25. számú Ajánlása

Magyar Informatikai Biztonsági Ajánlások (MIBA)

25/2.
Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)

25/2-1. segédlet
Modell és Folyamatok

1.0 verzió

2008. június
Közigazgatási Informatikai Bizottság
25. számú Ajánlása

Készült a
Miniszterelnöki Hivatal megbízásából

Összeállította:
Balázs István

Közreműködött:
Balázs István,
Staub Klára,
Szabó István

# TARTALOMJEGYZÉK

1. **BEVEZETÉS** ........................................................................................................ 5  
   1.1 ELŐZMÉNYEK ÉS ALKALMAZÁSI TERÜLET ............................................. 5  
   1.2 JELEN DOKUMENTUM CÉLJA ÉS FELÉPÍTÉSE ................................ 6  
   1.3 KAPCSOLÓDÓ DOKUMENTUMOK ................................................................. 6  

2. **FEJEZET AZ INFORMATIKA BIZTONSÁG TECHNOLÓGIAI ÉRTÉKELÉSÉNEK ALAPELVEI** ........................................................................................................ 7  
   2.1 A BIZTONSÁGI KÖVETELMÉNYEK CSOPORTOSÍTÁSA ......................... 7  
   2.2 AZ ELLENINTÉZKEDÉSEK CSOPORTOSÍTÁSA ........................................... 8  
   2.3 AZ INFORMATIKAI BIZTONSÁG ÉRTÉKELÉSE ......................................... 8  
   2.4 BIZTONSÁGI ELŐIRÁNYZAT ........................................................................ 11  
   2.5 A BIZTONSÁGI ÉRTÉKELÉS ÁLTALÁNOS ELVEI ......................................... 11  
      2.5.1 Az értékelési módszertan alkalmazási területe ........................................ 12  
      2.5.2 Az értékelési módszertan általános elvei ............................................... 12  
      2.5.3 Feltételek, feltételezések ......................................................................... 14  
   2.6 TANÚSÍTÁS ........................................................................................................ 15  

3. **FEJEZET A SÉMA RÉSZTEVŐI ÉS ÁLTALÁNOS FELELŐSSÉGÜK** ............. 16  
   3.1 MEGBÍZÓ ........................................................................................................... 16  
   3.2 FEJLESZTŐ ......................................................................................................... 17  
   3.3 ÉRTÉKELŐ .......................................................................................................... 17  
   3.4 TANÚSÍTÓ .......................................................................................................... 18  

4. **FEJEZET AZ INFORMATIKA BIZTONSÁG ÉRTÉKELÉS FOLYAMATA** ...... 19  
   4.1 AZ ÉRTÉKELÉS ELŐKÉSZÜLETI SZAKASZA ................................................ 19  
      4.1.1 Az értékelést megalapozó konzultációk ....................................................... 19  
      4.1.2 Biztonsági előirányzat ................................................................................. 20  
      4.1.3 Az értékelésre átadandó fejlesztői bizonyítékok ........................................... 20  
      4.1.4 A sikeres értékelés esélyének felmérése (megvalósíthatósági tanulmány) .... 22  
      4.1.5 Belépés a sémába ......................................................................................... 23  
   4.2. AZ ÉRTÉKELÉS LEBONYOLÍTÁSI SZAKASZA ............................................ 24  
   4.3. AZ ÉRTÉKELÉS KÖVETKEZTETÉSI SZAKASZA ......................................... 26  

5. **FEJEZET AZ INFORMATIKA BIZTONSÁG TANÚSÍTÁSI FOLYAMATA** ...... 27  
   5.1 AZ ÉRTÉKELÉSI FOLYAMAT SZAKMAI FELÜGYELETE ................................ 27  
   5.2 A TANÚSÍTÁS DÖNTÉSI SZAKASZA ................................................................. 28  
   5.3. A KIBOCSÁTOTT TANÚSÍTVÁNYOK ................................................................. 30  

6. **FEJEZET A SÉMÁBAN RÉSZTEVŐI FELADATAI** ........................................ 31  
   6.1 FELADATOK AZ ÉRTÉKELÉS ELŐKÉSZÜLETI SZAKASZÁBAN .................... 31  
   6.2 FELADATOK AZ ÉRTÉKELÉS LEBONYOLÍTÁSI SZAKASZÁBAN .................. 32  
   6.3 FELADATOK AZ ÉRTÉKELÉS KÖVETKEZTETÉSI SZAKASZÁBAN ............... 33  
   6.4 FELADATOK AZ ÉRTÉKELÉSI ÉS TANÚSÍTÁSI FOLYAMAT LEZÁRÁSÁT KÖVETŐEN .......................................................... 33  

7. **MELLÉKLETEK** ................................................................................................... 34  
   7.1 A BIZTONSÁGI ELŐIRÁNYZAT FELÉPÍTÉSE ÉS TARTALMA ........................ 34
7.1.1 A biztonsági előírások bevezetése ...................................................... 35
7.1.2 Az értékelés tárgya leírása .................................................................. 35
7.1.3 Az értékelés tárgya biztonsági környezete ........................................... 35
7.1.4 Biztonsági célok ..................................................................................... 36
7.1.5 Az informatikai biztonság követelményei ............................................. 36
7.1.6 Az értékelés tárgya összefoglaló előírása ............................................ 37
7.1.7 Védelmi profil nyilatkozatok .................................................................. 38
7.1.8 Indoklás ................................................................................................. 38

7.2 AZ ÉRTÉKELÉSI JELENTÉS FELÉPÍTÉSE ÉS TARTALMA ......................... 40
7.2.1 Az értékelés tárgyának áttekintése ......................................................... 40
7.2.2 Az értékelés tárgyának szerkezeti leírása .............................................. 40
7.2.3 Az értékelés jellemzése .......................................................................... 40
7.2.4 Az értékelés eredményei ...................................................................... 41
7.2.5 (Általános értékelési) Határozat ............................................................. 41
7.2.6 Indoklás .................................................................................................. 41
7.2.7 Javaslatok .............................................................................................. 41
7.2.8 Az értékeléshez felhasznált bizonyítékok .............................................. 41
7.2.9 A tanúsított termékek listájába javasolt szöveg .................................... 42
7.2.10 Észrevételezési jelentések és határozatok ........................................... 42
7.2.11 Rövidítések .......................................................................................... 42
7.2.12 Fogalmak .............................................................................................. 42
7.2.13 Biztonsági előírások ............................................................................. 42

7.3 A TANÚSÍTÁSI JELENTÉS TARTALMA ...................................................... 43
7.3.1 Összefoglaló .......................................................................................... 43
7.3.2 Azonosítás ............................................................................................. 44
7.3.3 Biztonsági szabályzat .......................................................................... 44
7.3.4 Feltételezések és hatókör .................................................................... 44
7.3.5 Szerkezeti leírás .................................................................................... 45
7.3.6 Dokumentáció ........................................................................................ 45
7.3.7 Az informatikai termék vagy rendszer tesztelése .................................. 45
7.3.8 Az értékelés konfiguráció ................................................................... 46
7.3.9 Az értékelés eredményei ...................................................................... 46
7.3.10 Értékelési megjegyzések és javaslatok ............................................... 46
7.3.11 Mellékletek .......................................................................................... 46
7.3.12 Biztonsági előírások .......................................................................... 47
7.3.13 Fogalmak és rövidítések .................................................................. 47
7.3.14 Felhasznált dokumentumok ................................................................. 47
7.3.15 Biztonsági előírások .......................................................................... 47

7.4 A MIBÉTS KERETÉBEN KIADOTT TANÚSÍTVÁNYOK ......................... 48
7.4.1 Informatikai termék értékeléséhez kapcsolódó MIBÉTS tanúsítványok .... 48
7.4.2 Kiegészítő nyilatkozat és sémajelzés informatikai termék esetén ........... 48
7.4.3 Informatikai rendszer értékeléséhez kapcsolódó MIBÉTS tanúsítványok .... 49
7.4.4 Kiegészítő nyilatkozat és sémajelzés informatikai rendszer esetén .......... 49

7.5 A MIBÉTS SÉMA JELZÉSE (LOGO) ......................................................... 51

HIVATKOZÁSOK .............................................................................................. 52
RÖVIDÍTÉSEK JEGYZÉKE .............................................................................. 53
MEGHATÁROZÁSOK ....................................................................................... 54
1. BEVEZETÉS

1.1 ELŐZMÉNYEK ÉS ALKALMAZÁSI TERÜLET

A Közigazgatási Informatikai Bizottság által kiadott Magyar Informatikai Biztonsági Ajánlások (MIBA) keretében két általános módszertani ajánlás készült, egy szervezeti-irányítási (MIBIK) és egy technológia-biztonsági (MIBÉTS). Mindkettő a biztonságos informatikai rendszerek kialakítását és fenntartását kívánják segíteni:

- a MIBIK (Magyar Informatikai Biztonsági Irányítási Keretrendszer) a szervezeti/irányítási szemléletet és szaktudást igénylő feladatokban,
- a MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma) pedig a technológiai szemléletet és szaktudást igénylő feladatokban.

A két ajánlás egymást kiegészítve és erősítve támogatást nyújt a rendszerfejlesztési életciklus valamennyi szakaszában a biztonság megtervezéséhez, megvalósításához, értékeléséhez és fenntartásához.

A MIBÉTS célja informatikai termékekre és rendszerekre irányuló, független, nemzetközi módszertanon alapuló értékelési és tanúsítási rendszer kialakítása, mely segíti:

- mind a felhasználókat, beszerzőket a felkínált informatikai termékek és rendszerek biztonsági szintjének megalapozott megítélésében, a rendszerek biztonságos üzemeltetési feltételeinek kialakításában;
- mind a fejlesztőket, gyártókat, forgalmazókat termékeik és rendszereik biztonságára vonatkozó állításait független igazolásában.

