

УДК 94(5) (075.8)
ББК 22.12 я73
М 34

Печатается по решению
редакционно-издательского совета
Северо-Кавказского федерального
университета

Составители:

канд. физ.-мат. наук, доцент **А. Н. Макоха**,
канд. техн. наук, доцент **А. В. Шапошников**,
канд. техн. наук, доцент **В. В. Бережной**

М 34 **Математическая логика и теория алгоритмов:** учебное пособие / сост.: А.Н. Макоха, А.В. Шапошников, В.В. Бережной. – Ставрополь: Изд-во СКФУ, 2017. – 418 с.

Пособие представляет курс лекций, освещающий наиболее важные разделы математической логики и теории алгоритмов; в нем рассматриваются элементы теории множеств, аксиоматическое построение исчисления высказываний, исчисления предикатов, теорий первого порядка и их приложения к некоторым системам искусственного интеллекта; излагаются основные проблемы аксиоматического метода, уточнение интуитивного понятия алгоритма на языке частично рекурсивных функций и машин Тьюринга. Изложение материала сопровождается содержательными примерами, приводятся вопросы и упражнения для самопроверки.

Предназначено для студентов математических и IT-специальностей; будет полезно преподавателям, ведущим курс математической логики и теории алгоритмов.

УДК 94(5) (075.8)
ББК 22.12 я73

Рецензенты:

канд. техн. наук, доцент **Д. Н. Резеньков** (СтГАУ),
канд. техн. наук, доцент, доцент **С. В. Аникуев** (СтГАУ)

© ФГАОУ ВО «Северо-Кавказский
федеральный университет», 2017

ВЕДЕНИЕ

Главным содержанием лекционного курса дисциплины «Математическая логика и теория алгоритмов» является формирования у студентов фундаментальных знаний в области основ построения математических теорий, а также построения и анализа алгоритмов.

Основными *задачами освоения дисциплины* являются:

- формирование научного мировоззрения, понимания широты и универсальности методов математической логики, умения применять эти методы в решении прикладных задач;
- воспитание математической культуры, которая предполагает четкое осознание необходимости и важности математической подготовки для специалиста в области компьютерной безопасности;
- ознакомление с основными объектами математической логики, а также их приложениями для решения различных задач, требующих применения вычислительных средств;
- ознакомление с основами теории алгоритмов и их приложениями к задачам математической кибернетики;
- овладение современным математическим аппаратом для дальнейшего использования при решении теоретических и прикладных задач в области защиты информации.

Освоение данной дисциплины позволит будущему специалисту в области компьютерной безопасности полноценно осуществлять свою профессиональную деятельность, в частности, обладать следующими **профессиональными и общекультурными компетенциями**:

Общекультурные компетенции (ОК)

1. Способность анализировать социально значимые явления и процессы, в том числе политического и экономического характера, мировоззренческие и философские проблемы, применять основные положения и методы гуманитарных, социальных и экономических наук при решении социальных и профессиональных задач (ОК-3).

Профессиональные компетенции (ПК)

2. Способность понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации (ПК-3).

3. Способность работать с программными средствами прикладного, системного и специального назначения (ПК-8).

4. Способность разрабатывать математические модели безопасности защищаемых компьютерных систем (ПК-18).

Материал предлагаемого пособия ориентирован на студентов математических и IT-специальностей. Главная цель, которую преследовали авторы при написании пособия, состоит в ознакомлении студентов с концептуальными положениями теории алгоритмов и математической логики, выросшей из формальной логики, с приложениями формальных исчислений к построению содержательных теорий первого порядка и систем искусственного интеллекта.

ОГЛАВЛЕНИЕ

Ведение	3
 ГЛАВА I. ИНФОРМАЦИОННО-ЛОГИЧЕСКИЕ СТРУКТУРЫ	
1. ЭЛЕМЕНТАРНОЕ ВВЕДЕНИЕ В ТЕОРИЮ МНОЖЕСТВ	5
1.1. Теоретико-множественная символика и терминология.....	7
1.2. Операции над множествами и их основные свойства.....	15
1.3. Декартово произведение множеств и отношения на множествах.....	20
1.4. Элементы теории отображений	25
1.5. Отношение эквивалентности и разбиение множества на классы..	27
1.6. Отношения порядка	32
1.7. Базовые алгебраические системы	36
Вопросы и упражнения для самопроверки	43
 2. АЛГЕБРА ВЫСКАЗЫВАНИЙ И ЛОГИКА ПРЕДИКАТОВ	50
2.1. Алгебраические операции над высказываниями и их свойства ..	50
2.2. Формулы и функции алгебры логики. Закон двойственности	55
2.3. Совершенные дизъюнктивные и конъюнктивные нормальные формы булевых функций	61
2.4. Полнота и замкнутость системы булевых функций. Представление о классах Поста	65
2.5. Логика предикатов	69
Вопросы и упражнения для самопроверки	76
 3. ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ.....	87
3.1. Алфавит, формулы и подформулы исчисления высказываний ..	88
3.2. Аксиомы исчисления высказываний	89
3.3. Основные правила вывода	90
3.4. Определение доказуемой (выводимой) формулы	92
3.5. Производные правила вывода. Теорема дедукции	94
3.6. Связь алгебры высказываний с исчислением высказываний	100
Вопросы и упражнения для самопроверки	109
 4. ИСЧИСЛЕНИЕ ПРЕДИКАТОВ	113
4.1. Определение формулы исчисления предикатов	113
4.2. Аксиомы исчисления предикатов и основные правила вывода... 116	116
4.3. Общезначимость и выполнимость формул исчисления предикатов	119
4.4. Предваренная, скулемовская и клаузная формы представления формул исчисления предикатов	121
Вопросы и упражнения для самопроверки	126

