотация. Основные свойства.

Классы сложности алгоритмов. Иерархия по времени и иерархия по памяти.

Классы сложности: P, NP, co-NP, NP-C, co-NP-C, UP, #P, #P-C, L, NL, NC, P-C, PSPACE, PSPACE-C, EXPTIME, NEXPTIME, EXPSPACE, 2-EXPTIME, PR, RE, Co-RE, RE-C, Co-RE-C, R, BQP, BPP, RP, ZPP, PP, PCP, IP, PH. Классы задач P и NP. Проблема: равенство классов P и NP? NP–полные и NP–трудные языки и задачи. Примеры NP-полных задач, методы доказательства NP-полноты. AI-полная задача.

4.3. Практические занятия

Номер темы	Наименование темы	Наименование практических занятий	Норматив времени, час.
Модуль 1. **Математическая логика**			
2	Логика высказываний	*Практическая работа № 1.* Логика высказываний	4
3	Алгебра логики	*Практическая работа № 2.* Алгебра логики	2
4	Логика предикатов	*Практическая работа № 3.* Логика предикатов	2
5	Логические схемы	*Практическая работа № 4.* Логические схемы компьютера	1
	Рубежный контроль 1 (*решение задач*)		1

Модуль 2. **Логика предикатов и основы искусственного интеллекта**			
6	Основы языка логического программирования	*Практическая работа № 5.* Язык логического программирования Prolog	6
Модуль 3. **Теория алгоритмов**			
11	Абстрактная машина А.Тьюринга	*Практическая работа № 6.* Абстрактная машина А.Тьюринга	4
12	Абстрактная машина Э. Поста	*Практическая работа № 7.* Абстрактная машина Э. Поста	2
13	Нормальные алгоритмы Маркова	*Практическая работа № 8.* Нормальные алгоритмы Маркова	4
14	Сложность алгоритмов	*Практическая работа № 9.* Сложность алгоритмов	4
	Рубежный контроль 2 (*решение задач по теории алгоритмов*)		2
		Всего за семестр	**32**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей практической работе.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения практических работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем перед началом работы.

Преподавателем запланировано применение на практических занятиях технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на практических занятиях в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает подготовку к практическим занятиям, к рубежным контролям, подготовку к зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.

Углубленное изучение разделов, тем дисциплины, не вошедших в лекционный курс, а именно: Логика предикатов, Логика высказываний, Алгебра логики, Основы логического программирования.	8
Подготовка к практическим занятиям (по 1 часа к каждому занятию)	14
Подготовка к рубежному контролю (по 2 ч к каждому рубежу)	4
Подготовка к зачету	18
Всего:	**44**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ.
2. Банк тестовых заданий к рубежным контролям № 1, № 2.
3. Вопросы к зачету.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

№	Наименование	Содержание					
1	Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)*	*Распределение баллов, 5 семестр*					
		Вид учебной работы:	Посещение лекций	Выполнение практических работ	Рубежный контроль №1	Рубежный контроль №2	зачет
		Балльная оценка:	$0{,}5_б$ x 16 = $8_б$	$6_б$ x 9 = $54_б$	4	4	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета	60 и менее баллов – незачтено; 61…73 – зачтено; 74… 90 – зачтено; 91…100 – зачтено					
3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации (зачету) студент должен набрать не менее 50 баллов, выполнить все практические работы. Для получения зачета «автоматически» студенту необходимо набрать 61 балл. По согласованию с преподавателем студенту могут быть добавлены дополнительные (бонусные) баллы за активность на практических занятиях, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения практических работ, за участие в значимых учебных и внеучебных мероприятиях кафедры.					

4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае, если к промежуточной аттестации (зачету) набрана сумма менее 50 баллов (не выполнены все задания), необходимо выполнить дополнительные задания, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных практических занятий. Формы дополнительных заданий (назначаются преподавателем): - выполнение и защита пропущенной практической работы (при невозможности дополнительного проведения работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 10 баллов. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежный контроль № 1 и Рубежный контроль № 2 проводятся в форме защиты решений практических заданий.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии.

Задания рубежного контроля № 1 состоят из заданий по соответствующим разделам теории математической логики. На решение заданий при рубежном контроле студенту отводится 1 академический час.

Задания рубежного контроля № 2 состоят из 3 заданий на построение алгоритмов для абстрактных машин. На решение заданий при рубежном контроле студенту отводится 2 академических часа.