A séma a [3] nemzetközi szabványban meghatározott értékelési módszertan honosítása mellett szervezeti és eljárásbeli keretet ad a Magyarországon belül végrehajtott technológiai értékelések számára, beleértve az értékeléseket végző vizsgáló laboratóriumok (értékelő szervezetek) és tanúsító szervezetek feladatleírását, valamint a javasolt technikák és eljárások meghatározását is.
1.2 JELEN DOKUMENTUM CÉLJA ÉS FELÉPÍTÉSE

Jelen dokumentum a MIBÉTS segédlet sorozatának első eleme.
Célja egy általános modell felállítása a MIBÉTS számára.
A 2. fejezet a séma keretében megvalósított, informatikai termékekre vagy rendszerekre irányuló, technológiai szempontú biztonsági értékelésekre és tanúsításokra vonatkozó alapfogalmakat és alapelveket rögzíti.
A 3. fejezet a séma különböző résztvevőit azonosítja, meghatározva sémán belüli szerepüket.
A 4. és 5. fejezet a sémán belül megvalósítható két fő folyamatot – a biztonsági értékelést és az értékelés eredményének tanúsítását – írja le. Ezzel minden érintett résztvevőnek szóló összképet ad a sémán belüli értékelésekről és azok tanúsításáról. /A folyamatok során alkalmazandó módszertani kérdéseket más MIBÉTS segédletek részletezik./
A 6. fejezet a sémát résztvevőinek feladatait tekinti át. /A feladatok részletezését más MIBÉTS segédletek fejtik ki./
A 7. fejezet mellékletei az értékelés és tanúsítás folyamatában elkészítendő alapdokumentumok tartalmát határozzák meg:
  • a 7.1 alfejezet a biztonsági előirányzatok tartalmát és felépítését szabja meg,
  • a 7.2 alfejezet az értékelési jelentések felépítését és tartalmát adja meg,
  • a 7.3 alfejezet a tanúsítási jelentések felépítését és tartalmát határozza meg,
  • a 7.4 alfejezet a MIBÉTS keretében kiadott tanúsítványokra vonatkozó tartalmi és formai elvárásokat tartalmazza, végül
  • a 7.5 alfejezet a MIBÉTS sémajelét (logo) mutatja be.
A segédletet a hivatkozások és rövidítések jegyzéke, valamint fogalom meghatározások zárják.

1.3 KAPCSOLÓDÓ DOKUMENTUMOK

A MIBA jelenlegi verziójához az alábbi segédletek készültek el:
  • 1. számú segédlet: Modell és folyamatok (jelen dokumentum)
  • 2. számú segédlet: Útmutató a megbízók számára
  • 3. számú segédlet: Útmutató a fejlesztők számára
  • 4. számú segédlet: Útmutató az értékelők számára
  • 5. számú segédlet: Értékelői módszertan

Magyar Informatikai Biztonsági Ajánlások
2. FEJEZET
AZ INFORMATIKA BIZTONSÁG TECHNOLÓGIAI ÉRTÉKELÉSÉNEK ALAPELVEI

Az alábbiak a MIBÉTS keretében megvalósított informatikai termékekre vagy rendszerekre irányuló, technológiai szempontú biztonsági értékelésekre és tanúsításokra vonatkozó alapfogalmakat és alapelveket rögzítik.

2.1 A BIZTONSÁGI KÖVETELMÉNYEK CSOPORTOSÍTÁSA

Az informatikai termékek és rendszerek tulajdonosai, működtetői legtöbbször elvárják, hogy termékük vagy rendszerük biztosan tegye lehetővé a felhasználók számára mindazt, amire szükségük van. Közismert technikák léteznek informatikai termékek és rendszerek olyan meghatározására, tervezésére és vizsgálatára (tesztelésére), hogy azok lehetővé tegyék felhasználói számára az elvártat (funkcionalitás).

Néha azonban az informatikai termékek és rendszerek tulajdonosai inkább arra nézve kívánnak bizonyosságot, hogy termékük vagy rendszerük ne engedjen meg semmi olyat felhasználóinak, amit nem kellene. Az ilyenfajta követelményeket gyakran biztonsági követelmények mondják. A fejlesztők és a felhasználók a biztonsági követelményeket sokkal kevésbé értik, mint az egyéb követelményeket, s másként is kell meghatározni, tervezni és vizsgálni (tesztelni).

A MIBÉTS keretén belül az informatikai biztonság a következő biztosítását jelenti:

- bizalmasság /az adatok megvédése attól, hogy illetéknelenek megismerjék tartalmukat/,
- sértetlenség /az adatok megvédése illetéklenek személyek általi módosítástól, és annak biztosítása, hogy az adatok pontosan megfeleljenek a valóságnak/,
- rendelkezésre állás /az adatok megvédése jogosulatlan vagy véletlen elvesztéstől, megsemmisítéstől, elrontástól/,
- hitelesség /egy entitás tulajdonságát igazoló állapot, melyet bizonyítani képes önmaga vagy egy másik entitás közreműködésével/

A fentiek bármelyike vagy mindegyike fontos szerepet kaphat bizonyos esetekben.
2.2 AZ ELLENINTÉZKEDÉSEK CSOPORTOSÍTÁSA

Egy informatikai termék vagy rendszer a biztonsági követelményeket az alábbi ellenintézkedések megvalósításával juttathatja érvényre:

- megakadályozás,
- észlelés,
- helyreállítás,
- elszámoltathatóság.

A megakadályozás a felhasználói kérések kiértékelés ét, s ezek közül a jogosulatlanok visszautasítását jelenti.

Az észlelés jelentése: a jogosulatlan tevékenységek észlelése, s ennek eredményeképp megfelelő cselekvés kiváltása.

A helyreállítás a nem kívánt tevékenységek és események meg nem történtté tételel, a korábbi állapot visszaállítását jelenti az erre a célra szolgáló eszközökkel.

Elszámoltathatóságról beszélünk akkor, ha a naplózás az adott egyed tevékenységeit egyértelműen az adott egyed tevékenységeiként rögzíti.

2.3 AZ INFORMATIKAI BIZTONSÁG ÉRTÉKELÉSE

Az informatikai termékek és rendszerek tulajdonosainak gyakran van szükségük arra vonatkozó bizonyosságra, hogy termékük vagy rendszerük képes a biztonsági követelményeket érvényesíteni. Ugyanakkor a legtöbb tulajdonos nem szívesen fogadja el közvetlenül a termék vagy rendszer fejlesztői erre vonatkozó garanciáit, mivel a fejlesztők saját eredményeikkel szemben nem elfogulatlanok.

Erre a problémára két megoldási lehetőség kínálkozik:

- vagy a szervezeten belül az informatikai biztonságért felelős részleg vállalja fel a biztonsági funkciók értékelését,
- vagy egy megbízható harmadik fél értékelni az adott termék vagy rendszer biztonságát.

A MIBÉTS a megbízható harmadik felek által végzett biztonsági értékelés számára biztosít keretet.

A megfelelő biztonsági tulajdonságú informatikai termékek kiválasztásáért felelős személyek gyakran kerülnek nehéz helyzetbe. Például egy adott termék erősségére és gyengeségére vonatkozó ismeretek hiánya a felesleges tulajdonságokra kidobott...
költségekkel járhat, vagy a még rosszabb esetben a biztonsági kockázatok növekedését okozhatják.

A biztonsági követelmények kielégítése céljából beszerzett termékek esetén további problémákat okozhatnak az alábbiak:

- a termék biztonságára vonatkozó állítások nem igazolhatók,
- a biztonságára vonatkozó állításokat olyan formában fogalmazzák meg, ami megnehezíti az egymással versengő termékek összehasonlítását,
- a termékeket nem támogatják megfelelő dokumentációk,
- a termékek olyan módon kapcsolódhatnak más termékekhez, mely sebezhetőséget eredményez,
- a termék potenciálisan megbízhatatlan forrásból származhat.

A MIBÉTS által támogatott értékelések megoldást nyújtanak a fenti problémákra. Az értékelés számára lehetővé tehetik a rendszer belső részleteinek megismerését anélkül, hogy nyilvánosságra hoznák azokat, mivel az értékelő csak vizsgálata eredményét hozza nyilvánosságra. Az értékelőben mindkét félnek meg kell bíznia: a tulajdonosnak (felhasználónak) abban, hogy mélyreható, alapos és hozzáértő munkát végez, a fejlesztőnek pedig abban, hogy a rendszer belsejének megismerésével nem fog visszaélni.

Az értékelések szabványosításából is nyilvánvaló előnyök származnak:

- a rendszer tulajdonosai meggyőződhetnek arról, hogy az értékelés megfelelő módon történt,
- a fejlesztők tudhatják, milyen támogatást kell adniuk az értékelőknek,
- az értékelések összehasonlíthatókká válnak.

Az értékelésre vonatkozó szabványokat értékelési követelményrendszernek nevezik. Az értékelési követelményrendszerek a biztonság két aspektusát határozhatják meg:

- milyen biztonsági tulajdonságok szükségesek a rendszerben (ezt a szempontot biztonsági funkcióknak hívják),
- a tulajdonságok hogyan elemezhetők és vizsgálhatók (ezt garanciának vagy bizalomnak nevezik).

Nem mindegyik követelményrendszer határozza meg a funkciók követelményeit. Amelyek megteszik ezt, azok egy választék-készletet adnak meg, s a funkciókhoz a rendszer releváns szükségletei alapján ebből választhatók ki.
Minden követelményrendszer meghatározza ugyanakkor a garanciát, s ezt a szigorúság és a költségesség növekvő szintjeiben fejezi ki. Ez lehetővé teszi a tulajdonosok számára, hogy megtalálhassák az értékelés költsége és megkövetelt szigorúsága közötti egyensúlyt.


A CEM a CC társdokumentuma. Célja azon tevékenységek részletes meghatározása és lefűzése, melyeket egy értékelőnek kell elvégeznie egy CC szerinti értékelés folyamán.

A CEM elsődlegesen az értékelők munkáját határozza meg, de ezzel más résztvevők is hasznos információkat nyerhetnek belőle, köztük a fejlesztők, az értékelés megbízói, a tanúsítók, valamint az értékelési eredmények közvetetélében és használatában érintett egyéb felek is.

A MIBÉTS az informatikai termékek és rendszerek biztonsági értékelési módszertanára a CEM egyszerűsített (honosított) változatát dolgozta ki és fogadja el. Összefoglalva a fentiakat, a MIBÉTS által elismert technológiai szempontú értékelési követelmények és módszertanok az alábbiak:

- CC, CEM
- CC, MIBÉTS értékelési módszertan /[7], mely a CEM egyszerűsített változata, hazai adaptációja/

A CC a korábbi észak-amerikai és európai követelményrendszer egységesítése érdekében végzett nemzetközi erősítésének az eredménye. A CC nemzetközi szabvánnyá vált [2], ami hozzájárul ahhoz, hogy az informatikai biztonsági értékelések világ szabványává váljanak. A CC (egy korábbi verziója) magyar szabvány is lett [1], s Magyarország csatlakozott a CCRA egyezményhez, melynek keretében tanúsítvány elfogadó státuszt nyert.