5. ОСНОВНЫЕ ПОНЯТИЯ АКСИОМАТИЧЕСКИХ ТЕОРИЙ ПЕРВОГО ПОРЯДКА	129
5.1. Формальные аксиоматические теории	131
5.2. Логические и специальные аксиомы	133
5.3. Правила вывода и понятие доказательства в теории первого порядка	134
5.4. Понятия интерпретации и модели теории. Изоморфизм интерпретаций	137
5.5. Примеры аксиоматических теорий первого порядка со специальными аксиомами	140
Вопросы и упражнения для самопроверки	150
6. ПРОБЛЕМЫ АКСИОМАТИЧЕСКОГО ПОСТРОЕНИЯ ТЕОРИЙ ПЕРВОГО ПОРЯДКА	156
6.1. Проблема непротиворечивости	156
6.2. Проблема независимости системы аксиом	157
6.3. Формализуемость и разрешимость теории	158
6.4. Категоричность теории	159
6.5. Проблема полноты теории	159
ЛИТЕРАТУРА К ГЛАВЕ I	162

ГЛАВА II. НЕТРАДИЦИОННЫЕ ЛОГИКИ

1. ОСНОВНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ В ОБЛАСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА	164
1.1 Естественный и искусственный интеллект	164
1.2. Некоторые философские аспекты проблем искусственного интеллекта	167
1.3. Примеры систем искусственного интеллекта	
Вопросы и упражнения для самопроверки	169
2. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ АВТОМАТИЗАЦИИ ДОКАЗАТЕЛЬСТВ.....	178
2.1. Постановка задачи автоматического доказательства теорем.....	179
2.2. Унификация.....	183
2.3. Метод резолюций.....	191
2.4. Алгоритм поиска опровержения методом резолюций.....	203
2.5. Доказательство истинности логических клауз методом резолюций.....	206
Вопросы и упражнения для самопроверки	213

3. ОСНОВНЫЕ ПРИНЦИПЫ ЛОГИЧЕСКОГО ПРОГРАММИРОВАНИЯ	218
3.1. Использование формализмов логики для алгоритмических вычислений. Факты, правила, запросы	220
3.2. Общие правила выполнения запросов логическими программами	223
3.3. Методика составления логических программ	226
Вопросы и упражнения для самопроверки	240
4. СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, ОСНОВАННЫЕ НА ЗНАНИЯХ	244
4.1. Представление и использование нечетких знаний	245
4.2. Нечеткая, вероятностная и монотонная логики	248
4.3. Нечеткие множества и нечеткие выводы	250
4.4. Многозначная логика	253
4.5. Модальные логики	258
4.6. Продукционные системы	273
4.7. О механизмах вывода в экспертных системах	289
Вопросы и упражнения для самопроверки	293
ЛИТЕРАТУРА К ГЛАВЕ II	296

ГЛАВА III. ТЕОРИЯ АЛГОРИТМОВ

1. УТОЧНЕНИЕ ПОНЯТИЯ АЛГОРИТМА НА ОСНОВЕ ЧАСТИЧНО РЕКУРСИВНЫХ ФУНКЦИЙ	298
1.1. Интуитивное понятие алгоритма. Общие свойства алгоритмов	299
1.2. Эффективно вычислимые и примитивно рекурсивные функции	304
1.3. Оператор минимизации и частично рекурсивные функции	311
Тезис Черча	311
Вопросы и упражнения для самопроверки	319
2. УТОЧНЕНИЕ ПОНЯТИЯ АЛГОРИТМА НА ОСНОВЕ МАШИН ТЬЮРИНГА	325
2.1. Модель одноленточной машины Тьюринга	326
2.2. Композиция, итерация и разветвление машин Тьюринга	333
2.3. Методологическое значение моделей машин Тьюринга	337
Вопросы и упражнения для самопроверки	339
3. НОРМАЛЬНЫЕ АЛГОРИТМЫ МАРКОВА	354
3.1. Основные понятия	355

3.2. Композиция, итерация и разветвление нормальных алгоритмов. Эквивалентность тезиса Черча и принципа нормализации Маркова.....	358
Вопросы и упражнения для самопроверки	365
4. АНАЛИЗ СЛОЖНОСТИ АЛГОРИТМОВ	368
4.1. Подходы к оценке сложности алгоритмов. Асимптотика	368
4.2. Меры и оценки сложности	377
4.3. Анализ сложности генерирования перестановок	381
4.4. Класс задач, детерминировано решаемых с полиномиальной Сложностью	385
4.5. NP-полные и NP-трудные задачи	395
4.6. Понятие алгоритмически неразрешимых проблем	398
4.7. Примеры алгоритмически неразрешимых проблем	401
Вопросы и упражнения для самопроверки	406
ЛИТЕРАТУРА К ГЛАВЕ III	411
ЗАКЛЮЧЕНИЕ	412