

	Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Požadavky na záruky bezpečnosti	ČSN ISO/IEC 15408-3 36 9789
---	--	---------------------------------------

Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

Technologies de l'information - Techniques de sécurité - Critères d'évaluation pour la sécurité TI - Partie 3: Exigences d'assurance de sécurité

Informationstechnik - IT-Sicherheitsverfahren; Evaluationskriterien für IT-Sicherheit - Teil 3: Anforderungen an die Vertrauenswürdigkeit

Tato norma je českou verzí mezinárodní normy ISO/IEC 15408-3:1999. Mezinárodní norma ISO/IEC 15408-3:1999 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 15408-3:1999. The International Standard ISO/IEC 15408-3:1999 has the status of a Czech Standard.

Národní předmluva

Citované normy

ISO/IEC 15408-1 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT
- Část 1: Úvod a všeobecný model

ISO/IEC 15408-2 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT
- Část 2: Bezpečnostní funkční požadavky

Národní poznámka

Anglické slovo „security“ se pro účely této normy překládá jako „bezpečnost“.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Strana 3

MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky -
Kritéria pro hodnocení bezpečnosti IT -
Část 3: Požadavky na záruky bezpečnosti

ISO/IEC 15408-3
První vydání
1999-12-01

ICS 35.040

Obsah

Strana

1 Předmět normy

.. 8

1.1 Organizace ISO/IEC
15408..... 8

1.2 Vzor záruky podle ISO/IEC
15408..... 8

1.2.1 Filosofie ISO/IEC
15408..... 8

1.2.2	Pojetí záruky	
.....		8
1.2.3	Stupnice hodnocení záruky podle ISO/IEC 15408.....	9
2	Požadavky na záruky bezpečnosti.....	10
2.1	Struktury	
.....		10
2.1.1	Struktura třídy	
....		10
2.1.2	Struktura rodiny záruky.....	10
2.1.3	Struktura komponent záruky.....	12
2.1.4	Prvky záruky	
.....		13
2.1.5	Struktura EAL	
....		14
2.1.6	Vzájemný vztah mezi zárukami a mírami záruk.....	16
2.2	Taxonomie komponent	
.....		16
2.3	Struktura tříd Profil ochrany a Bezpečnostní cíl kritérií hodnocení.....	16
2.4	Použití termínů v ISO/IEC 15408-3.....	16
2.5	Kategorizace záruk	

.....	18
2.6 Přehled tříd a rodin záruky.....	18
2.6.1 Třída ACM: Správa konfigurace.....	18
2.6.2 Třída ADO: Dodání a provoz.....	19
2.6.3 Třída ADV: Vývoj 19	
2.6.4 Třída AGD: Průvodní dokumentace.....	20
2.6.5 Třída ALC: Podpora životního cyklu.....	20
2.6.6 Třída ATE: Testy 20	
2.6.7 Třída AVA: Určení zranitelností.....	21
2.7 Kategorizace údržby	21
2.8 Přehled rodin a tříd údržby záruky.....	22
2.8.1 Třída AMA: Údržba záruky.....	22
3 Kriteria hodnocení Profilu ochrany a Bezpečnostního cíle.....	23
3.1 Přehled	23
3.2 Kritéria Profilu ochrany - přehled.....	23

3.2.1	Hodnocení Profilu ochrany.....	23
3.2.2	Vztah ke kritériím hodnocení Bezpečnostního cíle.....	23
3.2.3	Úlohy hodnotitele	23
3.3	Přehled kritérií Bezpečnostního cíle.....	24
3.3.1	Hodnocení Bezpečnostního cíle.....	24
3.3.2	Vztah k dalším kritériím hodnocení této části ISO/IEC 15408.....	24
3.3.3	Úlohy hodnotitele	24
4	Třída APE: Hodnocení Profilu ochrany.....	26
4.1	Popis TOE (APE_DES)	27
4.2	Bezpečnostní prostředí (APE_ENV).....	28
4.3	Uvedení PP (APE_INT)	29
4.4	Cíle bezpečnosti (APE_OBJ).....	30
4.5	Požadavky na bezpečnost IT (APE_REQ).....	31
4.6	Explicitně dané požadavky na bezpečnost IT (APE_SRE).....	33
5	Třída ASE: Hodnocení bezpečnostního cíle.....	34