A CEM 1.0 verzióját (mely megegyezik a [3] nemzetközi szabvánnyal, s mely az EAL1 – EAL4 értékelési garancia szintekre vonatkozik) széles körben a CC módszertanának ismerik el.

A MIBÉTS elismeri az EAL1 - EAL4 értékelési garancia szintekre vonatkozó - a CCRA egyezmény tanúsítvány kibocsátó országaiban kiadott - CC tanúsítványokat.
A [7]-ben meghatározott értékelési módszertan a CEM három értékelési garancia szintjére /EAL2, EAL3, EAL4/ kidolgozott módszertan egyszerűsített változata, hazai adaptációja. Célja kettős:

- a hazai CC tanúsítvány kibocsátás szakmai előkészítése,
- költség-, idő- és egyéb erőforrás kínálók értékelési módszertan alkalmazási lehetőségének biztosítása olyan informatikai termékek és rendszerek esetében, ahol nincs CC értékelte alternatívát, vagy ahol a tanúsítványok nemzetközi elismerése nem szükséges.

Az ennek keretében kiadott tanúsítványok csak a MIBÉTS keretében érvényesek (más nemzeti sémák nem fogadják el automatikusan).

### 2.4 BIZTONSÁGI ELŐIRÁNYZAT

A MIBÉTS keretében egy informatikai termék vagy rendszer értékelése csak egy konkrétan meghatározott biztonsági előirányzathoz képest lehetséges.

A biztonsági előirányzat biztonsági követelmények és előírások olyan összessége, amelyet egy adott értékelés tárgya1 értékelésének alapjaként használnak. Tartalmazza az értékelés tárgya összetevő specifikációnját, a biztonsági követelményekkel és célokkal, valamint a mögötté esvel és indokok kifejtését együtt. Ez az alapja a sémában résztvevő felek közötti bármilyen olyan megegyezésnek, mely arról szól, hogy az értékelés tárgya milyen biztonságot nyújt.

A biztonsági előirányzat készítése az értékelés megbízójának a feladata. A megbízó a biztonsági előirányzat készítéséhez kikérheti az értékelő tanácsát.

### 2.5 A BIZTONSÁGI ÉRTÉKELÉS ÁLTALÁNOS ELVEI

Ez az alfejezet a MIBÉTS értékelési módszertan közös, általános elveit ismerteti. Az értékelési módszertan önmagában nem juttatja érvényre ezeket az elveket, ehhez az értékelésben résztvevő felekre vonatkozó feltételeknek és a módszertan megvalósítását szolgáló előírásoknak is hozzá kell járulniuk.

---

1 Értékelés tárgya: az informatikai termék vagy rendszer azon része, amely értékelésre kerül.
2.5.1 AZ ÉRTÉKELÉSI MÓDSZERTAN ALKALMAZÁSI TERÜLETE

Az értékelési folyamat az értékelés folyamán végrehajtandó tevékenységekből, valamint az értékelési módszertan teljesítéséhez szükséges fejlesztői és tanúsítói folyamatokból tevődik össze.

A MIBÉTS értékelési módszertan minden informatikai termékre és rendszerre alkalmazható, köztük elsősorban az üzletmenet- és biztonság-kritikus szoftvertermékekre.


2.5.2 AZ ÉRTÉKELÉSI MÓDSZERTAN ÁLTALÁNOS ELVEI

Az alábbiak a MIBÉTS értékelési módszertan általános elveit határozzák meg.

Az alkalmasság elve

Az alkalmazott értékelési tevékenységeknek alkalmaznak kell lenniük a garancia megcélzott szintjének eléréséhez.

Egy értékelésben valamennyi résztvevő félnek végre kell hajtania a tőle megkövetelt feladatokat olyan mértékű szigorússággal, amely megfelel a megcélzott értékelési garanciaszint iránymutatásainak és követelményeinek.

A pártatlanság elve

Minden értékelési tevékenységnek elfogultság mentesnek kell lennie.

Az értékelésben résztvevők egyikének sem szabad elfogultnak lennie sem az éppen értékel informatikai termék vagy rendszer mellett, sem ellene. A megfelelő szakmai felügyeletnek (kiegészülve az érdekek konfliktusát kiküszöbölő előírásokkal) bármilyen fennmaradó elfogultságot elfogadható szintre kell csökkentenie. Az érdekek konfliktusát kiküszöbölő előírásokban részletesen meg kell határozni az érdekek elfogadhatatlan konfliktusát.
Az objektivitás elve

Az értékelési eredményeket úgy kell kialakítani, hogy azok csak minimálisan tartalmazzanak szubjektív megítéléseket, vagy személyes véleményt. Az értékelést végző személyek nem lehetnek teljesen mentesek személyes véleményüktől, vagy szubjektív megítélésektől. A megfelelő szakmai felügyeletnek jól definiált módszertanon és értelmezéseken alapulva elfogadható szintre kell csökkentenie ezen szubjektív véleményeket és megítéléseket.

A megismételhetőség elve

Ugyanazon termék vagy rendszer megismételt értékelése ugyanazon értékelők által, azonos követelményekre vonatkozóan, alapvetően az eredeti értékelési eredményeket szolgáltassa. Az értékelési tevékenység minden tevékenységi elemének ugyanazt az eredményt kell adnia, függetlenül attól, hogy mikor végezték az adott tevékenységi elemet. Az értékelés során a követelményeket egységesen kell értelmezni.

Az újraelállíthatóság elve

Az ugyanarra az informatikai termékre vagy rendszerre vonatkozó, azonos követelmények szerint és ugyanazon fejlesztői bizonyíték mellett megismételt értékelésnek ugyanazokra az eredményekre kell vezetnie. Az értékelési tevékenység minden tevékenységi elemének ugyanazt az eredményt kell adnia, függetlenül attól, hogy ki végezte az adott tevékenységi elemet. Az értékelés során a követelményeket egységesen kell értelmezni.
/Az újraelállíthatóság abban különbözik a megismételhetőségtől, hogy az utóbbi az értékelők közötti következetességgel kapcsolatos (egymástól függetlenül ugyanarra az eredményre jutna két különböző értékelő), míg az előbbi az ugyanazon értékelők eredményei közötti következetességgel áll kapcsolatban (ugyanaz az értékelő a korábbival megegyező eredményére jutna egy később megismételt értékelés esetén is)./ 

Az eredmények helyességének elve

Az értékelés eredményének teljesnek és szakmailag hibátlanakkal kell lennie. Az értékelés eredményének tükrözője kell az értékelő informatikai termék vagy rendszer helyes megítélését és pontos szakmai felbecsülését. Az értékelési folyamatot és az eredményeket szakmailag felül kell vizsgálni, hogy az értékelési módszertanra vonatkozó előírások kielégítése biztosított legyen.
2.5.3 FELTÉTELEK, FELTÉTELEZÉSEK

A fent ismertetett általános elvek több, az értékelés környezetére és az összes résztvevő fél tevékenységére vonatkozó feltételeken, feltételezésen alapulnak. Az elvek függenek ezen feltételezések érvényességétől.

A költség-hatékonyság feltétele

Egy értékelés értékének ellensúlyoznia kell az összes érdekelő fél által befektetett időt, erőforrásokat és pénzt.

Az informatikai termékek és rendszerek értékelésében folyamatosan egyensúlyt kell tartani annak értéke és a hozzá szükséges idő- és erőforrás felhasználás között.

A módszertan fejlődésének feltétele

A környezeti és műszaki tényezők változásának az értékelésre gyakorolt hatását jól meghatározott és következetes módon le kell képezni az értékelés módszertanába.

A környezet változása és a műszaki-technológiai fejlődés hatással lehet az informatikai termékek és rendszerek értékelésénél használt módszerek hatékonyságára. Az értékelés módszertanának figyelembe kell vennie a környezet változását, egyúttal alkalmazhatónak kell lennie a fejlődő technológiákra is.

Az ismételt felhasználhatóság feltétele

Egy értékelésnek hatékonyan fel kell használnia a korábbi értékelések eredményeit.

Egy informatikai termék vagy rendszer értelmezési eredményei, valamint az értékelés folyamán keletkezett értelmezések egy későbbi értékelésnél is hasznosíthatók, azonos feltételek érvényessége esetén. Az ismételt felhasználhatóság különösen hasznos az olyan értékeléseknél, amelyeknél az értékelő informatikai terméket vagy rendszert egy másik termékbe vagy rendszerbe integrálják. Az értelmezési eredmények tartalmának és felépítésének, valamint az értelmezési módszertannak támogatnia kell az ismételt felhasználhatóságot.

Szaknyelv használatának feltételezése

Az értékelésben résztvevő feleknek közös szakmai nyelvet kell használniuk.

Az értelmezési eredmények egységes szakmai minőségének biztosítása, valamint az értékelés során a kommunikáció és az értelmezések egységes bázisának megteremtése
érdekében az összes érdekelt félnek közös szakmai nyelvet kell beszélnie, s az egyes szakkifejezéseket azonosan kell értelmeznie a gyakorlatban.

2.6 TANÚSÍTÁS

A MIBÉTS keretében a tanúsítás célja az értékelési eredmények érvényességének független megerősítése, s így ezen eredmények összehasonlíthatóságának a biztosítása az összes értékelő (vizsgálólaboratórium) valamennyi értékelési eredményével.

A tanúsítási folyamat nem más, mint az értékelés eredményeinek független vizsgálata, amely a végső jóváhagyást kifejző tanúsítvány megadásához vezet.

Egy tanúsítás egyszerre erősíti meg az alábbiakat:

- az értékelés tárgya megfelel biztonsági előirányzatának,
- az értékelésre a séma szabályainak és eljárásainak megfelelően került sor.

A tanúsítás más tekintetben nem szentesíti az értékelés tárgyát. Nem következik belőle az sem, hogy az értékelés tárgya garantáltan mentes a kihasználható sebezhetőségektől. Kis valószínűséggel (annál kisebb, minél magasabb a garanciális szint) észrevétlenül megmaradhat néhány kihasználható sebezhetőség.
3. FEJEZET
A SÉMA RÉSZTVEVŐI ÉS ÁLTALÁNOS FELELŐSSÉGÜK

A MIBÉTS az alábbi szerepeket különbözteti meg:

- megbízó,
- fejlesztő,
- értékelő és
- tanúsító.

Az értékelési eljárásban minden résztvevő meghatározott felelősséggel bír.

