LITERATURA

1. Abramson,N. "A Class of Systematic Codes for Non-Independent Errors," IRE Transactions on Information Theory, IT-5, 150/1959/.

2. Anderson, J. P.: Computer Security Technology Planning Study, ESD-TR-73-51, vol. I. ESD/AFSC, Hanscom AFB, Bedford, Mass., October 1972 (NTIS AD-758 206).

3. Bell, D. E., LaPadula, L. J.: Secure Computer Systems: Unified Exposition and Multics Interpretation, MTR-2997 Rev. 1, MITRE Corp., Bedford, Mass., March 1976.

4. Bose,R. and Ray-Chaudhuri,D., "A Class of Error-Correcting Binary Group Codes," Information and Control, Vol.3/March 1960/.

5. Brand, S. L.: "An Approach to Identification and Audit of Vulnerabilities and Control in Application Systems", in Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls, Z. Ruthberg, ed., NBS Special Publication 500-57, MD78733, April 1980.

6. Brand, S. L.: "Data Processing and A-123", in Proceedings of the Computer Performance Evaluation User's Group 18th Meeting, C. B. Wilson, ed., NBS Special Publication 500-95, October 1982.

7. Clark,R. "The Death of Privacy," McCall's, Feb.1970.

8. "Computer Mixes Up 11-Plus Results,"
The Daily Telegraph (London), Aug.1, 1967

9. Denning, D. E.: "A Lattice Model of Secure Information Flow", in Communications of the ACM, vol. 19, no. 5 (May 1976), pp. 236-243.

10. Denning, D. E.: Secure Information Flow in Computer Systems, Ph.D. dissertation, Purdue Univ., West Lafayette Ind., May 1975.

11. Denning,D.E. "Cryptography and Data Security" Addison-Wesley,1982

12. DoD 5200.1-R, Information Security Program Regulation, August 1982.

13. DoD Directive 5200.28, Security Requirements for Automatic Data Processing (ADP) Systems, revised April 1978.

14. DoD 5200.28-M, ADP Security Manual -- Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems, revised June 1979.

15. DoD Directive 5215.1, Computer Security Evaluation Center, 25 October 1982.

16. DoD 5220.22-M, Industrial Security Manual for Safeguarding Classified Information, January 1983.

17. DoD 5220.22-R, Industrial Security Regulation, January 1983.

18. DoD Directive 5400.11, Department of Defense Privacy Program, 9 June 1982.

19. DoD 5200.28-STD-001, Trusted Computer System Evaluation Criteria (Orange Book), 1985.

20. Executive Order 12356, National Security Information, 6 April 1982.

21. Faurer, L. D.: "Keeping the Secrets Secret", in Government Data Systems, November - December 1981, pp. 14-17.

22. Federal Information Processing Standards Publication (FIPS PUB) 39, Glossary for Computer Systems Security, 15 February 1976.

23. Federal Information Processing Standards Publication (FIPS PUB) 46, Data Encryption Algorithm Standard, 1977.

24. Federal Information Processing Standards Publication (FIPS PUB) 73, Guidelines for Security of Computer Applications, 30 June 1980.

25. Federal Information Processing Standards Publication (FIPS PUB) 102, Guideline for Computer Security Certification and Accereditation.

26. Gasser, M.: "Building a Secure Computer System", van N. Reinhold Company Inc., 1988.

27. Gaines,H.F., Cryptoanalysis, Dover Publications, Inc., New York, 1959

28. Galland,J:S., An Historical and Analytical Bibliography of the Literature of Cryptography /Northwestern University Series in the Munanities, No.10/, Northwestern University, Evanston, III1, 1945

29. Chambers,A.D.: Audit test packs and audit programs, The Comp.Journal, 18,1975, 2,98-101.

30. Gogarview: Crime-Time for Advice on Ethics, Comp.Weekly, 12 ,April, 1979,p.4.

31. "Guidelines for Protection and Control in a Computer Environment," International Businness Maschines, Pouhghkeepsie, N.Y.,1971

32. Hagelbarger,D. "Error Detection Using Recurrent Codes." Presented at the AIEE Winter General Meeting Feb.1960.

33. Hamilton,P. Espionage and Subversion in an Industrial Society, Hutchinson Publishing Group Ltd., London, 1967

34. Hamming,R.W., "Error Detecting and Error Correcting Codes," Bell System Technical Journal /April 1950/.

35. Fire,P. "A Class of Multiple-Error-Correcting Binary Codes for Non-Independent Errors," Stanford Electronics Laboratories, Technical Report No.55 April 24,1959.