Баллы студенту выставляются в зависимости от качества и сложности алгоритма. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%

«удовлетворительно» – 50% - 70%

«хорошо» – 70% - 90%

«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты решения практических заданий каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Зачет проводится в форме ответа на вопросы билета. Экзаменационный билет состоит из 2 теоретических вопросов и 1 практического задания. Каждый теоретический вопрос оценивается в 6 баллов. Практическое задание оценивается в 18 баллов. Вопросы зачета доводятся до студентов на последней лекции в семестре. На подготовку ответа студенту отводится 1 астрономический час.

Результаты текущего контроля успеваемости, зачета заносятся преподавателем в экзаменационную ведомость, которые сдаются в орготдел института в день зачета, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей, зачета

1-ый рубежный контроль *(практические задания)*

1. Записать высказывания в виде формул логики высказываний.
   a. всякое N, делящееся на 12 делится на 2, 4 и 6.
2. Построить таблицы истинности для формул
   a. $BC \to (\overline{A \vee B} \sim \overline{C})$
3. Доказать, что формулы являются тавтологиями
   a. $((A \vee B)(A \vee \overline{B})) \sim A$
4. Доказать полноту (неполноту) систем булевых функций
   a. $\{\sim, \oplus\}$
5. Получить СДНФ для формул, а затем перейти к СКНФ:
   a. $(x \to y) \to (x \oplus z)$
6. Получить СКНФ, а затем перейти к СДНФ
   a. $(x \vee y)(x \vee z) \vee xy$
7. Получить МДНФ для формул
   a. $((x \oplus y) \sim z) \to x$
8. Проверить истинность соотношений тремя способами (используя определение логического следствия и пп. 3,4 теоремы 2).
   $x \to (y \to z), x \to y \vDash x \to z$;
9. Пусть Φ, Ψ, X, Θ - формулы исчисления высказываний. Построить вывод формулы исчисления высказываний из данного множества гипотез. $\Phi \vdash \Psi \to (\Phi \wedge \Psi)$;
10. Выписать все подформулы данной формулы сигнатуры $\Sigma = \{+, \cdot, \leq, 0\}$ и определить свободные и связанные переменные формулы: $\forall x((x + y \leq x) \wedge \neg (x = 0))$;

2-ый рубежный контроль *(практические задания)*

- Построить Машину Тьюринга T, вычисляющую следующую функцию.

$$\overline{sg}(x) = \begin{cases} 0, \text{если } x > 0, \\ 1, \text{если } x = 0; \end{cases}$$

- Построить Машину Поста, которая выполняет сложение двух целых неотрицательных чисел.
- Построить нормальный алгорифм Маркова, который добавляет две единицы к входному слову, состоящему из последовательности единиц.
- Вычислить сложность полученных алгоритмов.

Примерная тематика вопросов, выносимых на зачет в 5-ом семестре

1. Математическая логика как наука. Предмет. Объект. Задачи математической логики. История математической логики. Возникновение математической логики. Направления в математической логике.
2. Основные понятия математической логики. Логика высказываний. Понятие высказывания. Логические операции над высказываниями, таблицы истинности.
3. Алгебра логики. Формула алгебры логики высказываний, определение. Логические значения формулы алгебры логики. Таблицы истинности. Равносильные

формулы алгебры логики высказываний, тождественно-истинные и тождественно-ложные формулы, определения. Основные равносильности (доказательство).

4. Алгебра Буля, определение. Функции Буля. Различные интерпретации булевой алгебры. Функции Буля. Определение функции Буля n переменных. Постоянные и равные функции, понятия. Количество различных функций Буля n переменных. Таблицы истинности. Представление произвольной функции алгебры логики в виде формулы алгебры логики. Представление Булевой функции в виде формулы логики высказываний.

5. Критерии полноты систем булевых функций. Псевдобулевы функции и их представление рядами Фурье. Критерии полноты систем функций k-значной логики. Минимизация булевых функций.

6. Логика высказываний. Свойства совершенства формулы логики высказываний. Закон двойственности. Определение двойственной формулы и теорема (без доказательства). Дизьюнктивная нормальная форма и совершенная дизьюнктивная нормальная форма (ДНФ и СДНФ). Определения. Коньюнктивная нормальная форма и совершенная коньюнктивная нормальная форма (КНФ и СКНФ). Определения. Проблема разрешимости. Выполнимые формулы. Критерии тождественной истинности и тождественной ложности формул логики высказываний.

7. Приложения алгебры логики в технике и других областях. Приложения алгебры логики высказываний в технике (релейно-контактные схемы). Проблема минимизации.

