10.8 Odkazy

[1] ANSI X3.92-1981,"American National Standard for Information Systems - Data Encrypton Algorithm (DEA)", ANSI.

[2] BS 7799,"Code of practice for Information security management",BSI, U.K, 1995.

[3] ANSI X3.105-1983,"American National Standard for Information Systems - Data Link Encryption", ANSI.

[4] Canadian System Security Centre,"Canadian Trusted Computer Product Evaluation Criteria", V.3.0e, Government of Canada, 1993.

[5] CSC-STD-002-85,"Department of Defence Password Management Guideline", DoD,, 1985.

[6] CSC-STD-003-85,"Computer Security Requirements - Guidance for Applying the Department of Defence Trusted Computer System Evaluation Criteria in Specific Environments", DoD, 1985.

[7] CSC-STD-004-85,"Technical Rational behind CSC-STD-003-85: Computer Security Requirements - Guidance ro Applying the Departmentof Defence Trusted Computer System Evaluation Criteria in Specific Environments", DoD, 1985.

[8] DoD 5200.28-STD,"Trusted Computer Evaluation Criteria", Department of Defence, U.S.A.,1985

[9] EEC report," Security in Open Network",document Nr.303, 1989

[10] FIPS PUB 46,"Data Encryption Standard", Federal Information Processing Standard, National Bureau of Standards, U.S. Department of Commerce, U.S.A., 1977.

[11] ISO/IEC 7498,"Information processing - Open system interconnection - Basic reference model", ISO, 1984.

[12] ISO/IEC 7498-2,"Information processing - Open system interconnection - Basic reference model - Part 2: Security architecture", ISO/IEC, 1987.

[13] ISO/DIS 8227 Final text of,"Data cryptographic techniques", ISO/TC 20/SC 20, 1986.

[14] ISO 8372," Information proccessing - Data cryptographic techniques Modes of operation for a 64-bit cipher algorithm", ISO,1987.

[15] ISO 8572,"Information proccessing - OSI File Transfer, Access and Management - Security Features", ISO.

[16] ISO 8649," Information proccessing systems - OSI service definition for common Application service elements - Authentication", ISO.

[17] ISO 8731-1,"Banking- approved algorithms for message authentication - Part 1: DEA", ISO,1987.

[18] ISO/IEC 9160," " Information proccessing - Data cryptographic techniques - Physical layer interoperability requirements", ISO/IEC, 1990.

[19] ISO/IEC 9796," Information proccessing - Security techniques - Digital signature scheme giving message recovery",ISO/IEC, 1991.
[20] ISO/IEC 9797," Information proccessing - Security techniques - Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm",ISO/IEC, 1989.
[21] ISO/IEC 9798-1," Information proccessing - Security techniques - Data - Entity authentication - Part 1: General model", ISO/IEC, 1991.
[22] ISO/IEC 9798-2," Information proccessing - Security techniques - Data - Entity authentication - Part 2: Entity authentication using symmetric techniques", ISO/IEC, 1993.
[23] ISO/IEC 9798-3," Information proccessing - Security techniques - Data - Entity authentication - Part 3: Entity authentication using a public key algorithm", ISO/IEC, 1993.
[24] ISO/IEC 9798-4," Information proccessing - Security techniques - Data - Entity authentication - Part 4: Entity authentication using a cryptographic check function", ISO/IEC, 1995.
[25] ISO 9945,"POSIX- Portable operating system interface for computer environment", ISO.
[26] ISO/IEC 9979," Information proccessing - Security techniques -Procedures for the registration of cryptographic algorithms", ISO/IEC, 1991.
[27] [27]ISO/IEC 10116," Information proccessing - Security techniques - Modes of operation for an n-bit cipher algorithm", ISO/IEC,1991.
[28] ISO/IEC 10118-1," Information proccessing - Security techniques - Hash-functions - Part 1: General", ISO/IEC, 1992.
[29] ISO/IEC 10118-2," Information proccessing - Security techniques - Hash functions - Part 2: Hash-functions using an n-bit block cipher algoritm", O/IEC, 1992.
[30] ISO 10021,"Information proccessing- message oriented text interchange systems", ISO/CCITT.
[31] ITSEC," Information Technology Security Evaluation Criteria (ITSEC)", Provisional Harmonized Criteria, Version 1.2, 1991.
[32] ITSEM," Information Technology Security Evaluation Manual (ITSEM)", Version 1.0, 1994.
[33] S.M.Matyas, C.H.Mayer a J.Oseas,"Generating Strong One-way Functions with Cryptographic Algorithm", *IBM. Techn. Discl. Bull.*, vol.27, No.10A, 1985, str. 5658-5659.
[34] NCSC-TG-001,"A Guide to Understanding Audit in Trusted Systems",NCSC, 1988.
[35] NCSC-TG-002,"Trusted Product Evaluations: A Guide for Vendors", NCSC, 1990.
[36] NCSC-TG-003,"A Guide to Understanding Discretionary Access Control in Trusted Systems", NCSC, 1987.
[37] NCSC-TG-004,"Glossary of Computer Security Terms", NCSC,1988.

