

MEZINÁRODNÍ NORMA

Informační technologie –
Směrnice pro řízení bezpečnosti IT –
Část 4: Výběr ochranných opatření

ISO/IEC TR 13335-4

První vydání
2000-03-01

ICS 35.040

www.cni.cz

Obsah

Sp 261
 ODD. VĚDECKÝCH INFORMACÍ při MZČ
 Palackého nám. 4, 128 01 Praha 2 ©
 detašované pracoviště NLK Praha 2
 DIČ CZ00023825 IČO 00023825

11 761

Př. č. 306/2005

Strana

Úvod	7
1 Předmět normy	8
2 Odkazy	8
3 Termíny a definice	8
4 Cíl	8
5 Přehled	9
6 Úvod do výběru ochranných opatření a koncepce základní úrovně bezpečnosti	11
7 Základní odhady	15
7.1 Identifikace typu systému IT	15
7.2 Identifikace fyzikálních podmínek / podmínek okolního prostředí	15
7.3 Posouzení existujících / plánovaných ochranných opatření	16
8 Ochranná opatření	16
8.1 Organizační a fyzická ochranná opatření	16
8.1.1 Řízení bezpečnosti IT a politiky bezpečnosti IT	16
8.1.2 Kontrola bezpečnostní shody	17
8.1.3 Řešení incidentů	18
8.1.4 Zaměstnanci	18
8.1.5 Provozní problémy	18
8.1.6 Plánování kontinuity činnosti organizace	20
8.1.7 Fyzická bezpečnost	20
8.2 Ochranná opatření specifická pro systém IT	25
8.2.1 Identifikace a autentizace (I&A)	25
8.2.2 Řízení logického přístupu a audit	26
8.2.3 Ochrana před škodlivým programovým kódem	26
8.2.4 Správa sítí	27
8.2.5 Kryptografie	28
9 Přístup na základní úrovni: Výběr ochranných opatření podle typu systému IT	31
9.1 Všeobecně aplikovatelná ochranná opatření	32
9.2 Ochranná opatření specifická pro systém IT	32
10 Výběr ochranných opatření v závislosti na bezpečnostních problémech a hrozbách	33
10.1 Posouzení bezpečnostních problémů	34
10.1.1 Ztráta důvěrnosti	34

	Strana
10.1.2 Ztráta integrity.....	35
10.1.3 Ztráta dostupnosti.....	35
10.1.4 Ztráta individuální odpovědnosti.....	35
10.1.5 Ztráta autentičnosti.....	36
10.1.6 Ztráta spolehlivosti.....	36
10.2 Ochranná opatření zajišťující důvěrnost.....	36
10.2.1 Odposlouchávání.....	36
10.2.2 Elektromagnetická radiace	37
10.2.3 Škodlivý programový kód	37
10.2.4 Předstírání identity uživatele	37
10.2.5 Nesprávné směrování / přesměrování zpráv	37
10.2.6 Chyba software.....	38
10.2.7 Krádež	38
10.2.8 Neautorizovaný přístup k počítačům, datům, službám a aplikacím	38
10.2.9 Neautorizovaný přístup k paměťovým médiím	39
10.3 Ochranná opatření zajišťující integritu.....	39
10.3.1 Zhoršení kvality paměťového média.....	39
10.3.2 Chyba údržby	39
10.3.3 Škodlivý programový kód	39
10.3.4 Předstírání identity uživatele	40
10.3.5 Nesprávné směrování / přesměrování zpráv	40
10.3.6 Nepopiratelnost	40
10.3.7 Chyba software.....	40
10.3.8 Poruchy napájení (elektrická energie, klimatizace).....	41
10.3.9 Technické poruchy	41
10.3.10 Chyby přenosu	41
10.3.11 Neautorizovaný přístup k počítačům, datům, službám a aplikacím.	41
10.3.12 Použití neautorizovaných programů a dat	42
10.3.13 Neautorizovaný přístup k paměťovým médiím	42
10.3.14 Chyba uživatele	42
10.4 Ochranná opatření zajišťující dostupnost	42
10.4.1 Destruktivní útok.....	43
10.4.2 Zhoršení kvality paměťových médií	43
10.4.3 Chyby a poruchy komunikačních zařízení a služeb.....	43
10.4.4 Požár, voda	44
10.4.5 Chyba údržby	44
10.4.6 Škodlivý programový kód	44
10.4.7 Předstírání identity uživatele	44
10.4.8 Nesprávné směrování / přesměrování zpráv	45
10.4.9 Zneužití zdrojů	45
10.4.10 Přírodní katastrofy	45
10.4.11 Chyby software.....	45

	Strana
10.4.12 Poruchy napájení (elektrická energie, klimatizace)	46
10.4.13 Technické poruchy	46
10.4.14 Krádež	46
10.4.15 Přetížení provozu	46
10.4.16 Chyby přenosu	47
10.4.17 Neautorizovaný přístup k počítačům, datům, službám a aplikacím.	47
10.4.18 Použití neautorizovaných programů a dat	47
10.4.19 Neautorizovaný přístup k paměťovým médiím	47
10.4.20 Chyba uživatele	48
10.5 Ochranná opatření zajišťující individuální odpovědnost, autentičnost a spolehlivost	48
10.5.1 Individuální odpovědnost	48
10.5.2 Autentičnost	48
10.5.3 Spolehlivost	48
11 Výběr ochranných opatření podle podrobných posouzení	49
11.1 Vztah mezi částí 3 a částí 4 ISO/IEC TR 13335	49
11.2 Zásady výběru	49
12 Vývoj základní úrovně pro celou organizaci	50
13 Shrnutí	51
Bibliografie	52
Příloha A Code of Practice for Information Security Management	53
Příloha B ETSI Baseline Security Standard – Features and Mechanisms	55
Příloha C IT Baseline Protection Manual	57
Příloha D NIST Computer Security Handbook	59
Příloha E Medical Informatics: Security Categorisation and Protection for Healthcare Information Systems	61
Příloha F TC68 Banking and Related Financial Services – Information Security Guidelines	63
Příloha G Protection of sensitive information not covered by the Official Secrets Act – Recommendations for computer workstations.	65
Příloha H Canadian Handbook on Information Technology Security	67
Národní příloha NA (informativní)	69



Označeno
23.01.2009
OVI
ABE015



Národní lékařská knihovna - OVI

Název: ČSN ISO/IEC TR 13335-4

Autor:

Rok 2002



Přír. č.: SP20050306 Sign: Sp 261