3.1 MEGBÍZÓ

Egy informatikai biztonsági értékelés megbízója egy informatikai termék vagy rendszer biztonsági értékelésének kérelmezője.

Az informatikai termék vagy rendszer és a megbízó közötti kapcsolat sokféle lehet, a termék vagy rendszer természetétől és az értékelés körülményeitől függően. Gyakran az értékelés megbízója maga az adott termék vagy rendszer fejlesztője. Egy értékelés megbízója ugyanakkor lehet egy informatikai termék hozzáadott értéket teremtő viszonteladója, vagy az adott termékét kulcsfontosságú összetevőként tartalmazó informatikai rendszer vásárlásában, beszerzésében érdekelt szervezet, személy is. Megbízó lehet egy olyan független fél is, aki egy szerződés követelményeinek teljesítése érdekében egy informatikai rendszert fejleszt vagy integrál. Konzorciumok, kereskedelmi társulások is kijelölhetnek egy szerződő felet egy értékelés megbízójaként.

Azokban az esetekben, amikor a megbízó nem az informatikai termék vagy rendszer fejlesztője, a megbízónak el kell nyernie a fejlesztő együttműködő támogatását ahhoz, hogy az értékelő (vizsgálólaboratórium) számára biztosíthasson tudja az értékelés teljes és ellentmondásmentes végrehajtásához szükséges műszaki anyagokat és fejlesztői bizonyítékokat. Ezen dokumentumok biztosításának konkrét részleteit a megbízó és a fejlesztő szerződésben rögzítheti.
A megbízó általános felelőssége az alábbiakat foglalja magában:

1. az értékelés kereteit meghatározó döntések meghozatala,
2. az értékelés jogi előkészítése (a szükséges megállapodások, szerződések kezdeményezése és megkötése),
3. az értékeléshez szükséges támogatás biztosítása,
4. a tanúsítás eredményeinek korrekt felhasználása,
5. az értékelés és tanúsítás költségeinek vállalása.

3.2 FEJLESZTŐ

A fejlesztő általános felelőssége az alábbiakat foglalja magában:

1. az értékeléshez szükséges fejlesztői bizonyítékok elkészítésében való közreműködés,
2. az értékelés szakmai támogatása.

A fejlesztő alatt azt a szervezetet (vagy szervezeteket) értjük, amely előállította az értékelés tárgyát (vagy annak egyes összetevőit). Amennyiben nem a fejlesztő az értékelés megbízója, akkor megállapodásra kell jutnia a megbízóval a fenti kötelezettségei teljesítéséről.

Bizonyos körülmények esetén több fejlesztő is érintett lehet egy értékelésben, például alvállalkozók bevonása esetén. Ilyenkor még inkább szükség van, hogy a megbízó valamennyi fejlesztő együttműködő támogatását elnyerje.

3.3 ÉRTÉKELŐ

Amíg a MIBÉTS keretén belül fejlesztő és megbízó elvileg bárki lehet, értékelő nem. Annak, hogy egy szervezet értékelővé válhasson a sémában, az alábbi előfeltételei vannak:

- az értékelő egy olyan szervezet, melynek a [10] szabvány követelményeinek való megfelelőségét a NAT akkreditálási okiratban ismerte el, vizsgáló-laboratórium kategóriában,
- a vizsgáló-laboratóriumra akkreditált műszaki terület tartalmazza az alábbiakat:
  - [1] vagy [2] (a modell), és
- az értékelő szervezet felkerült a MIBÉTS séma nyilvántartásába, az informatikai biztonsági értékelésekre felhatalmazott (jóváhagyott) laboratóriumok (értékelő szervezetek) listájára.
Az értékelő általános felelőssége az alábbiakat foglalja magában:

1. az értékelésre átadandó fejlesztői bizonyítékok átvétele és megfelelő kezelése,
2. az értékelési módszertan által megkövetelt értékelési tevékenységek végrehajtása,
3. a szükséges értékelési támogatás kérése, fogadása (pl. a fejlesztő általi képzés, a tanúsító értelmezései),
4. a tanúsításra átadandók elkészítése,
5. a tanúsító szervezetet az értékelés során képviselő átvizsgáló számára az értékelői általános határozat és minden más közbenső értékelői határozat dokumentálása és indoklása,
6. a MIBÉTS általános elveinek és az értékelésre vonatkozó előírásainak való megfelelés.

3.4 TANÚSÍTÓ

Amíg a MIBÉTS keretén belül fejlesztő és megbízó elvileg bárki lehet, tanúsító nem. Annak, hogy egy szervezet tanúsítóvá válhasson a sémába, az alábbi előfeltételei vannak:

- a tanúsító egy olyan szervezet, melynek a [11] szabvány követelményeinek való megfelelőségét a NAT akkreditálási okiratban ismerte el, terméktanúsítás kategóriában,
- a terméktanúsításra akkreditált műszaki terület tartalmazza az alábbiakat:
  - [1] vagy [2] (a modell), és
- az értékelő szervezet felkerült a MIBÉTS séma nyilvántartásában, az informatikai biztonsági tanúsításra felhatalmazott (jóváhagyott) tanúsító szervezetek listájára.

A tanúsító általános felelőssége az alábbiakat foglalja magában:

1. az értékelések ellenőrzése (az értékeléshez kirendelt átvizsgálón keresztül),
2. a tanúsításra átadandók átvétele és megfelelő kezelése,
3. azoknak a feltételeknek a megteremtése, melyek biztosítják, hogy az értékelés megfeleljen az értékelés általános elveinek,
4. az értékelések támogatása előírások készítésével, a séma követelmények értelmezésével és iránymutatással,
5. az értékelői általános határozat jóváhagyása vagy elvetése,
6. a tanúsítási jelentés és tanúsítvány elkészítése.
4. FEJEZET
AZ INFORMATIKA BIZTONSÁGI ÉRTÉKELÉS FOLYAMATA

Az értékelési folyamat három szakaszra osztható, melyek át is fedhetik egymást:

• előkészület /ebben a szakaszban teremtik meg a kezdeti kapcsolatot a megbízó és az
  értékelő között/, 
• lebonyolítás /ebben a szakaszban hajtják végre az értékelést/, 
• következtetés /ebben a szakaszban adják át az értékelési eredményeket/.

4.1 AZ ÉRTÉKELÉS ELŐKÉSZÜLETI SZAKASZA

Az értékelés első, előkészületi szakaszból a tevékenységek többsége a megbízó és az
értékelő szervezet között zajlik. A megbízó felelőssége a biztonsági előirányzat, valamint
az értékelés tárgyát képező informatikai termék vagy rendszer átadása.

Egy értékelés tárgya nagyon különböző összetevőkből állhat. Egy informatika terméknek
hardver, formver és szoftver komponensei lehetnek, illetve ezek bármilyen kombinációja
szóba jöhet. Egy informatikai rendszer különböző informatikai termék közül áll, némelyeket
ezek közül esetleg már értékeltek is. Az értékelő szervezet számára biztosítani kell a
fejlesztés során keletkezett valamennyi, a biztonságot érintő információt és dokumentációt.
A megbízónak biztosítania kell, hogy egyezményes keretek között, az értékelő
megkaphasson a sikeres értékeléshoz szükséges minden lényeges dokumentációt.

4.1.1 AZ ÉRTÉKELÉST MEGALAPOZÓ KONZULTÁCIÓK

A MIBÉTS nem korlátozza az értékelés előkészületi szakaszában folytatott konzultációk
hatókörét, ez a megbízó, a potenciális értékelő szervezet(ek), illetve egyéb tanácsadók
közötti megegyezés kérdése. Ebben a szakaszban törekedni kell az alábbi két szempont
közötti elfogadható egyensúlyra:

• az értékelésre készülő értékelő szervezetnek szem előtt kell tartania az akkreditálása
  során vállalt pártatlanágra, függetlenségre és fedhetetlenségére vonatkozó alábbi
  feltételeket:
• biztosítania kell, hogy vezetősége és személyzete mentes legyen mindennemű illetéktelen belső vagy külső kereskedelmi, pénzügyi és más nyomástól és befolyástól, amelyek hátrányosan befolyásolhatnának munkájuk minőségét;
• garantálnia kell, hogy elkerül minden olyan tevékenységben való részvételt, amely csökkentene a bizalmat felkészültségében, pártatlanságában, ítéletében és működésének fedhetetlenségében;
• a MIBÉTS által meghatározott egyszerűsített és költség-hatékony értékelési módszertan [7] lehetővé teszi az értékelő szervezetnek, hogy egyes fejlesztői bizonyítékokat a fejlesztővel és a megbízóval együttműködésben közösen készítsen el, az értékelés előkészületi szakaszában.

Minden értékelésnél az értékelő szervezetnek tájékoztatnia kell a tanúsító szervezetet az értékelés szempontjából jelentősséggel bíró konzultációs tevékenységeiről, amely az értékelési folyamat szakmai felügyelete (lásd 5.1 alfejezet) során kitér erre a kérdéskörre is.

Az értékelést megalapozó konzultációk során az értékelő szervezet konzultációs tevékenysége, valamint az értékelésre átadandó bizonyítékok összeállításában és elkészítésében játszott szerepe nem veszélyeztetheti a pártatlanságra, függetlenségre és fedhetetlenségére vonatkozó feltételek jövőbeli kimutathatóságát.

4.1.2 BIZTONSÁGI ELŐIRÁNYZAT

A biztonsági előirányzat egyrészt azokat a biztonsági funkciókat határozza meg, amelyeknek való megfelelését az értékelésnek igazolnia kell, másrészt a termék vagy rendszer tervezett (feltételezett) működtetési környezetét írja le.

A biztonsági előirányzatot (vagy annak tervezetét, kiinduló verzióját) a megbízó biztosítja, s ebben felsorolja az informatikai termékre vagy rendszerre vonatkozó nyilatkozatait is.

A MIBÉTS keretében a biztonsági előirányzatot a Közös szempontoknak mindenben megfelelő formában és tartalommal kell összeállítani. A biztonsági előirányzatra megkövetelt tartalmi és formai elvárásokat a 7.1 alfejezet ismerteti.

4.1.3 AZ ÉRTÉKELÉSRE ÁTADANDÓ FEJLESZTŐI BIZONYÍTÉKOK

Egy informatikai biztonsági értékelésre átadandó bizonyítékok (röviden átadandók) tipikusan hardver-, förmer-, szoftver- vagy egyéb más műszaki dokumentáció, melyet általában a termékek fejlesztése során hoztak létre. Egy értékelés megbízójának megfelelő időben gondoskodnia kell az értékeléshez szükséges átadandók biztosítására. A megbízó és
az értékelő szervezet között megkötendő megfelelő szerződésben rögzíteni kell a megbízó kötelezettségét az értékelésre átadandók biztosításáról.