5.1	Popis TOE (ASE_DES)	35
5.2	Bezpečnostní prostředí (ASE_ENV)	36
5.3	Uvedení ST (ASE_INT)	37
5.4	Cíle bezpečnosti (ASE_OBJ)	38
5.5	Tvrzení PP (ASE_PPC)	39
5.6	Požadavky na bezpečnost IT (ASE_REQ)	40
5.7	Explicitně dané požadavky na bezpečnost IT (ASE_SRE)	42
5.8	Souhrnná specifikace TOE (ASE_TSS)	43
6	Míry záruky hodnocení	45
6.1	Míry záruk hodnocení - přehled	45
6.2	Podrobnosti úrovní míry záruky hodnocení	45
6.2.1	Míra záruky hodnocení 1 (EAL1) - funkčně testováno	47
6.2.2	Míra záruky hodnocení 2 (EAL2) - strukturovaně testováno	48
6.2.3	Míra záruky hodnocení 3 (EAL3) - metodicky testováno a kontrolováno	50
6.2.4	Míra záruky hodnocení 4 (EAL4) - metodicky navrženo, testováno a revidováno	52
6.2.5	Míra záruky hodnocení 5 (EAL5) - poloformálně navrženo a testováno	54
6.2.6	Míra záruky hodnocení 6 (EAL6) - poloformálně ověřený návrh a	

testováno.....	56
6.2.7 Míra záruky hodnocení 7 (EAL7) - formálně ověřený návrh a testováno.....	58
7 Třídy, rodiny a komponenty záruky.....	60
8 Třída ACM: Správa konfigurace.....	61
8.1 Automatizace CM (ACM_AUT).....	61
8.2 Schopnosti CM (ACM_CAP).....	63
8.3 Rozsah CM (ACM_SCP).....	68
9 Třída ADO: Dodání a provoz.....	70
9.1 Dodání (ADO_DEL).....	71
9.2 Instalace, generování a spuštění (ADO_IGS).....	73
10 Třída ADV: Vývoj.....	75

10.1 Funkční specifikace (ADV_FSP).....	78
10.2 Návrh na vyšší úrovni (ADV_HLD).....	81
10.3 Reprezentace implementace (ADV_IMP).....	85
10.4 Vnitřní struktura TSF (ADV_INT).....	88

10.5	Návrh na nižší úrovni (ADV_LLD).....	91
10.6	Soulad reprezentace (ADV_RCR).....	94
10.7	Modelování bezpečnostní politiky (ADV_SPM).....	96
11	Třída AGD: Průvodní dokumentace.....	98
11.1	Příručka pro správce (AGD_ADM).....	99
11.2	Příručka pro uživatele (AGD_USR).....	100
12	Třída ALC: Podpora životního cyklu.....	101
12.1	Bezpečnost vývoje (ALC_DVS).....	102
12.2	Náprava závad (ALC_FLR).....	104
12.3	Definice životního cyklu (ALC_LCD).....	106
12.4	Nástroje a techniky (ALC_TAT).....	108
13	Třída ATE: Testy	110
13.1	Pokrytí (ATE-COV)	111
13.2	Hloubka (ATE_DPT)	113
13.3	Testování funkčnosti (ATE_FUN).....	116
13.4	Nezávislé testování (ATE_IND).....	118

14	Třída AVA: Posouzení zranitelnosti.....	121
14.1	Analýza skrytých kanálů (AVA_CCA).....	122
14.2	Nesprávné použití (AVA_MSU).....	125
14.3	Síla bezpečnostních funkcí TOE (AVA_SOF).....	128
14.4	Analýza zranitelnosti (AVA_VLA).....	129
15	Příklad údržby záruky.....	133
15.1	Úvod.....	133
15.2	Cyklus údržby záruky.....	133
15.3	Třídy a rodiny údržby záruky.....	136
16	Třída AMA: Údržba záruky.....	140
16.1	Plán údržby záruky (AMA_AMP).....	141
16.2	Zpráva o kategorizaci komponenty TOE (AMA_CAT).....	143
16.3	Důkaz o údržbě záruky (AMA_EVD).....	145
16.4	Analýza dopadu na bezpečnost (AMA_SIA).....	147
Příloha A	(informativní) Vzájemné vztahy komponent záruky z hlediska závislostí.....	149
Příloha B	(informativní) Vzájemné vztahy EAL a komponent záruky.....	151
	Seznam obrázků	

Obrázek 2.1 - Hierarchie třídy/rodiny/komponenty/prvku záruky.....	11
Obrázek 2.2 - Struktura komponent záruky.....	12
Obrázek 2.3 - Struktura EAL.....	14
Obrázek 2.4 - Přidružení záruky a míry záruky.....	15
Obrázek 2.5 - Ukázka diagramu dekompozice třídy.....	16