8. Решение логических задач методами алгебры логики высказываний.

9. Исчисление высказываний (определение, этапы построения). Алфавит. Определение формулы исчисления высказываний. Подформулы. Доказуемость формул. Аксиомы исчисления высказываний. Правила вывода (правило подстановки и правило заключения). Производные правила вывода (правило одновременной подстановки, правило сложного заключения, правило силлогизма, правило контрпозиции, снятия двойного отрицания).

10. Исчисление высказываний. Понятие выводимости формул из совокупности формул (определение формулы, определение вывода). Правила вывода из совокупности формул. Доказательство некоторых законов логики: Закон перестановки посылок, Закон соединения посылок, Закон разъединения посылок, Закон исключения третьего.

11. Связь между алгеброй высказываний и исчислением высказываний. Проблемы аксиоматического исчисления высказываний (разрешимость, непротиворечивость, полнота, независимость).

12. Логика предикатов. Исчисления предикатов. Понятие субъекта, понятие предиката. Одноместный предикат, область определения предиката. Множество истинности предиката. Тождественно-истинный и тождественно-ложный предикат. Двухместный предикат. Логические операции над предикатами. Область истинности. Кванторные операции. Применение кванторных операций к одноместному и двухместному предикатам.

13. Логика предикатов. Определение формулы логики предикатов. Логические значения формулы логики предикатов. Определение равносильных формул логики предикатов. Основные равносильности логики предикатов (с доказательством). Нормальная форма формулы логики предикатов и предваренная нормальная форма формулы логики предикатов (определения). Определение выполнимой формулы логики предикатов, общезначимой, тождественно-ложной.

14. Логика предикатов. Общезначимость и выполнимость формул. Проблема разрешимости в логике предикатов. Алгоритмы распознавания общезначимости формул.
15. Логика предикатов. Применение языка логики предикатов для записи математических определений, построения отрицания предложений. Аксиоматическое исчисление предикатов.
16. Исчисление предикатов. Применение языка логики предикатов в языках логического программирования (на примере языка Prolog).
17. Гёделевская нумерация формул, аксиом и правил вывода исчисления предикатов. Рекурсивно перечислимые множества. Разрешимые и неразрешимые теории. Теорема Гёделя о неполноте арифметики. Теорема Чёрча о неразрешимости исчисления предикатов.
18. Теория алгоритмов как наука. Задачи теории алгоритмов. Возникновение теории алгоритмов. Направления в теории алгоритмов. Дескриптивная и метрическая теория алгоритмов. Качественная и количественная теория алгоритмов.
19. Возникновение термина «алгоритм». Наивное определение понятия "алгоритм". Различные подходы к понятию «алгоритм». Свойства алгоритма. Формализация понятия "алгоритм".
20. Способы представления алгоритмов. Язык блок-схем для представления алгоритмов.
21. Теория рекурсивных функций. Рекурсивные функции. Базовые функции. Операторы суперпозиции, примитивной рекурсии и минимизации. Свойства операторов суперпозиции, примитивной рекурсии и минимизации (μ-операция). Примитивно-рекурсивные функции. Частично-рекурсивные функции. Свойства примитивно-рекурсивных функций. Примеры примитивно-рекурсивных функций. Относительная примитивная рекурсивность. Свойства относительной примитивной рекурсивности. Тезис Черча. Определение частично рекурсивных функций. Универсальная частично-рекурсивная функция. Примеры частично-рекурсивных функций. Общерекурсивные функции. Примеры общерекурсивных функций. Иерархия классов рекурсивных функций.
22. Три основных класса алгоритмических моделей. Эквивалентность математических моделей понятия "алгоритм". Эквивалентность формальных определений алгоритма.
23. Формализация понятия алгоритма. Понятие алгоритма и вычислимой функции. Невычислимые функции. Качественная и количественная теория алгоритмов. Понятие алгоритмической системы.
24. Формализация понятия алгоритма. Машина А. Тьюринга. Определение. Простейшие машины Тьюринга. Тезис Тьюринга. Основная гипотеза теории алгоритмов в форме Машины Тьюринга. Операции на машинах Тьюринга (операция композиции, операция ветвления, операция зацикливания) и их свойства. Базис элементарных машин Тьюринга. Универсальная машина Тьюринга. Недетерминированные машины Тьюринга.
25. Формализация понятия алгоритма. Машина А. Тьюринга. Функция, вычислимая по Тьюрингу. Функция, правильно-вычислимая по Тьюрингу. Доказательство существования функций, невычислимых по Тьюрингу. Пример невычислимой по Тьюрингу функции. Совпадение класса функций, правильно-вычислимых по Тьюрингу, и класса частично рекурсивных функций.

