Міністерство освіти і науки України
Львівський національний університет імені Івана Франка

Основи теорії інформації та кодування

Навчальний посібник

Львів
2023

УДК 519.7:004(075.8)
О 75

Автори:
І. А. Прокопишин, Р. Є. Рикалюк, В. Ф. Чекурін, К. А. Червінка

Рецензенти:
д-р техн. наук, проф. В. Б. Дудикевич
(Національний університет "Львівська політехніка", м. Львів);
д-р фіз.-мат. наук, проф. Т. С. Нагірний
(Інститут механічної інженерії, Зеленогурський Університет,
м. Зелена Гура, Польща);
д-р техн. наук, проф. Р. М. Пасічник
(Західноукраїнський національний університет, м. Тернопіль)

Рекомендовано до друку Вченою радою
Львівського національного університету імені Івана Франка
(протокол № 49/6 від 29.06.2023 року)

О 75 **Основи теорії інформації та кодування** : навч. посібник / [І. А. Прокопишин, Р. Є. Рикалюк, В. Ф. Чекурін, К. А. Червінка]. – Електрон. вид. – Львів : ЛНУ ім. Івана Франка, 2023. – 156 с.

ISBN 978-617-10-0820-5 (електрон. вид.)

Розглянуто головні поняття теорії інформації, ефективного кодування даних, моделювання та кодування графічних зображень, звуку та відео, кодування з захистом від завад та шифрування, а також теоретичні основи побудови електронних схем комп’ютерів.

Для студентів математичних та інших спеціальностей, які вивчають комп’ютерні науки.

УДК 519.7:004(075.8)

ISBN 978-617-10-0820-5 (електрон. вид.)

ЗМІСТ

СПИСОК АБРЕВІАТУР

АІС – автоматизована інформаційна система
АЦП – аналого-цифровий перетворювач
ДКП – дискретне косинус-перетворення
ЕОМ – електронно-обчислювальна машина
ЕПТ – електронно-променева трубка
ІС – інформаційна система
МК – матриця квантування
МКО – міжнародна комісія з освітленості
НСД – найбільший спільний дільник
ОП – оперативна пам’ять
ОС – операційна система
ТВЧ – телебачення високої чіткості
ЦАП – цифро-аналоговий перетворювач
AAC – *Advanced Audio Coding*
AC-3 – *family of Audio Compression technologies developed by Dolby Laboratories*
AES – *Advanced Encryption Standard*
ANSI – *American National Standard Institute*
ASCII – *American Standard Code for Information Interchange*
AT&T – *American Telephone and Telegraph*
AVC – *Advanced Video Coding – video compression standard*
BD – *Blu-ray Disc*
BMP – *Bitmap Picture – bitmap image storage format developed by Microsoft*
CCITT – *Comité Consultatif International Téléphonique et Télégraphique*
CD – *Compact Disc*
CD-DA – *Compact Disc Digital Audio – standard for recording sound on CD*
CD-R – *Compact Disc-Recordable*
CD-RW – *Compact Disc-ReWritable*
CIE – *Commission Internationale de l´Eclairage*
CIELAB – *color space developed by CIE in 1976 based on CIE XYZ*
CIE XYZ – *color space created by the CIE in 1931*
CIF – *Common Interchange Format – video standard with scan of 352x288 pixels*
CMM – *Color Matching Module*

CMS – *Color Management System*

CMY – *subtractive color model, in which the main colors are Cyan, Magenta and Yellow*

CMYK – *subtractive color model, in which the main colors are Cyan, Magenta, Yellow and blacK*

DES – *Data Encryption Standard – symmetric block encryption algorithm*

DjVu – *lossy image compression technology and the corresponding format*

DVD – *Digital Video Disc*

ENIAC – *Electronic Numerical Integrator and Computer*

EPS – *Encapsulated PostScript – simplified version of PostScript*

FPX – *FlashPix – bitmapped computer graphics file format*

GIF – *Graphics Interchange Format – 8-bit bitmap graphics format*

HDTV – *High-Definition Television – high-definition television standard with scan of 1920x1080 pixels*

Full HD – *see HDTV*

HSB – *color intuitive model based on three color characteristics: Hue, Saturation, and Brightness*

HSV – *see HSB*

ICC – *International Color Consortium*

ISO – *International Organization for Standardization*

JPEG – *name of full-color image compression algorithm and corresponding format, developed by the Joint Photographic Expert Group*

LZ – *prefix for family of data compression algorithms (LZ77, LZ78, LZW etc.) – the initials of Abraham Lempel and Jacob Ziv*

MD – *prefix for family of Message-Digest Algorithms (MD1–MD5 etc.)*

MIDI – *Musical Instrument Digital Interface*

MP3 – *coding forma for digital audio*

MPEG – *Moving Pictures Experts Group – line of digital television standards*

NTSC – *National Television System Committee – standard for analog television broadcast*

PAL – *Phase Alternating Line – color encoding system for analogue television*

PCM – *Pulse Code Modulation*

PDF – *Portable Document Format*

PGP – *Pretty Good Privacy – encryption program*

PKE – *Public Key Encryption*

PNG – *Portable Networks Graphic – raster-graphics file format*

PS – *PostScript – page description language and the corresponding format*

QCIF – *Quartet Common Interchange Format – video standard with scan of 176x144 pixel*

