

LITERATURA

Teorie kódování úzce souvisí s dalšími obory, o kterých jsme se nemohli zmínit. Je to především teorie informace. Velmi podrobnou monografií je kniha

- [1] GALLAGER, R.G. : Information theory and reliable communication. New York, J. Wiley 1968. (Ruský překlad: Teoriija informacii i naděžnaja svjaz. Moskva, Sovetskoje radio 1974.)

V textu jsem se opíral o čtivou učebnici

- [2] ABRAMSON, N. : Information theory and coding. New York, McGraw-Hill 1963.

Z novějších publikací je třeba jmenovat

- [3] MACELIECE, R.J. : The theory of information and coding. Reading, Addison-Wesley 1978.

Souvislosti teorie kódování s kombinatorikou a geometrií najde čtenář ve fundamentální monografii

- [4] MACWILLIAMS, F.J. - SLOANE, N.J.A. : The theory of error-correcting codes. Amsterdam-New York-Oxford, North Holland 1981 (3. vydání).

Tato monografie, ze které jsem vycházel v kapitolách 9 až 38, obsahuje podrobné informace o bezpečnostních kódech z nejrůznějších hledisek a přináší také obsáhlou bibliografii. K dalším významným monografiím, věnovaným bezpečnostním kódům, patří

- [5] BERLEHAMP, E.R. : Algebraic coding theory. New York, McGraw-Hill 1968. (Ruský překlad: Algebrajičeskaja teoriija kodirovanija. Moskva, Mir 1971.)

a

- [6] PETERSON, W.W. : Error-correcting codes. Cambridge, Mass., MIT Press 1961. (Ruský překlad: Kody, ispravlajuščije ošibky. Moskva, Mir 1964.)

Souvislosti bezpečnostních kódů s konečnou algebrou probírá skriptum matematicko-fyzikální fakulty KU v Praze

- [7] BICAN, L. - KEPKA, T. - NĚMEC, P. : Úvod do teorie konečných těles a lineárních kódů. Praha, SPN 1982.

Základy lineární algebry potřebné pro pochopení naší knihy najde čtenář například v knihách

- [8] MACLANE, S. - BIRKHOFF, G. : Algebra. Bratislava, Alfa 1973

a

- [9] DEMLOVÁ, M. - NAGY, J. : Algebra (Matematika pro vysoké školy technické III). Praha, SNTL 1982.

Konkrétní aplikace v práci počítačů probírá kniha

- [10] MARTIN, J. : Security, accuracy and privacy in computer systems. New Jersey, Prentice Hall 1973.

Kódování tajných zpráv je věnována monografie

- [11] van TILBORG, H. C. A. : An introduction to cryptology. Kluwer, Boston 1988.

Z novějších publikací, věnovaných bezpečnostním kódům, bych čtenáři doporučil tyto dvě :

- [12] BLAHUT, R.E. : Theory and practice of error control codes. Reading, Addison-Wesley 1983,
- [13] LIN, SHU-CASTELLO, D.J. : Error control coding. Englewood Cliffs N. J., Prentice Hall 1983.