Amennyiben több informatikai termékből álló rendszer az értékelés tárgya, előfordulhat, hogy egyes termékeket korábban már értékeltek, s a MIBÉTS által elfogadott tanúsítvánnyal, valamint az ennek kibocsátását megalapozó értékelési eredményekkel rendelkezik. Ilyen esetben a megbízónak az értékelő szervezettel kötött szerződésében azt is vállalnia kell, hogy megszerzi a korábbi értékelési eredmények megismerésére való felhatalmazásokat. A korábbi értékelési eredmények idő- és egyéb erőforrás-megtakarítást eredményező hasznosításához az alábbi átadandókhoz való hozzáférést kell a megbízónak az értékelő szervezet számára biztosítania:

- A Közös szempontok szerint a CCRA megállapodás hatálya alatt kibocsátott tanúsítvánnyal rendelkező informatikai termék esetén:
  - a tesztelésre alkalmas értékelés tárgya (maga a termék),
  - biztonsági előírások,
  - tanúsítási jelentés,
  - Common Criteria tanúsítvány.

- A MIBÉTS keretén belül kibocsátott tanúsítvánnyal rendelkező informatikai termék esetén:
  - a tesztelésre alkalmas értékelés tárgya (maga a termék),
  - biztonsági előírások,
  - értékelési jelentés,
  - tanúsítási jelentés,
  - MIBÉTS tanúsítvány.

A fenti dokumentációkon túl a megbízónak garantálnia kell, hogy az értékelő szervezet és a tanúsító szervezet minden üzleti titkot képező olyan információhoz is hozzáférhet, mely az értékeléshez és a tanúsításhoz szükséges. Ennek hiányában az értékelő szervezet esetleg nem lenne képes az értékelést elvégezni, a tanúsító szervezet pedig nem lenne képes tanúsítási jelentését megfogalmazni.
Az értékelő szervezetnek és a tanúsító szervezetnek ugyanakkor azt kell garantálnia, hogy jogosulatlanokkal semmi olyat nem közel, amely érzékeny vagy üzleti titkot tartalmazó információk kompromittálódásához vezethetne. Az értékelő szervezetnek azt is vállalnia kell, hogy az üzleti titkok természetének és tartalmának megfelelő szabályokat alkalmaz azok megvédésére.
A fent leírt kötelezettségeket a felek között kötött szerződésbe kell foglalni.

4.1.4 A SIKERES ÉRTÉKELÉS ESÉLYÉNEK FELMÉRÉSE
(MEGVALÓSÍTHATÓSÁGI TANULMÁNY)

Miután a megbízó az értékelésre átadandók ügyében megtette a szükséges lépéseket, egy értékelő szervezethez fordulhat az értékelés kezdeményezése céljából.
A MIBÉTS lehetőséget biztosít arra, hogy az értékelésre átadandó fejlesztői bizonyítékok közül a biztonsági előirányzatot, a többi bizonyíték átadása után, az értékelő szervezet aktív közreműködésével fejezze be a megbízót. Ilyen esetben is a megbízőé a végző felelősség arról, hogy:
- a véglegesített biztonsági előirányzat valóban azokat a biztonsági funkciókat tartalmazza, amelyeknek való megfelelést az értékelésnek majd igazolnia kell, valamint
- a véglegesített biztonsági előirányzat valóban a termék vagy rendszer tervezett (feltételezett) működtetési környezetét írja le.

A véglegesített biztonsági előirányzat és az átadott többi bizonyíték birtokában az értékelésre kiválasztott értékelő szervezet egy megvalósíthatósági tanulmányt készíti, melyben felméri a sikeres értékelés valószínűségét. Ennek legfontosabb elemeként áttekinti magát a biztonsági előirányzatot annak eldöntése érdekében, hogy az megfelelő szakmai alapot biztosít-e az értékeléshez. Ez az áttekintés csak informális, nem helyettesíti a későbbi értékelés során a biztonság előirányzatra elvégzendő ([7]-ben meghatározott) formális vizsgálati módszert. Az értékelő szervezet tájékoztatja a megbízót, ha bármilyen problémát talál, illetve olyan változásokat tanácsolhat, melyek az értékelés biztosabb megalapozásához szükségesek. Amennyiben a sikeres értékelés megvalósíthatónak tűnik, a választott értékelő szervezet ezt a megvalósíthatósági tanulmányban rögzíti.

A megvalósíthatósági tanulmány pozitív következtetése esetén az értékelő értékelési munkatervet készít a tervezett értékelési tevékenységek megnevezésével és rövid leírásával.
Az értékelési munkaterv tartalmazza az értékelésre átadandó fejlesztői bizonyítékok listáját, mely pontosítja (kiegészíti) az értékelésre átadandók körét.

Az értékelési munkaterv keretén belül, vagy egy önálló anyagban az értékelő értékelési ütemtervet is készít, mely az értékelési feladatok ütemezése mellett arra is kitér, mely hiányzó átadandók, mely időpontig biztosítandóak a megbízó részéről.

4.1.5 BELÉPÉS A SÉMÁBA

A tanúsító szervezet attól fogva kapcsolódik be az értékelés folyamatába, amikor egy megbízó, s az általa az értékelésre kiválasztott értékelő szervezet értesíti a tervezett értékelésről, s egy formális közös kérelmet nyújtanak be az értékelés MIBÉTS kereteibe való befogadására. A tanúsító szervezet mielőtt elfogadná a kérelmet, információkat kér a megbízótól és az értékelő szervezettől, köztük az alábbiakat:

- az értékelés tárgya leírását és biztonsági előírányzatát,
- értékelési munkaterv,
- értékelési ütemterv (amennyiben ezt az értékelési munkaterv nem tartalmazza).

Az értékelés formális sémába fogadása részeként a tanúsító szervezet áttekinti a megbízó és az értékelő szervezet által biztosított dokumentumokat, annak felmérése érdekében, hogy mindkét fél megfelelően felkészült-e a tervezett értékelésre. Ennek során találkozhatnak a megbízó és az értékelő szervezet kulcsszereplőivel annak biztosítása érdekében, hogy valamennyi fél számára csökkentsék az értékelési és tanúsítási folyamat sikertelenségének kockázatát.

A tanúsító szervezet által elvárt tanúsítási tevékenységek, valamint az értékelés szakmai felügyeleti támogatása érdekében az értékelő szervezetnek nem szabad konkrét értékelési tevékenységébe fognia mindaddig, amíg a sémába fogadásra irányuló kérelmet a tanúsító szervezet formálisan el nem fogadta.

A formális elfogadás egy "értékelő projektindító megbeszéléssel" keretén belül történik.
Az 1. ábra az értékelés előkészületi szakaszában végzendő fontosabb tevékenységeket tekinti át.

4.2. AZ ÉRTÉKELÉS LEBONYOLÍTÁSI SZAKASZA

A lebonyolítás szakasza az értékelési folyamat fő része.
Az értékelés egy informatikai termék vagy rendszer (az értékelés tárgya) felmérése a Közös szempontoknak való megfelelőség szempontjából. Az értékelés célja, hogy az értékelő szervezet megállapítsa, hogy az értékelés tárgya megfelel (vagy nem felel meg) saját biztonsági előíranyzatának.
/Maga a formális biztonsági értékelés két fázisra osztható: előbb a biztonsági előíranyzat értékelése a [7]-ben leírt módszertani követelményeknek megfelelően, majd az értékelés tárgya (az értékelendő informatikai termék vagy rendszer) értékelése saját biztonsági előíranyzatának való megfelelőség szempontjából, szintén a [7]-ben leírt módszertani követelményeknek megfelelően. A fenti két fázis között bizonyos átfedés lehetséges egy értékelés során./
A lebonyolítás során az értékelő szervezet az értékelési munkaterve alapján áttekinti a megbízótól vagy fejlesztőtől kapott, az értékelésre átadandó fejlesztői bizonyítékok listája által tartalmazott átadandókat és végrehajtja az elvárt garanciális szintek megfelelő értékelési tevékenységeket.
Egy értékelési munkaterv fejlődhet, változhat az értékelés folyamán, amennyiben az értékelő szervezet a megbízótól kiegészítő információhoz jut. Az értékelő szervezet az értékelés lebonyolítási szakaszában bármikor a tanúsító szervezethez fordulhat speciális szakkérdések megvitatása, felmerülő ellentmondások és problémák tisztázása, illetve bármely más, az értékeléssel kapcsolódó fontos kérdés megbeszélése céljából.

Az informatikai biztonsági értékelés eredményeit az értékelés előrehaladásával az értékelő szervezet folyamatosan dokumentálja. Az értékelő szervezetnek "észrevételezési jelentés" formájában tájékoztatnia kell a megbízót és a tanúsító szervezetet az értékelés tárgyával, az értékelési módszertannal vagy a MIBÉTS sémaival kapcsolatban felmerülő problémákról.

Amennyiben a bejelentett kérdés vagy probléma a szervezet tárgyával kapcsolatos, a megoldásra, és ez az elvehez szükséges teendők ütemezésére még az eddigiunknál kell részletes javaslatot tennie a tanúsító és értékelő szervezetek számára. Ha egy bejelentett kérdést vagy problémát nem sikerül megoldani, és a tanúsító szervezet úgy ítéli meg, hogy ez az értékelésre hihetően van, a tanúsító szervezet kapcsolatba lép a megbízóval a potenciális kihatások és lehetséges alternatívák megvitatására. A megbízó ilyen esetekben az értékelő szervezettel megtárgyalva a kérdést, a következőképpen dönthet:

- abbahagyja a biztonsági értékelést,
- a tanúsító szervezettel egyetértésben folytatja az értékelést, de elfogadja a problémát, s ennek az értékelésre gyakorolt hatását,
- az értékelés átütése kezdeményezi, s a tanúsító szervezettel egyetértésben biztosítja az értékelés tárgyának szükséges módosítását.