[38] NCSC-TG-005,"Trusted Network Interpretation of the Trusted ComputerSystem Evaluation Criteria",NCSC, 1987.
[39] NCSC-TG-006,"A Guide to Understanding Configuration Management in Trusted Systems", NCSC, 1988.
[40] NCSC-TG-007," A Guide to Understanding Design Documentation in Trusted Systems", NCSC, 1988.
[41] NCSC-TG-008," A Guide to Understanding Trusted Distribution in Trusted Systems", NCSC, 1988.
[42] NCSC-TG-009," Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria",NCSC, 1988.
[43] NCSC-TG-010," A Guide to Understanding Security Modeling in Trusted Systems", NCSC, 1990.
[44] NCSC-TG-011,"Trusted Network Interpretation Environments Guideline - Guidance for Applying the Trusted Network Interpretation", NCSC, 1990.
[45] NCSC-TG-013," Rating Maintenance Phase Program Document", NCSC, 1989.
[46] NCSC-TG-014,"Guidelines for Formal Verification Systems", NCSC, 1989.
[47] NCSC-TG-015,"A Guide to Understanding Trusted Facility Management", NCSC, 1989.
[48] NCSC-TG-016," Guidelines for Writing Trusted Facility Manuals", NCSC, 1991.
[49] NCSC-TG-017," A Guide to Understanding Identification and Authentication in Trusted Systems", NCSC, 1991.
[50] NCSC-TG-018," A Guide to understanding Object Reuse in Trusted Systems", NCSC, 1991.
[51] NCSC-TG-019,"Trusted Product Evaluation Questionaire", NCSC, 1989.
[52] NCSC-TG-020-A,"Trusted UNIX Working Group (TRUSIX) Rationale for Selecting Access Control ListFeatures for the UNIX* System", NCSC, 1989.
[53] NCSC-TG-021,"Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria", NCSC, 1991.
[54] NCSC-TG-022," A Guide to understanding Trusted Recovery in Trusted systems", NCSC, 1991.
[55] NCSC-TG-023," A Guide to Understanding Security Testing and Test Documentation in Trusted Systems", NCSC.
[56] NCSC-TG-024, vol.1/4," A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements", NCSC.
[57] NCSC-TG-024,vol.2/4," A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators", NCSC.

[58] NCSC-TG-024,vol.3/4," A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Items Description Tutorial", NCSC.
[59] NCSC-TG-025,"A Guide to Understanding Data Remanence in Automated Information Systems", NCSC, 1991.
[60] NCSC-TG-026," A Guide to Writing the Security Features User's Guide for Trusted Systems",NCSC, 1991.
[61] NCSC-TG-027," A Guide to understanding Information System Security Officer Responsibilities for Automated Information Systems", NCSC.
[62] NCSC-TG-028,"Assessing Controlled Access Protection", NCSC.
[63] NCSC-TG-029," Introduction to Certification and Accreditation Concepts", NCSC.
[64] NCSC-TG-030," A Guide to Undestanding Cover Channel Analysis of Trusted Systems", NCSC.
[65] OCDE/GD(92)190,"Guidelines for the Security of Information systems", OECD, 1992.
[66] B.Preneel, R.Govaerts a J. Vandewalle,"Computer Security and Industrial Cryptography", LNCS 741,Springer-Verlag, 1991.
[67] D.Russell a G.T.Gangemi Sr., „Computer Security Basics", O'Reilly&Associates, Inc., 1992.
[68] X.400,"Eight CCITT Recommendations on Message Handling Systems", CCITT.
[69] X.509/ ISO 9594-8,"Eight CCITT Recommendations on Directory Services, Directory - Authentication Framework", CCITT/ISO.