

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

První vydání

1999-12-01

ICS 35.040

Deskriptory: informační technologie, kritéria hodnocení IT, míra záruky hodnocení, schéma hodnocení, organizační bezpečnostní politika, produkt, profil ochrany, bezpečnostní atribut, bezpečnostní funkce, předmět hodnocení, model bezpečnostní politiky

**Obsah**

|                                                          | Strana |
|----------------------------------------------------------|--------|
| 1 Předmět normy .....                                    | 7      |
| 2 Definice .....                                         | 8      |
| 2.1 Společné zkratky .....                               | 8      |
| 2.2 Rozsah slovníku .....                                | 8      |
| 2.3 Slovník .....                                        | 8      |
| 3 Přehled .....                                          | 11     |
| 3.1 Úvod .....                                           | 11     |
| 3.2 Komu jsou CC určena .....                            | 11     |
| 3.2.1 Spotřebitelé .....                                 | 11     |
| 3.2.2 Vývojáři .....                                     | 11     |
| 3.2.3 Hodnotitelé .....                                  | 12     |
| 3.2.4 Ostatní .....                                      | 12     |
| 3.3 Kontext hodnocení .....                              | 12     |
| 3.4 Organizace CC .....                                  | 13     |
| 4 Obecný model .....                                     | 14     |
| 4.1 Bezpečnostní kontext .....                           | 14     |
| 4.1.1 Obecný bezpečnostní kontext .....                  | 14     |
| 4.1.2 Kontext bezpečnosti informačních technologií ..... | 16     |
| 4.2 Přístup CC k hodnocení .....                         | 17     |
| 4.2.1 Vývoj .....                                        | 17     |
| 4.2.2 Hodnocení TOE .....                                | 19     |
| 4.2.3 Provoz .....                                       | 20     |
| 4.3 Bezpečnostní pojmy .....                             | 20     |
| 4.3.1 Bezpečnostní prostředí .....                       | 21     |
| 4.3.2 Bezpečnostní cíle .....                            | 22     |
| 4.3.3 IT bezpečnostní požadavky .....                    | 22     |
| 4.3.4 Souhrnná specifikace TOE .....                     | 23     |
| 4.3.5 Implementace TOE .....                             | 23     |
| 4.4 Popisný materiál CC .....                            | 23     |
| 4.4.1 Vyjádření bezpečnostních požadavků .....           | 23     |

Sp 262  
 ODD. VĚDECKÝCH INFORMACÍ při MZČR  
 Palackého nám. 4, 128 01 Praha 2 ③  
 detašované pracoviště NLK Praha 2  
 DIČ CZ00023825 IČO 00023825

Pr. č. 307/2005

|                                                                     | Strana    |
|---------------------------------------------------------------------|-----------|
| 4.4.2 Použití bezpečnostních požadavků .....                        | 24        |
| 4.4.3 Zdroje bezpečnostních požadavků .....                         | 26        |
| 4.5 Typy hodnocení .....                                            | 26        |
| 4.5.1 Hodnocení PP .....                                            | 26        |
| 4.5.2 Hodnocení ST .....                                            | 26        |
| 4.5.3 Hodnocení TOE .....                                           | 26        |
| 4.6 Aktualizace záruky .....                                        | 26        |
| 5 Požadavky na CC a výsledky hodnocení .....                        | 27        |
| 5.1 Úvod .....                                                      | 27        |
| 5.2 Požadavky v PP a ST .....                                       | 27        |
| 5.2.1 Výsledky hodnocení PP .....                                   | 28        |
| 5.3 Požadavky v TOE .....                                           | 28        |
| 5.3.1 Výsledky hodnocení TOE .....                                  | 28        |
| 5.4 Námitky proti výsledkům hodnocení .....                         | 28        |
| 5.5 Použití výsledků hodnocení TOE .....                            | 28        |
| <b>Příloha A (informativní) Projekt Společná kritéria .....</b>     | <b>30</b> |
| A.1 Pozadí projektu Společná kritéria .....                         | 30        |
| A.2 Vývoj Společných kritérií .....                                 | 30        |
| A.3 Organizace sponzorující projekt Společná kritéria .....         | 30        |
| <b>Příloha B (normativní) Specifikace profilů ochrany .....</b>     | <b>32</b> |
| B.1 Přehled .....                                                   | 32        |
| B.2 Obsah profilu ochrany .....                                     | 32        |
| B.2.1 Obsah a prezentace .....                                      | 32        |
| B.2.2 Úvod PP .....                                                 | 32        |
| B.2.3 Popis TOE .....                                               | 33        |
| B.2.4 Bezpečnostní prostředí TOE .....                              | 33        |
| B.2.5 Bezpečnostní cíle .....                                       | 34        |
| B.2.6 IT bezpečnostní požadavky .....                               | 34        |
| B.2.7 Aplikační poznámky .....                                      | 35        |
| B.2.8 Zdůvodnění .....                                              | 35        |
| <b>Příloha C (normativní) Specifikace bezpečnostních cílů .....</b> | <b>36</b> |
| C.1 Přehled .....                                                   | 36        |
| C.2 Obsah bezpečnostního cíle .....                                 | 36        |
| C.2.1 Obsah a prezentace .....                                      | 36        |
| C.2.2 Úvod ST .....                                                 | 36        |
| C.2.3 Popis TOE .....                                               | 37        |
| C.2.4 Bezpečnostní prostředí TOE .....                              | 38        |
| C.2.5 Bezpečnostní cíle .....                                       | 38        |
| C.2.6 IT bezpečnostní požadavky .....                               | 38        |
| C.2.7 Specifikace shrnutí TOE .....                                 | 39        |
| C.2.8 Nároky PP .....                                               | 40        |
| C.2.9 Zdůvodnění .....                                              | 41        |
| <b>Příloha D (informativní) Bibliografie .....</b>                  | <b>42</b> |

|                                                       | Strana |
|-------------------------------------------------------|--------|
| Seznam obrázků                                        |        |
| Obrázek 3.1 – Kontext hodnocení .....                 | 11     |
| Obrázek 4.1 – Bezpečnostní pojmy a vztahy .....       | 13     |
| Obrázek 4.2 – Pojmy hodnocení a vztahy .....          | 14     |
| Obrázek 4.3 – Vývojový model TOE .....                | 16     |
| Obrázek 4.4 – Proces hodnocení TOE .....              | 17     |
| Obrázek 4.5 – Odvození požadavků a specifikací .....  | 20     |
| Obrázek 4.6 – Organizace a konstrukce požadavků ..... | 24     |
| Obrázek 4.7 – Použití bezpečnostních požadavků .....  | 26     |
| Obrázek 5.1 – Výsledky hodnocení .....                | 29     |
| Obrázek 5.2 – Použití výsledků hodnocení TOE .....    | 32     |
| Obrázek B.1 – Obsah Profilu ochrany .....             | 38     |
| Obrázek C.1 – Obsah Bezpečnostního cíle .....         | 44     |
| Seznam tabulek                                        |        |
| Tabulka 3.1 Schéma použití CC .....                   | 17     |