Amennyiben a bejelentett kérdés vagy probléma az értékelési módszertannal vagy a sémaval kapcsolatos, a tanúsító szervezet teszi meg a következő lépéseket közvetlenül az észrevételezési jelentés átvételét követően:

- felméri a közvetlen kérdést vagy problémát, és az adott informatikai biztonsági értékelésre vonatkozó előzetes döntést hoz,
- a kérdést vagy problémát a sémnél belüli csatornákon eljuttatja mindazokhoz, akik segíthetnek a meghatározásban (műszaki munkabizottságok, az értékelő szervezetek biztonsági és vizsgálati szakértői közösségét képviselők, szükség esetén egyéb műszaki szakértők).
4.3. AZ ÉRTÉKELÉS KÖVETKEZETTÉSI SZAKASZA

Az értékelés lebonyolítási szakaszának lezárásaként az értékelő szervezet értékelési jelentést készíti, amely egy általános értékelői határozatot és ennek indoklását tartalmazza. Az értékelő szervezet átadja az értékelési jelentést a tanúsító szervezetnek (pontosabban az általa delegált átvizsgálónak). Az értékelési jelentés tartalmának és formájának meg kell felelnie a 7.2 alfejezetben meghatározottaknak (ami egyúttal a Közös szempontoknak is megfelel). Az értékelési jelentést úgy kell strukturálni, hogy a benne lévő esetleges érzékeny vagy magán információk könnyen eltávolíthatóak legyenek belőle. A 2. ábra az értékelés lebonyolítási és következtetési szakaszaiban végzendő fontosabb tevékenységeket tekinti át.

2. ábra: Tevékenységek az értékelés lebonyolítási és következtetési szakaszaiban
5. FEJEZET
AZ INFORMATIKA BIZTONSÁGI TANÚSÍTÁSI FOLYAMATA

Ez a fejezet a MIBÉTS keretében folytatott informatikai biztonsági értékelési folyamatainak szakmai felügyeletével kapcsolatos tevékenységeket, a tanúsítás folyamatát, a tanúsítványok kibocsátását, valamint az értékelt termékek listájának nyilvánosságra hozását írja le.

5.1 AZ ÉRTÉKELÉSI FOLYAMAT SZAKMAI FELÜGYELETE

Az értékelés szakmai felügyelete az az általános folyamat, melyet a tanúsító szervezet annak érdekében alkalmaz, hogy a séma keretében végzett értékelési és tanúsítási tevékenységek összhangban álljanak a MIBÉTS elfogadott értékelési szempontrendszerével (CC, Közös szempontok), módszertanával (lásd [7]) és valamennyi egyéb séma-specifikus szabályzattal és eljárással. Az értékelés szakmai felügyelete az értékelő szervezetek és bizonyos értékelési tevékenységek folyamatos ellenőrzését jelenti. A MIBÉTS nagy jelentőséget tulajdonít az értékelő szervezetek akkreditálási folyamatának, mely megalapozza, hogy a piaci viszonyok között működő értékelő szervezetek magas szakmai színvonalon, egységes szemlélettel legyenek képesek a biztonsági értékelésekre végrehajtására. Ugyanakkor az informatikai biztonsági értékelésektől elvárt tervezés-elemzés és tesztelés miatt minden értékelés egyedi és bonyolult feladat. Tovább növelik az értékelések bonyolultságát az informatikai biztonság területének alábbi sajátosságai:

- az informatikai biztonságot meg kell védeni a tudatos ellenséges emberi cselekedettekkel szemben is (melyek a védelmi mechanizmusokat szándékosan megkerülni, hatástalanítani, lerontani vagy feltörni igyeksznek),

- állandóan változó, robbanásszerűen fejlődő területen kell lépést tartani a fejlődéssel.

Ez a bonyolultság és egyediség, valamint a sémán belüli összhang biztosításának igénye teszi alapvető fontosságúvá az értékelés szakmai felügyeletét.

Az értékelés szakmai felügyelete az egyes informatikai biztonsági értékelések sémába fogadásával kezdődik. A tanúsító szervezet ezt követően is rendszeres kapcsolatban áll az értékelés megbízójával és az értékelést végző értékelő szervezettel:
• a sikeres biztonsági értékeléshez fontosnak ítélt műszaki és egyéb információkat bocsát rendelkezésükre (különböző segédletek, útmutatók, továbbképzési tematikák formájában, a Közös szempontok értelmezésének és a módszertan alkalmazásának a támogatásával),
• a tanúsítási folyamathoz fontosnak ítélt műszaki és egyéb információkat kér, illetve nyújt,
• a felmerülő fontos szakmai problémák megoldásában közreműködik.

A tanúsító szervezet az értékelés szakmai felügyeletét olyan módon valósítja meg, hogy az garantálja: az értékelő szervezetek a séma közös szempontjait és módszertanát helyesen és teljesen alkalmazzák a különböző értékeléseken, illetve az eltérő garanciaszinteken.

A szakmai felügyelet célja a kockázatok csökkentése a séma valamennyi résztvevője számára. A szakmai felügyelet során végzett tevékenységek száma, típusa, és intenzitása függ:
• az értékelés megcélzott garanciaszintjétől (alap, fokozott, illetve kiemelt),
• az értékelés tárgyának bonyolultságától,
• az értékelő szervezetnek a vizsgált informatikai termék vagy rendszer speciális szakmai területén való gyakorlottságától.

5.2 A TANÚSÍTÁS DÖNTÉSI SZAKASZA

A tanúsítás annak független megerősítése, hogy egy informatikai biztonsági értékelésre a séma előírásainak megfelelően került sor, s hogy az értékelő szervezet következtetései összhangban vannak az értékelési jelentésben bemutatott tényekkel. A tanúsító szervezet a tanúsítási folyamatot annak biztosítására használja, hogy a sémán belül következetes és egységes szakmai döntések szülessenek az elfogadott szempontrendszer és módszertan alkalmazásával. A tanúsítási folyamat lezárásaként a tanúsító szervezet közzétesz egy formális (tanúsítási) jelentést, s kiad egy tanúsítványt.

A tanúsító szervezet minden értékeléshez egy szakmai képviselőt (az úgynevezett átvizsgálót) jelöl ki, aki az elsődleges kapcsolattartó lesz az értékelés megbízója, illetve az értékelő szervezet felé. A megbízónak és az értékelő szervezetnek is ki kell jelölnie egy-egy személyt a kapcsolattartásra. Egy adott értékelés sikere érdekében, a konkrét igényektől függően, a tanúsító szervezet képviselője az értékelés folyamatát áttekintő megbeszéléseken vagy egyéb találkozókon vehet részt a megbízóval vagy/és az értékelő szervezettel.
A biztonsági értékelés lezárása után a tanúsító szervezet áttekinti az értékelő szervezet által készített értékelési jelentést. Ennek során megerősíti, hogy:

- az értékelés tárgya megfelel biztonsági előirányzatának,
- az értékelést a CC szempontrendszerének, a séma értékelési módszerének és a MIBÉTS által megkövetelt egyéb szabályoknak megfelelően végezték,
- a jelentés kellő alapot biztosít a tanúsítási jelentéshez.

A tanúsító szervezet kiegészítő információkat is kérhet az értékelő szervezöttől az értékeléssel kapcsolatos egyes kérdések tisztázására, illetve az értékelési jelentés egyes következtetéseinek alátámasztása érdekében betekinthet a szükséges bizonyítékokba és értékelési nyilvántartásokba.


A tanúsítási jelentés tervezetét a tanúsító szervezet áttekintése után a megbízó és az értékelő szervezet rendelkezésére kell bocsátani, annak érdekében, hogy megerősíthessék az alábbiakat:

- a tanúsítási jelentés tervezet következtetései szakmailag helyesek,
- nem merül fel egyetlen olyan tény sem, mely érvényteleníti a jelentést,
- minden érzékeny vagy üzleti titkot képező információt kihagynak belőle.

A megbízó és az értékelő szervezet külső áttekintése után a tanúsító szervezet megkapja a végleges értékelési jelentést és a tanúsítási jelentés tervezetét, áttekintés és véleményezés céljából. Az ezt követően véglegesített tanúsítási jelentést nyilvánosságra hozzák. A tanúsítási jelentés összegzi és megerősíti az értékelő szervezet által végzett értékelés eredményeit (azaz, hogy az értékelést a CC szempontrendszerének, a MIBÉTS értékelési módszerének és a séma által megkövetelt egyéb szabályoknak megfelelően végezték, következtetései pedig összhangban állnak a felsorakoztatott bizonyítékokkal).
A tanúsítási jelentés felépítésére és tartalmára vonatkozó sémá elvárásokat a 7.3 alfejezet határozza meg.
A tanúsítási jelentés nyilvános dokumentum, mentes az érzékeny információktól és üzleti titkoktól, egyben a tanúsító szervezet tulajdonát képezi. A tanúsító szervezet felhatalmazza a megbízót a tanúsítási jelentés sokszorosítására és terjesztésére, de a tanúsítási jelentés csak teljes egészében másolható, terjeszthető.

5.3. A KIBOCSÁTOTT TANÚSÍTVÁNYOK

Miután a tanúsító szervezet jóváhagyta a végleges tanúsítási jelentést, egy MIBÉTS tanúsítványt bocsát ki. Miután a tanúsítványt átadták az értékelés megbízójának, egy megfelelő bejegyzés kerül a sémá "jóváhagyott termékek listája" adatbázisába.
A 3. ábra összegzi a tanúsítási folyamat egyes szakaszait.

3. ábra: Tanúsítási tevékenységek a lebonyolítási és következtetési szakaszaiban
6. FEJEZET
A SÉMÁBAN RÉSZTVEVŐK FELADATAI

Ez a fejezet a MIBÉTS résztvevőinek általános feladatait tekinti át az értékelés különböző szakaszaiban. A feladatok részletezését és magyarázatát más MIBÉTS segédletek tartalmazzák, megbízók esetén [4], fejlesztők esetén [5], értékelők esetén pedig [6].

6.1 FELADATOK AZ ÉRTÉKELÉS ELŐKÉSZÜLETI SZAKASZÁBAN

A megbízó feladatai:

- az értékelés kereteit meghatározó döntések meghozatala
  - az értékelés tárgyának (s ezzel az értékelés határainak) pontos meghatározása,
  - a biztonsági előírányzat elkészítése vagy elkészítettése,
  - az értékelési garanciaszint meghatározása,
  - választás a fejlesztéssel párhuzamos és a fejlesztés lezárását követő értékelések között,
  - az értékelő szervezet kiválasztása,
- az értékelés jogi előkészítése
  - szerződés az értékelő szervezettel,
  - szerződés alvállalkozókkal,
  - az érzékeny információk kezelése,
  - a szerzői jogok rendezése,
- az értékelés megkezdéséhez szükséges támogatás biztosítása
  - az értékeléshez szükséges fejlesztői bizonyítékok biztosítása,
  - képzés biztosítása,
  - konzultációs és egyéb támogatás.