RA – *Real Audio – audio data format that uses several audio codecs*

RGB – *additive color model, in which the main colors are Red, Green and Blue*

RIFF – *Resource Interchange File Format – standard for storing any data structures*

RLE – *Run Length Encoding*

RSA – *Rivest–Shamir–Adleman – public-key cryptosystem developed by Ron Rivest, Adi Shamir and Leonard Adleman*

SECAM – *Séquentiel de couleur à mémoire – analog color television system*

SHA – *prefix for family of Secure Hash Algorithm standards, SHA-1– SHA-3*

SI – *Système International d'Unités*

TIFF – *Tagged Image File Format – format for storing raster graphic images*

UHDTV – *Ultra High Definition Television – digital ultra high definition television standards*

VOC – *Voice File – 8-bit audio format*

WAV – *Wave Form Audio File – 16-bit audio format developed by Microsoft*

WCS – *Windows Color System*

WMA – *Widows Media Audio – series of audio codecs and their corresponding audio coding formats developed by Microsoft*

WMF – *Windows Meta File – universal vector graphics file format for Windows applications*

XOR – *eXclusive OR – logical and bitwise operation modulo two addition*

XYZ – *see CIE XYZ*

YCbCr – *color model that uses a luminance component and two color difference components*

YUV – *color model that uses a luminance component and two color difference components*

ПЕРЕДМОВА

Сьогодні важливим чинником у розвитку суспільства є інформаційні технології, що проникають у всі сфери людської діяльності – в державне управління, економіку, науку, освіту, культуру та побут.

Отож доволі строгий, проте доступний виклад основ теорії інформації та кодування, як одних з фундаментальних галузей комп'ютерних наук, є своєчасним і потрібним для підготовки спеціалістів.

Посібник містить дванадцять розділів.

Перший розділ, вступний, окреслює предмет комп'ютерних наук. У ньому означено поняття інформаційної системи та інформаційної технології.

У другому та третьому розділах викладено головні поняття теорії інформації та питання кількісної оцінки інформації дискретних ймовірнісних джерел. Зокрема, розглянуто математичні моделі сигналів, перетворення аналогових сигналів у цифрові, теорему про відліки, способи кодування тексту та чисел у комп'ютерах, ентропію простого та стаціонарного джерела інформації.

У четвертому та п'ятому розділах викладено основи теорії ефективного кодування та її застосування до стиснення даних. Розглянуто побудову префіксних кодів за допомогою бінарних дерев, теорему Шеннона для стаціонарних джерел, методи ефективного кодування Шеннона–Фано, Гаффмана та арифметичного кодування, а також приклади їхнього використання. Описано методи стиснення даних без втрати інформації, зокрема, словникові методи стиснення і метод Лемпела–Зіва–Велча.

У розділах 6, 7 та 8 розглянуто основи моделювання та представлення у комп'ютерах графічних, звукових та відеоданих. Викладено основи колориметрії, колірні моделі та кодування кольорів. Розглянуто базові графічні моделі та формати, методи кодування звуку та відеозображень, а також методи їхнього стиснення.

У розділі 9 вивчатимемо проблеми завадостійкого кодування. На строгому математичному рівні розглянуто загальні питання побудови лінійних систематичних кодів, зокрема, коду Геммінґа.

У десятому та одинадцятому розділах викладено основи криптографії. Детально описано симетричні криптосистеми та криптосистеми з відкритим ключем. Розглянуто стандарти шифрування даних, гешувальні функції, цифровий підпис, викладено алгоритм *RSA* та його надійність.

У дванадцятому розділі розглянуто теоретичні основи побудови електронних схем комп'ютерів, які ґрунтуються на апараті математичної логіки.

Для розуміння головних теоретичних положень, викладених у посібнику, достатньо знань з курсу вищої математики для ЗВО. Посібник містить значну кількість прикладів, які ілюструють теоретичний матеріал. Наприкінці кожного розділу подано запитання для самоконтролю.

Під час підготовки посібника автори використали усі джерела, наведені у списку літератури.

Автори висловлюють глибоку вдячність професорам В. Б. Дудикевичу, Т. С. Нагірному та Р. М. Пасічнику за зауваження та пропозиції, надані ними під час рецензування посібника.

Електронне навчальне видання

ПРОКОПИШИН Іван Анатолійович
РИКАЛЮК Роман Євстахович
ЧЕКУРІН Василь Феодосійович
ЧЕРВІНКА Костянтин Андрійович

Основи теорії інформації та кодування

Навчальний посібник

Редактор
Ірина Лоїк

Комп'ютерне верстання
Іван Прокопишин

Дизайн обкладинки
Василь Роган

Формат 60x84/8. Умовн. друк. арк. 18,1. Зам. № 8Е

Видавець і виготовлювач:
Львівський національний університет імені Івана Франка,
вул. Університетська, 1, м. Львів, 79000 Львів.

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців,
виготівників і розповсюджувачів видавничої продукції:
Серія ДК № 3059 від 13.12.2007.