26. Формализация понятия алгоритма. Сверхтьюринговые вычисления (или гипервычисления). Машина Зенона. Машина Зенона и вычислимость.
27. Формализация понятия алгоритма. Определение машин Шенфилда и функций, вычислимых на ней. Макросы. Теорема об элиминации макросов. Теорема о совпадении классов функций, вычислимых на машинах Шенфилда и класса частично рекурсивных функций.
28. Формализация понятия алгоритма. Машина Э. Поста. Машина Поста-Успенского. Универсальная машина Поста.
29. Формализация понятия алгоритма. Нормальный алгоритм (алгорифм) Маркова. Нормальный алгорифм Маркова в алфавите и над алфавитом. Нормально-вычислимые функции. Примеры нормальных алгорифмов (тождественный нормальный алгорифм, нормальный алгорифм левого присоединения, нормальный алгорифм правого присоединения, нормальный алгорифм удвоения, некоторые арифметические алгорифмы). Основная гипотеза теории алгоритмов в форме Маркова. Эквивалентность определений алгоритма в виде машины Тьюринга и нормального алгоритма Маркова. Универсальный алгоритм Маркова.
30. Алгоритмически неразрешимые задачи. Понятие об алгоритмически разрешимых и неразрешимых проблемах. Теорема о неподвижной точке. Теорема Райса. Неразрешимость проблемы распознавания свойств функций по задающим их программам. Примеры алгоритмически неразрешимых проблем (проблема распознавания самоприменимости, проблема применимости).
31. Сложность алгоритмов и задач. Меры сложности алгоритмов. Понятие сложности алгоритмов и вычислений. Полиномиальная эквивалентность. Экспоненциальная сложность. Недетерминированные алгоритмы. Недетерминированная машина Тьюринга. Псевдополиномиальный алгоритм. Эффективные алгоритмы. Легко и трудно разрешимые задачи. Θ-нотация. Основные свойства.
32. Характеристики сложности алгоритма. Вычисление сложности алгоритмов для различных конструкций: «Следование», «Ветвление», «Цикл». Характеристики сложности алгоритма на примере Машины Э.Поста, на примере Машина А.Тьюринга.
33. Характеристики сложности алгоритма. Временная и ленточная сложности машины Тьюринга, вычисляющей заданную функцию. Теоремы о верхней границе сложности вычислений. Теорема об ускорении.
34. Сложность алгоритмов. Классы сложности алгоритмов. Иерархия по времени и иерархия по памяти. Классы сложности: P, NP, co-NP, NP-C, co-NP-C, UP, #P, #P-C, L, NL, NC, P-C, PSPACE, PSPACE-C, EXPTIME, NEXPTIME, EXPSPACE, 2-EXPTIME, PR, RE, Co-RE, RE-C, Co-RE-C, R, BQP, BPP, RP, ZPP, PP, PCP, IP, PH.
35. Классы задач P и NP. Проблема: равенство классов P и NP? Полиномиальная сводимость. NP–полные и NP–трудные языки и задачи. Примеры NP-полных задач, методы доказательства NP-полноты. AI-полная задача.
36. Методы построения алгоритмов.
37. Основы нечеткой логики, элементы алгоритмической логики.

Примерные практические задания на зачете

1. Записать высказывания в виде формул логики высказываний.
   a. всякое N, делящееся на 12 делится на 2, 4 и 6.
2. Построить таблицы истинности для формул
   a. $BC \to (\overline{A \vee B} \sim \overline{C})$
3. Доказать, что формулы являются тавтологиями

a. $((A \vee B)(A \vee \overline{B})) \sim A$

4. Доказать полноту (неполноту) систем булевых функций

a. $\{\sim, \oplus\}$

5. Получить СДНФ для формул, а затем перейти к СКНФ:

a. $(x \to y) \to (x \oplus z)$

6. Получить СКНФ, а затем перейти к СДНФ

a. $(x \vee y)(x \vee z) \vee xy$

7. Получить МДНФ для формул

a. $((x \oplus y) \sim z) \to x$

8. Проверить истинность соотношений тремя способами (используя определение логического следствия и пп. 3,4 теоремы 2).