A fejlesztő feladatai:

- a megbízó támogatása az értékelés kereteit meghatározó döntések meghozatalában
  - az értékelés tárgyának (s ezzel az értékelés határainak) pontos meghatározása,
  - a biztonsági előírányzat elkészítésének támogatása,
  - az értékelési garanciaszint meghatározásának támogatása,
  - az értékelési munkaterv és ütemterv véleményezése,
• a fejlesztői bizonyítékok elkészítésében való közreműködés.

Az értékelő feladatai:
• a megbízó támogatása az értékelés kereteit meghatározó döntések megalapozásában
  • megvalósíthatósági tanulmány készítése,
  • a biztonsági előírások áttekintése, előzetes értékelése,
• felkészülés az értékelésre
  • szerződéskötés a megbízóval,
  • értékelési munkaterv és ütemterv készítése.

6.2 FELADATOK AZ ÉRTÉKELÉS LEBONYOLÍTÁSI SZAKASZÁBAN

A megbízó feladatai:
• az értékelés támogatása a szerződésben rögzített ütemben,
• az értékelés során felmerülő kérdések tisztázása,
• az értékelés során felmerülő problémák megoldása.

A fejlesztő feladatai:
• az értékelés támogatása a fejlesztői bizonyítékok elkészítésében való közreműködéssel,
• az értékelés egyéb támogatása,
• az értékelés során felmerülő kérdések tisztázása,
• az értékelés során felmerülő problémák megoldása.

Az értékelő feladatai:
• az értékelésre átadandó fejlesztői bizonyítékok átvetele és megfelelő kezelése,
• az értékelési módszertan által megkövetelt értékelési tevékenységek végrehajtása,
• a szükséges értékelési támogatás kérése, fogadása (pl. a fejlesztő általi képzés, a tanúsító értelmezései),
• az értékelői bizonyítékok elkészítése,
• az értékelési nyilvántartások folyamatos vezetése.
6.3 FELADATOK AZ ÉRTÉKELÉS KÖVETKEZTETÉSI SZAKASZÁBAN

A megbízó feladatai:

- az értékelés eredményeinek elfogadása,
- a tanúsítási folyamat támogatása.

A fejlesztő feladatai:

- az értékelés eredményeinek elfogadása,
- a tanúsítási folyamat támogatása.

Az értékelő feladatai:

- az értékelés eredményeinek dokumentálása és indoklása (az értékelési jelentés elkészítése).

6.4 FELADATOK AZ ÉRTÉKELÉSI ÉS TANÚSÍTÁSI FOLYAMAT LEZÁRÁSÁT KÖVETŐEN

A megbízó feladatai:

- a tanúsítás eredményeinek korrekt felhasználása,
- a tanúsítás érvényességének nyomon követése.

A fejlesztő feladatai:

- nincs feladata

Az értékelő feladatai:

- a fejlesztői és az értékelői bizonyítékok kezelése,
- az értékelési módszertan változásának nyomon követése,
- az értékelési tapasztalatok leszürése,
- sebezhetőségek gyűjtése és kategorizálása.
7. MELLÉKLETEK

7.1 A BIZTONSÁGI ELŐIRÁNYZAT FELÉPÍTÉSE ÉS TARTALMA

Az alábbi ábra a biztonsági előirányzat elvárt felépítését és tartalmát határozza meg.

A biztonsági előirányzat egy azonosított értékelés tárgya (mely lehet egy informatikai termék vagy egy informatikai rendszer) informatikai biztonsági követelményeit tartalmazza, és előírja azokat a funkcionális és garanciális biztonsági intézkedéseket, amelyeket ez az értékelés tárgya ajánl fel, hogy a kinyilvánított követelményeket kielégítse.
Az értékelés tárgya számára készült biztonsági előirányzat alkojtja a fejlesztők, az értékelők és a vásárlók között létrejött, az értékelés tárgya biztonsági sajátosságait és az értékelés hatókörét rögzítő megállapodás alapját.

7.1.1 A BIZTONSÁGI ELŐIRÁNYZAT BEVEZETÉSE

A biztonsági előirányzat bevezetésének a következő dokumentumkezelő és áttekintő információt kell tartalmaznia:

- **A biztonsági előirányzat azonosításának** azt a címkéző és leíró információt kell tartalmaznia, amely a biztonsági előirányzat és az általa kiválasztott értékelés tárgya ellenőrzéséhez és azonosításához szükséges, amelyre a biztonsági előirányzat hivatkozik.

- **A biztonsági előirányzat áttekintésének** leíró módon kell a biztonsági előirányzatot összefoglalnia. Az áttekintés a biztonsági előirányzat potenciális használója számára legyen elég részletes ahhoz, hogy annak alapján eldönthesse, érdemes-e a értékelés tárgyával foglalkoznia.

- **A CC-nek való megfelelőségről szóló kijelentésnek** ki kell nyilvánítania minden, az értékelés tárgyára vonatkozó, értékelhető, a CC-nek való megfelelőségről szóló kijelentést.

7.1.2 AZ ÉRTÉKELÉS TÁRGYA LEÍRÁSA

A biztonsági előirányzat ezen részének úgy kell az értékelés tárgyát leírnia, hogy az segítsége az értékelés tárgya biztonsági követelményeinek könnyebb megértését, emellett meg kell neveznie a termék vagy rendszer fajtáját. Az értékelés tárgya tárgyát, hatókörét és határait általános kifejezésekkel, fizikai (hardver és/vagy szoftver összetevőkkel/modulokkal), vagy logikai módon (az értékelés tárgya által felajánlott informatikai és biztonsági tulajdonságokkal) kell leírni.

7.1.3 AZ ÉRTÉKELÉS TÁRGYA BIZTONSÁGI KÖRNYEZETE

A értékelés tárgya biztonsági környezetéről szóló nyilatkozatban szerepeltetni kell azon környezet biztonsági szempontjainak a leírását, amelyben az értékelés tárgyát használni szándékozzák, és annak a módnak a leírását, ahogyan alkalmazni fogják. E nyilatkozatnak a következőket kell magában foglalnia:
• A feltételezések leírásában be kell mutatni annak a környezetnek a biztonsági szempontjait, ahol az értékelés tárgyát használják vagy használni akarják.

• A fenyegetések leírásában a vagyontárgyakat érintő minden olyan fenyegetést szerepelteni kell, amely miatt különleges védelmet igényel az értékelés tárgya vagy annak környezete.

• A szervezetbiztonsági szabályzatok leírásának meg kell határoznia, és ha szükséges meg kell magyarázna azokat a szervezetbiztonsági szabályzatokat vagy szabályokat, amelyeknek az értékelés tárgyának eleget kell tennie.

7.1.4 BIZTONSÁGI CÉLOK

A biztonsági célokról szóló nyilatkozatnak mind az értékelés tárgya, mind környezete biztonsági céljait meg kell határoznia. A célok következő kategóriáit kell azonosítani:

• Az értékelés tárgya biztonsági céljait világosan kell megállapítani, és vissza kell vezetni azokra az azonosított fenyegetésekre, amelyek ellen az értékelés tárgya tesz ellenértékelést és/vagy azokra a szervezetbiztonsági szabályzatokra, amelyeknek az értékelés tárgyának eleget kell tennie.

• A környezet biztonsági céljait világosan kell megállapítani, és vissza kell vezetni azokra az azonosított fenyegetésekre, amelyek ellen az értékelés tárgya nem tesz átfogó ellenértékeléseket és/vagy azokra a szervezetbiztonsági szabályzatokra vagy feltételezésekre, amelyeknek az értékelés tárgya nem tesz teljesen eleget.

7.1.5 AZ INFORMATIKAI BIZTONSÁG KÖVETELMÉNYEI

A biztonsági előirányzat e része az informatikai biztonság azon követelményeit határozza meg, amelyeket vagy az értékelés tárgyának, vagy környezetének kell kielégíteni. Az informatikai biztonság követelményeit a következő formában kell felállítani:

• Az értékelés tárgya biztonsági követelményeiről szóló nyilatkozatnak kell azokat a funkcionális és garanciális biztonsági követelményeket meghatároznia, amelyeket az értékelés tárgyának és az értékelését támogató bizonyítéknak azért kell kielégítenie, hogy teljesítsze a biztonsági célokat. Az értékelés tárgya biztonsági követelményeit a következő formában kell felállítani:
• Az értékelés tárgya funkcionális biztonsági követelményeiről szóló nyilatkozat az értékelés tárgya funkcionális követelményeit a Közös szempontok 2. részének funkcionális összetevőivel határozza meg, ahol azok alkalmazhatók.

• Az értékelés tárgya garanciális biztonsági követelményeiről szóló nyilatkozat a garanciális követelményeket egy garanciaszintként határozza meg. (A MIBÉTS keretében választható garanciaszintek: alap, fokozott és kiemelt.)

• Az informatikai környezet biztonsági követelményeiről szóló, opcionálisan választható nyilatkozatnak azokat az informatikai biztonsági követelményeket kell meghatároznia, amelyeket az értékelés tárgya informatikai környezetének kell kielégítenie.

7.1.6 AZ ÉRTÉKELÉS TÁRGA ÖSSZEFOGLALÓ ELŐÍRÁSA

Az értékelés tárgya összefoglaló előírásának kell meghatároznia az értékelés tárgya biztonsági követelményeinek megvalósítását. Ennek az előírásnak kell megadnia a biztonsági funkciók olyan leírását és az értékelés tárgya olyan garanciális intézkedéseit, amelyek kielégítik az értékelés tárgya biztonsági követelményeit.

Az értékelés tárgya összefoglaló előírása a következőket tartalmazza:

• **Az értékelés tárgya biztonsági funkciókról** szóló nyilatkozatnak le kell fednie az informatikai biztonsági funkciókat, és meg kell határoznia azt, hogy ezek a funkciók hogyan elégték ki az értékelés tárgya funkcionális biztonsági követelményeit. Ennek a nyilatkozatnak kell tartalmaznia a funkciók és követelmények közötti olyan kétirányú megfeleltetést, amely világosan mutatja, hogy melyik funkció melyik követelményt elégtéti ki, és hogy minden követelmény megvalósul. Minden biztonsági funkcióknak legalább egy értékelés tárgya funkcionális biztonsági követelmény teljesítéséhez hozzá kell járulnia.