36. Hoffman, Lance, "Regue Programs: Viruses, Worms and Trojan Horses, Van Nostrand Reinhold, 1990.

37. Friedman,H.F., Military Cryptoanalysis, War Department, Office of the Chief Signal Officer, Washington, D.C., U.S. Government Printing Office, series of papers from 1939 to 1943.

38. Hruska, J., Keith, J.: Computer Security Solutions, CRC Press, 1990.

39. Information Technology Security Evaluation Criteria (ITSEC), Bonn, 1990 (draft).

40. International Standard Organization (ISO) 9160, Information Processing - Data Encipherment - Physical Layer Interoperability, 1988.

41. International Standard Organization (ISO) 7498-2, Information Processing-Open Systems Interconnection Reference Model-Part 2 Security Architecture, 1985.

42. Kahn, D.: "The Codebreakers, Macmillan, 1967.

43. Konheim, A. G.: "Cryptography: A Primer", Wiley - Interscience, 1981.

44. Krauss,L.I. - McGahan,A.: Computer Fraud and Countermeasure, Prentice Hall 1979.

45. "L'Affaire Eole, "Science, 29,Oct.1971.

46. Lampson,B.W "A Note on the Confinement Problem," in Communications of the ACM, vol.16, no. 10 (October 1973), pp. 613-615

47. Lee, T. M. P., et al. "Processors, Operating Systems and Nearby Peripherals: A Consensus Report", in Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls, Z. Ruthberg, ed., NBS Special Publication 500-57, MD78733, April 1980.

48. Lipner, S. B.: A Comment on the Confinement Problem, MITRE Corp., Bedford, Mass.

49. Melas,M. "A New Group of Codes for Correction of Dependent Errors in Data Transmission," IBM Journal, Vol.4,58/1960

50. Merkle,R.C.: Secure Communications over Insecure Channels, CACM 21, No 4, April 1978, 294-299.

51. McGuire,E.P.: Target for Terrorists. The Conference Board Record, August 1971

52. Millen, J. K.: "An Example of a Formal Flow Violation", in Proceedings of the IEEE Computer Society 2nd International Computer Software and Applications Conference, November 1978, pp. 204-208.

53. Millen, J. K.: "Security Kernel Validation in Practice", in Communications of the ACM, vol. 19, no. 5 (May 1976), pp. 243-250.

54. Myers,E.: Computer Criminals, Beware Datamation, 21.Dec.1975, 12,105-107.

55. Myers,E.: Computer Security: Each Case is Different, Datamation,21,April 1975, 4, 107-109.

56. National Fire Protection Association, "Standards for the Installation of Portable Fire Extinguishers," Pamphlet No.10, Boston, 1968.

57. Needham,R.M., Schroeder M.D.: Using Encryption for Authentisation in Large Networks of Computers, CACM 21, No 12, Dec.1978, 993-998.

58. NCSC-TG-005, Trusted Network Interpretation of TCSEC (Red Book), 1987.

59. Nibaldi, G. H.: Proposed Technical Evaluation Criteria for Trusted Computer Systems, MITRE Corp., Bedford, Mass., M79-225, AD-A108-832, 25 October 1979.

60. Nibaldi, G. H.: Specification of A Trusted Computing Base, (TCB), MITRE Corp., Bedford, Mass., M79-228, AD-A108-831, 30 November 1979.