Strana 6

Strana

Obrázek 4.1 - Dekompozice třídy Hodnocení Profilu ochrany.....	26
Obrázek 5.1 - Dekompozice třídy Hodnocení Bezpečnostního cíle.....	34
Obrázek 8.1 - Dekompozice třídy Správa konfigurace.....	61
Obrázek 9.1 - Dekompozice třídy Dodání a provoz.....	70
Obrázek 10.1 - Dekompozice třídy Vývoj.....	75
Obrázek 10.2 - Vzájemné vztahy mezi reprezentacemi a požadavky TOE.....	76
Obrázek 11.1 - Dekompozice třídy Původní dokumentace.....	98
Obrázek 12.1 - Dekompozice třídy Podpora životního cyklu.....	101
Obrázek 13.1 - Dekompozice třídy Testy.....	110
Obrázek 14.1 - Dekompozice třídy Posouzení zranitelnosti.....	121
Obrázek 15.1 - Příklad cyklu údržby záruky.....	134

Obrázek 15.2 - Příklad akceptace pojetí TOE.....	135
Obrázek 15.3 - Příklad pojetí monitorování TOE.....	136
Obrázek 16.1 - Dekompozice třídy Údržba záruky.....	140
Seznam tabulek	
Tabulka 2.1 - Rozpis a mapování rodin záruky.....	18
Tabulka 2.2 - Dekompozice třídy Údržba záruky.....	22
Tabulka 3.1 - Rodiny Profilu ochrany - pouze požadavky podle ISO/IEC 15408.....	23
Tabulka 3.2 - Rodiny Profilu ochrany - požadavky rozšířené nad rámec ISO/IEC 15408.....	24
Tabulka 3.3 - Rodiny Bezpečnostního cíle - pouze požadavky podle ISO/IEC 15408.....	24
Tabulka 3.4 - Rodiny Bezpečnostního cíle - rozšířené požadavky podle ISO/IEC 15408.....	25
Tabulka 6.1 - Míry záruky hdnocení - shrnutí.....	46
Tabulka 6.2 - EAL1	47
Tabulka 6.3 - EAL2	49
Tabulka 6.4 - EAL3	51
Tabulka 6.5 - EAL4	53
Tabulka 6.6 -	

EAL5

..... 55

Tabulka 6.7 -
EAL6

..... 57

Tabulka 6.8 -
EAL7

..... 59

Tabulka 15.1 - Rozpis a mapování rodiny údržba
záruky..... 137

Tabulka A.1 - Závislosti komponent
záruky..... 149

Tabulka A.2 - Vnitřní závislosti
AMA..... 150

Tabulka B.1 - Míry záruky hodnocení -
shrnutí..... 151

Strana 7

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených příslušnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i další mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

Mezinárodní normy jsou navrhovány v souladu s pravidly uvedenými v části 3 direktiv ISO/IEC.

ISO a IEC ustavily v oblasti informačních technologií společnou technickou komisi, ISO/IEC JTC 1. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Mezinárodní norma ISO/IEC 15408-3 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie*, ve spolupráci s organizacemi sponzorujícími projekt „Common Criteria“. Identický text ISO/IEC 15408-3 je zveřejněn organizacemi sponzorujícími projekt „Common Criteria“ pod názvem *Společná kritéria pro hodnocení bezpečnosti informačních technologií*. Další informace o projektu „Common Criteria“ a kontaktní informace na sponzory projektu jsou uvedeny v příloze A normy ISO/IEC 15408-1.

ISO/IEC 15408 se skládá z následujících částí se společným názvem *Informační technologie* -

Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT:

- Část 1: Úvod a všeobecný model
- Část 2: Bezpečnostní funkční požadavky
- Část 3: Požadavky na záruky bezpečnosti

Přílohy A a B této části ISO/IEC 15408 jsou pouze informativní.

Na základě žádosti byla do všech částí ISO/IEC 15408 umístěna tato PRÁVNÍ POZNÁMKA:

Sedm vládních organizací (společně nazývaných „Organizace sponzorující projekt Common Criteria“), které jsou uvedené v příloze A ISO/IEC 15408-1, přidělují tímto jako společní držitelé autorských práv dokumentu Společná kritéria pro hodnocení bezpečnosti informačních technologií, část 1 až 3 (nazývaných „CC“) organizaci ISO/IEC neexkluzivní licenci k používání CC při vývoji mezinárodní normy ISO/IEC 15408. Organizace sponzorující projekt Common Criteria si však ponechávají právo používat, kopírovat, šířit nebo pozměňovat CC, jak uznají za vhodné.

Strana 8

1 Předmět normy

Tato část ISO/IEC 15408 definuje požadavky normy na záruku. Obsahuje hodnocení míry záruky (Evaluation Assurance Levels, EALs), které definují měřítko pro posouzení záruky, jednotlivé komponenty záruky, ze kterých se skládají míry záruky, a kritéria pro hodnocení PP a ST.

-- Vynechaný text --