$x \to (y \to z), x \to y \vDash x \to z$;

9. Пусть Φ, Ψ, X, Θ - формулы исчисления высказываний. Построить вывод формулы исчисления высказываний из данного множества гипотез. $\Phi \vdash \Psi \to (\Phi \wedge \Psi)$;

10. Выписать все подформулы данной формулы сигнатуры $\Sigma = \{+, \cdot, \leq, 0\}$ и определить свободные и связанные переменные формулы: $\forall x((x + y \leq x) \wedge \neg (x = 0))$;

11. Построить Машину Тьюринга T, вычисляющую следующую функцию.

$$\overline{sg}(x) = \begin{cases} 0, \text{если } x > 0, \\ 1, \text{если } x = 0; \end{cases}$$

12. Построить Машину Поста, которая выполняет сложение двух целых неотрицательных чисел.

13. Построить нормальный алгорифм Маркова, который добавляет две единицы к входному слову, состоящему из последовательности единиц.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

Основная литература:

1. Игошин В.И. Математическая логика и теория алгоритмов. М.: Просвещение. 2008. – 448с. [Электронный ресурс]: http://efremov-el.ru/wp-content/uploads/2019/05/%D0%98%D0%B3%D0%BE%D1%88%D0%B8%D0%BD-%D0%92.%D0%98.-%D0%9C%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F-%D0%BB%D0%BE%D0%B3%D0%B8%D0%BA%D0%B0-%D0%B8-%D1%82%D0%B5%D0%BE%D1%80%D0%B8%D1%8F-%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%D0%BE%D0%B2.pdf

7.2 Дополнительная литература

1. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / М., МЦНМО, 2003, 328 с

2. Ершов Ю.Л., Палютин Е.А. Математическая логика. – М.: Наука, 1979, 1987; СПб.: Лань, 2004, 2005, 2006.

3. Ершов Ю.Л., Палютин Е.А. Математическая логика. – М.: ФИЗМАТЛИТ, 2011.
4. Игошин В.И. Задачник-практикум по математической логики. М.: Просвещение.
5. Маховенко Е.Б. Теоретико-числовые методы в криптографии. М.:Гелиос АРБ,2006.
6. Ростовцев А.Г. Алгебраические основы криптографии. СПб.: Мир и семья, Интерлайн, 2000. — 354 с : илл.

7.3 Методические материалы

1. Теория алгоритмов [Электронный ресурс]: методические рекомендации для проведения лабораторных работ для студентов очной и заочной форм обучения направления 230700.62 «Прикладная информатика» / Министерство образования и науки Российской Федерации, Курганский государственный университет, Кафедра информационных технологий и методики преподавания информатики ; [сост.: Т.А. Никифорова]. - Электрон. текстовые дан. (тип файла: pdf ; размер: 990 Kb). - Курган: Издательство Курганского государственного университета, 2013. - 36 с.: рис. - Библиогр.: с. 36. по ссылке http://dspace.kgsu.ru/xmlui/handle/123456789/3535

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Черемушкин А.В. Вычисления в алгебре и теории чисел. – Загл. с титул. экрана. – Свободный доступ из сети Интернет. – Текстовый документ. www.cryptography.ru.
2. Теоретические основы информатики // Никифорова Т.А. – Свободный доступ из сети Интернет. – it.kgsu.ru/TI_4/oglav.html.

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, LibreOffice.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при выполнении заданий лабораторных работ: Windows XP, LibreOffice, программы, разработанные преподавателем.

10. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн.

Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1.

Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения.

Решение кафедры об используемых технологиях и системе оценивания достижений обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Переносной проектор BENQ PB6110 с экраном, локальная сеть компьютеров на базе Intel Core i3-2120 - 16 шт. с выходом в Internet, коммутатор 2-го уровня D-LINK DGS-101D/E1A

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Математическая логика и теория алгоритмов»

образовательной программы высшего образования –
программы специалитета
10.05.03 Информационная безопасность автоматизированных систем
Специализация: Безопасность открытых информационных систем
Форма обучения: очная

Трудоемкость дисциплины: 3 з.е. (108 академических часа).
Семестр: 5 (очная форма обучения).
Форма промежуточной аттестации: зачет.
Содержание дисциплины. Основные разделы.

Математическая логика. Логические высказывания. Алгебра логики. Логические функции. Минимизация логических функций в классе ДНФ. Предикаты. Формулы логики предикатов.

Приложение логики предикатов в теории практики информационной безопасности и основ искусственного интеллекта.

Теория алгоритмов как наука. Понятие ”алгоритм”. Свойства алгоритма. Формализация понятия алгоритма. Абстрактная машина А. Тьюринга. Абстрактная машина Э. Поста. Нормальные алгорифмы А.А. Маркова. Сложность алгоритма.