61. OMB Circular A-71, Transmittal Memorandum No. 1, Security of Federal Automated Information Systems, 27 July 1978.

62. OMB Circular A-123, Internal Control Systems, 5 November 1981.

63. Parker,D.B., Computer Crime, Infotsch Seminar, 14-16 Nov.1968.

64. Peterson,W.W., Error Correcting Codes, The M.I.T. Press, Cambridge, Mass., John Wiley & Sons, Inc., New York, 1961.

65. Pfleger,Ch.F. "Security in Computing," Prentice-Hall, 1989

66. Rabin,M.O.: Digitalized Signatures and Public-Key Functions as Intractable as Factorization, MIT Lab.Comp.Sci.Tech.Dept.212.

67. Rivest,R.L., et al.: A Method for Obtaining Digital Signatures and Public-key Cryptosystems, CACM 21, No 2, Feb.1978, 120-126.

68. Ruthberg, Z., McKenzie, R., eds. Audit and Evaluation of Computer Security, in NBS Special Publication 500-19, October 1977.

69. Schaefer, M., Linde, R. R., et al. "Program Confinement in KVM/370", in Proceedings of the ACM National Conference, October 1977, Seattle.

70. Schell,R.R. "Security Kernels: A Methodical Design of System Security," in Technical Papers, USE Inc. Spring Conference, 5-9 March 1979, pp. 245-250

71. Shannon,C.E. "The Communication Theory of Secrecy Systems," Bell System Technical Jornal, Vol.28/Oct.1949/

72. The Daily Mail /London/, March 18, 1968.

73. Trotter, E. T., Tasker, P. S.: Industry Trusted Computer Systems Evaluation Process, MITRE Corp., Bedford, Mass., MTR-3931, 1 May 1980.

74. Turn, R.: Trusted Computer Systems: Needs and Incentives for Use in government and Private Sector, (AD A103399), Rand Corporation (R-28811-DR&E), June 1981.

75. US index to combat insurance fire frauds, Comp. Weekly, 15,March 79

76. Vernam,A.S. "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications," Journal of the IEE, Vol.45,109-115/1926/.

77. Walker, S. T.: "The Advent of Trusted Computer Operating Systems", in National Computer Conference Proceedings, May 1980, pp. 655-665.

78. Ware, W. H.: Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security, AD A076617/0, Rand Corporation, Santa Monica, Calif., February 1970, reissued October 1979.

79. Williams D., Hindin,H.: Cann Software do Encription Job?, Electronics, July 3, 1980, str.102-103.

Literatura k příloze A

[1] Petterson,W.W., Weldon,E.: Error-Correcting Codes,MIT Press, Massachusetts 1972 (ruský překlad Mir, Moskva 1976).

[2] Alexander,A.A., Gryb,R.M., Nast,D.W.: Capabilities of the telephone network for data transmission. BSTJ 39 (1960), 431-476.

[3] Kubín,B.,Průcha,S.,Přibyl,J.,Pužman,J.: Oborová norma FMS: Po a definice v oboru abecední a obrazové telegrafie a přenosu dat. Tech.ústředna spojů, Praha 1976.

[4] Přibyl,J. a kol.: Výzkumná zpráva k HS 5/78 B. Kate telekomunikační techniky FEL ČVUT, 1978.

[5] Vajda,I.: Odhadování a simulace šumu v telekomunikačn kanálech. DROMS 84, Dům techniky ČSVTS Ostrava 1984, 143-158.

[6] Brayer,K.: Error control techniques using binary symbol bur codes. Trans.IEEE, COM-16 (1968), 781-789

[7] Ephremides,A., Snyder,R.O.: Modelling of high error rate linory communication channels. Trans.IEEE, IT-28(1982), 549-555.

[8] Bek,Z.: Diplomová práce. Katedra telekomunikační techniky FEL ČVUT, Praha 1987.

[9] Vajda,I.: Teoretické aspekty rychlého přenosu dat v telekomunikačních sítích. Přenos dat. ČSVTS Brno 1981.

[10] Vajda,I.: Minimum chi-square estimates of multistate communication models. Probl.Contr.Inform.Theory 13 (1984), 343-356.

[11] Barg,A.M., Vvedenskaja,N.D., Zyablov,V.V.: On error and erasure probabilites for block codes decoding in a fading channel: Probl.Contr.Inform.Theory 16 (1987), 329-340.