

УДК 004
ББК 32.97
М15

М15 Дж. Маккормик

Девять алгоритмов, которые изменили мир. Остроумные идеи, лежащие в основе современных компьютеров / Пер. с англ. Слинкин А. А. – М.: ДМК Пресс, 2016. – 236 с.: ил.

ISBN 978-5-97060-204-1

Ежедневно мы используем впечатляющие технологические достижения, даже не задумываясь об этом. Мы передаем по сети гигабайты информации, просматриваем тысячи документов в поисках необходимого, совершаем покупки в интернет-магазинах. Мы архивируем объемные материалы, так чтобы их можно было отправить по электронной почте, и пользуемся искусственным интеллектом компьютеров, которые автоматически исправляют опечатки в тексте, ретушируют фотографии и делают за нас многое другое...

Все это при нынешнем уровне развития технологий воспринимается как должное. Но ведь такие «чудеса» были бы невозможны без величайших идей информатики, родившихся в XX веке!

Эта книга – о том, как эти идеи зародились и как воплощались в жизнь.

Издание рассчитано на широкую аудиторию. Предварительного знакомства с информатикой от читателей не требуется.

УДК 004
 ББК 32.97

Original English language edition published by Princeton University Press, 41 William Street, Princeton, New Jersey 08540. In the United Kingdom: Princeton University Press, 6 Oxford Street, Woodstock, Oxfordshire OX20 1TW Copyright © 2012 by Princeton University Press. Russian-language edition copyright (c) 2013 by ДМК Press. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но, поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 978-0-691-15819-8 (англ.)
 ISBN 978-5-97060-204-1 (рус.)

© 2012 by Princeton University Press
 © Оформление, перевод на русский язык
 ДМК Пресс, 2014



ОГЛАВЛЕНИЕ

Глава 1. Введение: необычные идеи, каждодневно используемые в компьютерах.....	11
Алгоритмы – чародейство услужливого джинна.....	13
Какой алгоритм считать великим?	14
А какое нам, собственно, дело до великих алгоритмов?	19
Глава 2. Индексирование в поисковых системах: поиск иголки в самом большом в мире стоге сена	21
Сопоставление и ранжирование.....	22
AltaVista: первый алгоритм сопоставления масштаба веб.....	23
Старое доброе индексирование.....	24
Трюк с позициями слов	26
Ранжирование и близость	29
Трюк с метасловами	31
Трюки индексирования и сопоставления – это еще не все.....	35
Глава 3. PageRank: технология, породившая Google	37
Трюк с гиперссылками	38
Трюк с авторитетностью	40
Трюк со случайным посетителем	42
Алгоритм PageRank на практике.....	48
Глава 4. Криптография с открытым ключом: отправка секретов почтовой открыткой	51
Шифрование с помощью общего секрета	53
Открытая выработка общего секрета	56
Трюк со смешиванием красок.....	56
Числа вместо красок	61
Смешивание красок в реальной жизни	64
Криптография с открытым ключом на практике	69
Глава 5. Коды, исправляющие ошибки: ошибки, которые исправляются сами собой.....	73
Нужда в обнаружении и исправлении ошибок	74
Трюк с повторением	75
Трюк с избыточностью.....	78
Трюк с контрольной суммой	81

Трюк с указкой.....	87
Обнаружение и исправление ошибок в реальном мире	91
Глава 6. Распознавание образов: обучение на опыте	94
В чем состоит задача?.....	95
Трюк с ближайшими соседями	98
Различные виды «ближайших» соседей	101
Трюк с двадцатью вопросами: деревья решений	103
Нейронные сети	107
Биологические нейронные сети.....	108
Нейронная сеть для задачи о зонтике	109
Нейронная сеть для задачи о солнечных очках.....	111
Добавление взвешенных сигналов	113
Настройка нейронной сети посредством обучения.....	114
Использование сети для задачи о солнечных очках	117
Распознавание образов: прошлое, настоящее и будущее	118
Глава 7. Сжатие данных: кое-что задаром.....	121
Сжатие без потери информации: бесплатный сыр бывает	
не только в мышеловке.....	122
Трюк «то же, что и раньше»	124
Трюк «более короткий символ»	126
Резюме: откуда берется бесплатный сыр?.....	129
Сжатие с потерей информации: не бесплатный сыр,	
но отличная сделка.....	131
Трюк с пропуском	132
Истоки алгоритмов сжатия	137
Глава 8. Базы данных: в поисках непротиворечивости	139
Транзакции и трюк со списком дел	142
Трюк со списком дел.....	146
Атомарность в большом и в малом	148
Трюк «подготовить и зафиксировать» для реплицированных	
баз данных	149
Реплицированные базы данных	149
Откат транзакций	151
Трюк «подготовить и зафиксировать»	154
Реляционные базы данных и трюк с виртуальной таблицей	158
Ключи	160
Трюк с виртуальной таблицей	162
Реляционные базы данных	164
Базы данных с точки зрения человека	165
Глава 9. Цифровые подписи: кто на самом деле	
написал эту программу?	167
Для чего в действительности применяются цифровые	
подписи?.....	167

Рукописные подписи	169
Подписание с помощью замка	171
Подписание с помощью перемножающего замка	174
Подписание степенным замком	181
Безопасность RSA	185
Связь между RSA и разложением на множители	186
Связь между RSA и квантовыми компьютерами	188
Цифровые подписи на практике	189
Парадокс разрешен	191
Глава 10. Что можно вычислить?	192
Ошибки, сбои и надежность программ	193
Доказательство ложности чего-либо	194
Программы, анализирующие другие программы	196
Некоторые программы невозможны	200
Простые программы да–нет	201
AlwaysYes.exe: программа да–нет, анализирующая другие программы	202
YesOnSelf.exe: упрощенный вариант AlwaysYes.exe	204
AntiYesOnSelf.exe: противоположность YesOnSelf.exe	206
Невозможность обнаружения сбоев	210
Проблема остановки и неразрешимость	213
Что следует из невозможности некоторых программ?	214
Неразрешимость и использование компьютеров	214
Неразрешимость и мозг	215
Глава 11. Послесловие: еще один услужливый джинн?	218
О некоторых потенциально великих алгоритмах	220
Могут ли великие алгоритмы уйти в тень?	221
Чему мы научились?	222
Конец пути	223
Благодарности	225
Источники и литература для дальнейшего чтения	226
Предметный указатель	230