

УДК 519.854(075.8)

ББК 22.176я73

К43

Электронные версии книг
на сайте www.prospekt.org

Авторы:

Кириллов И. А., кандидат технических наук, доцент, заслуженный профессор Московского государственного лингвистического университета;

Шептунов М. В., кандидат технических наук, доцент.

Рецензент:

Викторова Н. Б., кандидат физико-математических наук, доцент кафедры «Фундаментальная и прикладная математика» Российского государственного гуманитарного университета.

Кириллов И. А., Шептунов М. В.

К43 Дискретная математика и ее специальные разделы : учебное пособие. — Москва : Проспект, 2022. — 264 с.

ISBN 978-5-392-36007-9

Цель данного учебного пособия — изложение не очень большого по объему, но достаточного для понимания материала по дискретной математике и ее специальных разделов для студентов первого и/или (преимущественно) второго курсов университета.

Издание подготовлено на основе федеральных государственных образовательных стандартов (ФГОС) в соответствии с рабочими (учебными) программами Московского государственного лингвистического университета для направления подготовки бакалавриата «Информационная безопасность» и Финансового университета для направлений подготовки бакалавриата «Информационная безопасность», «Прикладная информатика», «Бизнес-информатика» (профиль «ИТ-менеджмент в бизнесе»).

Труд авторов распределен следующим образом: часть I создана И. А. Кирилловым, часть II, материал которой преподавался в Российском государственном гуманитарном университете (РГУ) и в Московском гуманитарном университете (МосГУ), — М. В. Шептуновым, предисловие и заключение написаны авторами совместно.

УДК 519.854(075.8)

ББК 22.176я73

Учебное издание

**КИРИЛЛОВ ИГОРЬ АЛЕКСЕЕВИЧ,
ШЕПТУНОВ МАКСИМ ВАЛЕРЬЕВИЧ
ДИСКРЕТНАЯ МАТЕМАТИКА
И ЕЕ СПЕЦИАЛЬНЫЕ РАЗДЕЛЫ
Учебное пособие**

Подписано в печать 20.07.2022. Формат 60×90 ¹/₁₆.

Печать цифровая. Печ. л. 16,5. Тираж 1000 (2-й завод 100) экз. Заказ №

ООО «Проспект»

111020, г. Москва, ул. Боровая, д. 7, стр. 4.

ISBN 978-5-392-36007-9

© Кириллов И. А., Шептунов М. В., 2021
© ООО «Проспект», 2021

СОДЕРЖАНИЕ

Предисловие.....	3
------------------	---

ЧАСТЬ 1 (авт. — Кириллов И. А.)

Глава 1. Конечные множества и комбинаторика	5
1.1. Понятие множества, способы задания множеств	5
1.2. Подмножества	6
1.3. Операции над множествами.....	7
1.4. Бинарные отношения элементов множества.....	10
1.5. Отображения множеств	11
Глава 2. Основы комбинаторного анализа.....	14
2.1. Формула включений-исключений	16
2.2. Правило произведения. Размещения и перестановки с повторениями	19
2.3. Количество подмножеств данного конечного множества.....	21
2.4. Мультимножества. Сочетания с повторениями	22
2.5. Размещение частиц по ячейкам.....	24
2.6. Числа Стирлинга и числа Белла	29
Глава 3. Группы подстановок.....	33
3.1. Разложение подстановок в произведение независимых циклов.....	34
3.2. Представление подстановок в виде произведения транспозиций	37
3.3. Знакопеременная группа подстановок степени n	38
Глава 4. Упражнения и задачи.....	40
Глава 5. Конечные кольца и поля	50
5.1. Построение конечных колец и полей классов вычетов	50
5.2. Функции и уравнения в конечных кольцах и полях.....	52

Глава 6. Применение конечных односторонних функций в современной криптографии.....	58
6.1. Протокол открытого распределения ключей Диффи и Хеллмана	58
6.2. Асимметричный шифр RSA	60
6.3. Электронная цифровая подпись	69
6.4. Задачи и упражнения	70
Глава 7. Элементы теории кодирования.....	72
7.1. Линейные пространства над конечными полями.....	72
7.2. Понятие блочных кодов и их корректирующие свойства.....	74
7.3. Линейные блочные коды.....	78
7.4. Процессы кодирования и декодирования линейных блочных кодов.....	80
7.5. Коды Хэмминга	82
ЧАСТЬ 2 (авт. — Шептунов М. В.)	
Глава 8. Некоторые особенности выбора помехоустойчивого кода при проектировании устройств защиты от ошибок (УЗО).....	88
8.1. О некоторых особенностях помехоустойчивых кодов в ракурсе устройств защиты от ошибок (УЗО)	88
8.2. О матрицах Адамара и коде Адамара	93
Глава 9. Производящие функции и рекуррентные последовательности.....	95
9.1. Основные понятия	95
9.2. Понятия о линейных операциях для производящих функций и о свертке для производящих функций.....	100
9.3. О переходе от бесконечных сумм к конечным с помощью асимптотических формул и некоторых сложностных оценках задач.....	103
9.4. Элементы целочисленного программирования и производящие функции	106
9.5. Рекуррентные соотношения и конечные суммы: сумма первых n натуральных чисел.....	116
9.6. Об отношении эквивалентности и производящей функции запаса классов эквивалентности	117

Глава 10. Элементы теории конечных автоматов и возможности их применения в криптографии и информационной безопасности; автоматная модель системы защиты GM	123
10.1. Основные понятия и обозначения конечных автоматов.....	123
10.2. Простые примеры автоматов: сканирующего, декодирующего и автомата, представляющего бесконечное множество (последовательность).....	130
10.3. О диаграммах состояний и способах задания автоматов в ракурсе распознавания множеств конечными автоматами.....	135
10.4. Запоминающие функции логических переключательных узлов и релейно-контактных схем (РКС) и конечные автоматы.....	154
10.5. Автоматная модель защиты GM.....	168
Глава 11. Рекурсия и рекурсивные функции; доказательство рекурсивности функций с помощью метода (принципа) математической индукции	176
11.1. Рекурсия и рекурсивные функции.....	176
11.2. Доказательство рекурсивности функций с помощью метода (принципа) математической индукции.....	183
Глава 12. Шифрование на основе маршрутов Гамильтона	189
12.1. Сущность метода шифрования на основе маршрутов Гамильтона.....	189
12.2. Некоторые примеры шифрования.....	191
Глава 13. Расширенный алгоритм Евклида и его применение в криптографических целях	195
13.1. Модулярная арифметика и основные способы отыскания обратных величин.....	195
13.2. Некоторые примеры отыскания обратных величин с помощью расширенного алгоритма Евклида.....	197
Глава 14. Основы теории графов	202
14.1. Основные понятия теории графов.....	202
14.2. Задача о кенигсберских мостах; эйлеровы и гамильтоновы циклы.....	209
14.3. Деревья.....	211

14.4. Диаметр, радиус и центр графа	214
14.5. Специальные маршруты в графах	215
14.6. Планарные графы.....	218
14.7. Обходы деревьев и стратегии поиска в глубину и ширину	220
14.8. Матрицы смежности и инцидентий графа	222
Глава 15. Линейные рекуррентные последовательности	
над конечными полями	233
15.1. Вводные определения и теоремы	233
15.2. Регистры сдвига (сдвиговые регистры).....	241
15.3. Основные утверждения о максимальных линейных рекуррентных последовательностях как псевдослучайных последовательностях	250
Заключение.....	254