

Федеральное государственное автономное  
образовательное  
учреждение высшего образования  
«Московский физико-технический институт  
(государственный университет)»  
Центр развития ИТ-образования

## **Алгоритмы и модели вычисления**

*Дмитрий Голубенко  
Алексей Крошин  
Эдуард Горбунов*

Москва, 2019

# Оглавление

Предисловие	3
<b>Часть 1. Введение</b>	<b>5</b>
Асимптотические оценки. Метод Акра-Баззи	10
Линейные рекурренты	16
Вероятность: введение	19
<b>Часть 2. Сортировки и медианы</b>	<b>25</b>
Сортировки	26
Поиск $k$ -ой статистики	39
<b>Часть 3. Алгебра и теория чисел</b>	<b>41</b>
Полиномиальные арифметические алгоритмы	50
Полиномиальность алгоритма Евклида	51
Быстрое умножение чисел и матриц	55
Быстрое возведение в степень	57
Полиномиальность алгоритма Гаусса	59
Простейшие криптографические протоколы	62
Дискретное преобразование Фурье	65
Быстрое перемножение многочленов	70
Решето Эратосфена	75
Вероятностные тесты на простоту	75
Алгоритм АКС	82
Взятие квадратного корня по модулю	87
Дискретное логарифмирование	88
Факторизация целых чисел	89
Факторизация многочленов. Алгоритм Кантора-Цассенхауса	96
Алгоритм Берлекемпа	100

Теоретико-групповые алгоритмы	101
Задача принадлежности	104
Фильтр Джеррама	109
Задача GRAPH-ISO и теоретико-групповые алгоритмы	110
<b>Часть 4. Графы и алгоритмы</b>	<b>115</b>
Depth-first search	117
Поиск точек сочленения	121
Компоненты сильной связности	125
Breadth-first search	130
Поиск кратчайших путей	133
Минимальные остовные деревья	143
Алгоритмы Прима, Крускала и Борувки	144
Потоки и сети	151
Метод Форда-Фалкерсона. Алгоритм Эдмондса-Карпа	154
Метод проталкивания предпотока. Алгоритм Тарьяна-Голдберга	161
0-1 потоки	166
Вершинная и реберная связности	169
<b>Часть 5. Элементы теории сложности</b>	<b>177</b>
Вероятностные алгоритмы: определения	187
Классы $P$ , $NP$ и $co - NP$	189
$PRIMES \subset NP \cap co - NP$	195
Системы линейных неравенств	199
Полиномиальная сводимость	203
<b>Часть 6. Избранные задачи и решения</b>	<b>219</b>
<b>Библиография</b>	<b>235</b>