

УДК 519.72:003.26(075.8)

ББК 32.811+16.84 я73

М74

*Печатается по решению кафедры алгебры и дискретной математики  
Южного федерального университета (протокол № 7 от 7 июня 2022 г.)*

**Рецензенты:**

доцент кафедры «Алгебра и дискретная математика» ИММиКН ЮФУ  
кандидат технических наук *В. В. Мкртчян*

заведующий кафедрой «Программное обеспечение вычислительной техники  
и автоматизированных систем» Донского государственного технического  
университета, кандидат технических наук, доцент *В. В. Долгов*

**М74** **Могилевская, Н. С.** **Some lectures on information theory and cryptography:** учебное пособие / Н. С. Могилевская ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2022. – 130 с.

ISBN 978-5-9275-4188-1

Учебное пособие разработано для студентов бакалавриата, обучающихся по направлению 02.03.02 Фундаментальная информатика и информационные технологии. Это пособие рассматривает часть тем, входящих в учебную программу англоязычного курса «Mathematical Foundations of Information Security». Пособие знакомит читателя с вопросами количественного измерения информации, сжатия данных, помехоустойчивого кодирования данных и обеспечения конфиденциальности данных. Теоретический материал полностью соответствует известным публикациям по изучаемым вопросам. Отличительной особенностью пособия является большое количество практических примеров, иллюстрирующих теоретические положения, а также большой набор задач для самоконтроля студентов.

УДК 519.72:003.26(075.8)

ББК 32.811+16.84 я73

ISBN 978-5-9275-4188-1

© Южный федеральный университет, 2022

© Могилевская Н. С., 2022

© Оформление. Макет. Издательство Южного  
федерального университета, 2022

## ОГЛАВЛЕНИЕ

---

<b>INTRODUCTION</b> . . . . .	5
<b>1. INFORMATION, ENTROPY</b> . . . . .	7
1.1. Information is Nonmaterial Object . . . . .	7
1.2. Discrete Information Source. . . . .	8
1.3. Information Content and Entropy . . . . .	10
1.4. Axiomatic Definition of Entropy. . . . .	12
1.5. Cheat Sheet for Problem Solving. . . . .	17
1.6. Examples of Problems with Solutions . . . . .	20
1.7. Brief Summary . . . . .	23
1.8. Practical Tasks on the Topic «Information, Entropy» . . . . .	23
1.9. Special Task . . . . .	26
1.10. An Approximate Version of a Test for the Section . . . . .	26
<b>2. DATA COMPRESSION</b> . . . . .	31
2.1. Basic Definitions . . . . .	31
2.2. Tree Representation of Prefix Code. . . . .	38
2.3. Kraft's Inequality and McMillan's Assertion. . . . .	42
2.4. Source Encoding Theorem . . . . .	44
2.5. Types of Compression Algorithms . . . . .	46
2.6. Huffman Coding . . . . .	47
2.7. Discussion of the Huffman Algorithm . . . . .	55
2.8. Lempel-Ziv Algorithms . . . . .	58
2.8.1. LZ78 Algorithm . . . . .	59
2.8.2. LZ77 Algorithm . . . . .	61
2.8.3. Example of Lempel-Ziv Algorithm with Restriction on Dictionary and Sliding Window Lengths . . . . .	64
2.9. Brief Summary . . . . .	66
2.10. Practical Tasks on the Topic «Data Compression» . . . . .	66
2.11. Individual Tasks. . . . .	72
2.12. An Approximate Version of a Test for the Section . . . . .	74
<b>3. ALGEBRAIC CODING THEORY</b> . . . . .	78
3.1. Code Classification . . . . .	81
3.1.1. Block and Convolutional Codes . . . . .	81
3.1.2. q-ary Codes. . . . .	84
3.1.3. Error-Detecting and Error-Correcting Codes . . . . .	84
3.1.4. Linear and Non-linear Codes . . . . .	84
3.2. Geometric Representation of Block Codes. . . . .	84
3.3. Some Estimations for Codes . . . . .	90

---

3.4. Linear Codes . . . . .	91
3.4.1. Generator and Parity-Check Matrices . . . . .	91
3.4.2. Syndrome. . . . .	97
3.4.3. Equivalent Codes. . . . .	99
3.5. Decoders . . . . .	102
3.5.1. Minimum Distance Decoding . . . . .	103
3.5.2. Syndrome Decoding . . . . .	105
3.6. Hamming Code. . . . .	108
3.6.1. Encoding Algorithm. . . . .	109
3.6.2. Decoding Algorithm. . . . .	110
3.7. Brief Summary . . . . .	112
3.8. Practical Tasks on the Topic «Algebraic Coding Theory» . . .	113
3.9. Individual Tasks. . . . .	117
<b>4. CRYPTOGRAPHY . . . . .</b>	<b>120</b>
4.1. The Classic Problem of Cryptography . . . . .	120
4.2. Some Historical Ciphers . . . . .	122
4.2.1. Caesar Cipher . . . . .	122
4.2.2. Affine Cipher . . . . .	123
4.2.3. Discussion of Cipher Strength . . . . .	124
4.3. Brief Summary . . . . .	125
4.4. Practical Tasks on the Topic «Cryptography» . . . . .	125
4.5. Individual Tasks. . . . .	126
<b>BIBLIOGRAPHY . . . . .</b>	<b>127</b>
<b>ANSWERS . . . . .</b>	<b>128</b>