• **A garanciális intézkedések**ről szóló nyilatkozat az értékelés tárgya azon garanciális intézkedéseit határozza meg, amelyekről kijelentették, hogy eleget tesznek a kinyilvánított garanciális követelményeknek. A garanciális intézkedéseket a garanciális követelményekre úgy kell visszavezetni, hogy láthatóvá váljon, melyik intézkedés melyik követelmény kielégítéséhez járul hozzá.
7.1.7 VÉDELMI PROFIL NYILATKOZATOK

A biztonsági előirányzat szabadon választható módon olyan kijelentést tehet, hogy az értékelés tárgya egy (vagy akár több) védelmi profil követelményeinek megfelel. Bármilyen, védelmi profilnak való megfelelőségről szóló kijelentés esetén a kijelentésbe foglalt valamennyi védelmi profilra nézve a következőket kell a nyilatkozatnak tartalmaznia:

• A **védelmi profil hivatkozás** nyilatkozatnak azonosítania kell azt a védelmi profilt, amelynek való megfelelőségről a kijelentés szól, és azokat az esetleges kiegészítéseket, amelyek a kijelentés állításainak megerősítésére szükségesek lehetnek. Egy érvényes kijelentés magában foglalja azt is, hogy az értékelés tárgya eleget tesz a védelmi profil valamennyi követelményének.

• A **védelmi profil illesztés** nyilatkozatnak azonosítania kell az informatikai biztonsági követelményekről szóló azon nyilatkozatokat, amelyek kielégítik a védelmi profil megengedett műveleteinek a végrehajtását, vagy egyéb módon jellemzik tovább a védelmi profil követelményeit.

• A **védelmi profil kiegészítés** nyilatkozatnak meg kell adnia az értékelés tárgya azon céljait és követelményeit, amelyek kiegészítik a védelmi profil céljait és követelményeit.

7.1.8 INDOKLÁS

A biztonsági előírányzat ezen része a biztonsági előírányzat értékeléséhez használható bizonyítékokat mutatja be. Ez a bizonyíték támogatja azt a kijelentést, hogy a biztonsági előírányzat teljes és ellentmondásmentes követelménykészlet, és hogy az ennek megfelelő értékelés tárgya a biztonsági környezetben belül hatékony informatikai ellenintézkedés készletet képes nyújtani, valamint hogy az értékelés tárgya összefoglaló előírása tárgyalja ezeket a követelményeket. Az indoklás azt is bemutatja, hogy minden védelmi profilnak való megfelelőségi kijelentése valós. Az indoklásnak a következőket kell magában foglalnia:

• A **biztonsági célok indoklásának** meg kell mutatnia, hogy a kinyilvánított biztonsági célok visszavezethetők az értékelés tárgya biztonsági környezetében azonosított valamennyi szempontra, és hogy alkalmasak azok lefedésére.
• A biztonsági követelmények indokolásának meg kell mutatnia, hogy az értékelés tárgya és környezete biztonsági követelménykészlete alkalmas a biztonsági célok kielégítésére, sőt azokra visszavezethetők.

• Az értékelés tárgya összefoglaló előírása indoklásának meg kell mutatnia, hogy az értékelés tárgya funkcionális és garanciális biztonsági intézkedései alkalmasak arra, hogy az értékelés tárgya biztonsági követelményeit kielégítsék.

• A védelmi profilról szóló kijelentések indoklásának meg kell magyaráznia bármely különbséget a biztonsági előírások biztonsági céljai és követelményei, valamint azon (opcionálisan választott) védelmi profilok biztonsági céljai és követelményei között, amelynek való megfelelőséget kijelentették.
7.2 AZ ÉRTÉKELÉSI JELENTÉS FELÉPÍTÉSE ÉS TARTALMA

Az értékelési jelentést az értékelő szervezet készíti el a megbízó és a tanúsító szervezet számára, ez képezi a tanúsítási jelentés legfőbb alapját.

Az értékelési jelentés célja, hogy bemutassa az értékelés során végrehajtott tevékenységekből származó határozatokat, ezek indokolását, és minden ténymegállapítást, beleértve az informatikai termék vagy rendszer fejlesztése során elkövetett hibákat és az értékelés során feltárt kiaKNázható sebezhetőségeket.

Az értékelési jelentés tartalmazhat védett információt is, amennyiben ezek szükségesek az értékelési eredmények igazolásához.

Az alábbiak az értékelési jelentés kötelező felépítését és elvárt tartalmát határozzák meg.

7.2.1 AZ ÉRTÉKELÉS TÁRGYÁNAK ÁTTEKINTÉSE

Ez a fejezet az értékelés tárgyának egy magas szintű áttekintését, rövid leírását adja.

Az áttekintés célja olyan bevezető információk nyújtása, mely a jelentés későbbi részeinek megértéséhez szükségesek, egyben egy összkép adása az értékelt termékről vagy rendszerről.

7.2.2 AZ ÉRTÉKELÉS TÁRGYÁNAK SZERKEZETI LEÍRÁSA

Ez a fejezet az informatika termék vagy rendszer és legfőbb összetevői magas szintű tervét írja le. A fejezet célja a fő összetevők szerkezeti elkülönülésének a jellemzése.

7.2.3 AZ ÉRTÉKELÉS JELLEMZÉSE

Ebben a fejezetben az értékelő az alkalmazott értékelési módszereket, technikákat, eszközöket és szabványokat dokumentálja. Az értékelő a teszteléshez használt eszközökre is hivatkozhat. Az értékelő itt jelez minden értékelésre, illetve az értékelési eredmények terjesztésére vonatkozó korlátozást, valamint az értékelés során tett mindazon feltételezést, mely az eredményekre hatással van. Az értékelő ebben a részben helyezheti el a jogi kötöttségekre, szervezetre vagy bizalmasságra vonatkozó információkat.
7.2.4 AZ ÉRTÉKELÉS EREDMÉNYEI

Ebben a részben mutatja be az értékelő az értékelés eredményeit, az alábbi alfejezetekben:

- A biztonsági előirányzat értékelése,
- A konfiguráció kezelés értékelése,
- A szállítás és működtetetés értékelése,
- A fejlesztés értékelése,
- Az útmutatók értékelése,
- Az életciklus támogatás értékelése (csak fokozott és kiemelt garanciaszinten),
- A tesztelés értékelése,
- A sebezhetőség értékelése.

Minden alfejezet megnevezi az értékelés alapját képező dokumentumokat (fejlesztői bizonyítékokat), majd az értékelés módszertanának (lásd [7]) megfelelő szerkezetben és jelölésekkel felsorolja az elvégzett értékelői feladatelemeket, azok következtetéseit, illetve az ezekre vonatkozó (rész)határozatokat.

7.2.5 (ÁLTALÁNOS ÉRTÉKELŐI) HATÁROZAT

Az értékelőnek itt kell összegeznie az értékelés fő következtetését, mely arra vonatkozik, hogy megfelel-e biztonsági előirányzatának.

7.2.6 INOKLÁS

Az értékelő itt indokolja meg végső határozatát, illetve annak fontosabb részhatározatait.

7.2.7 JAVASLATOK

Az értékelő javaslatokat fogalmazhat meg, mely hasznos lehet mind a megbízónak, mind a tanúsító szervezetnek. Ezek a javaslatok az adott terméknek vagy rendszernek az értékelés során feltárt hiányosságaira, gyengeségeire, vagy ellenkezőleg, a különösen hasznos tulajdonságaira vonatkozhatnak.

7.2.8 AZ ÉRTÉKELÉSHEZ FELHASZNÁLT BIZONYÍTÉKOK

Az értékelőnek valamennyi értékeléshez felhasznált bizonyítékről külön-külön meg kell adjnia az alábbiakat:
7.2.9 A TANÚSÍTOTT TERMÉKEK LISTÁJÁBA JAVASOLT SZÖVEG

Ebben a részben egy (szó szerinti) javaslatot kell adni a tanúsított termékek listájába az értékelés tárgyához kapcsolódóan (ami egy igen rövid, 5-7 mondatos összefoglalása a teljes jelentésnek).

7.2.10 ÉSZREVÉTELEZÉSI JELENTÉSEK ÉS HATÁROZATOK

Az értékelőnek ebben a részben fel kell sorolnia valamennyi (esetlegesen) megírt észrevételezési jelentését, s az erre kapott válaszra hozott döntését (határozatát a jelzett probléma megfelelő megoldásáról).

7.2.11 RÖVIDÍTÉSEK

Ez a rész a jelentés olvashatóságához járul hozzá, meghatározva az értékelési jelentésben használt betűszavak jelentését.

7.2.12 FOGALMAK

Ez az opcionális rész a jelentés olvashatóságához járul hozzá, meghatározva azokat a jelentésben előforduló fogalmakat, amelyeknek jelentése nem nyilvánvaló.

7.2.13 BIZTONSÁGI ELŐIRÁNYZAT

A biztonsági előirányzat az értékelési jelentés részét képezi. Ugyanakkor a biztonsági előirányzat különálló dokumentumként is csatolható.
7.3 A TANÚSÍTÁSI JELENTÉS TARTALMA

A tanúsítási jelentés az informatikai termékre vagy rendszerre vonatkozó részletes biztonsági információk forrása minden érdekelt fél számára. Célja az, hogy gyakorlati információkat nyújtson az informatikai termékről vagy rendszerről a beszerzőknek/vásárlóknak.

A tanúsítási jelentésnek nem szükséges és nem is szabad védett információt tartalmaznia, mivel a biztonsági előirányzathoz hasonlóan, a beszerzők/vásárlók számára tartalmazza az informatikai termék vagy rendszer biztonságos alkalmazásához szükséges információkat.

Az alábbiak a tanúsítási jelentés kötelező felépítését és felépítését és elvárt tartalmát határozzák meg.

7.3.1 ÖSSZEFoglaló

Az összefoglaló a teljes tanúsítási jelentés egy rövid összefoglalása. Az ebben a fejezetben tartalmazott információknak világos és tömör áttekintést kell nyújtania az olvasóknak az értékelési eredményekről. Ennek a fejezetnek az olvasóközönsége magában foglalhatja a biztonságos informatikai termékek és rendszerek fejlesztőit, fogyasztóiit és értékelőit. Az összefoglalóból az olvasó alapvető ismereteket nyerhet az informatikai termékről vagy rendszerről, illetve a jelentés eredményeiről. Lehetséges, hogy egy olvasó (pl. egy döntéshozó) a tanúsítási jelentésnek csak ezt a fejezetét olvassa el, ezért fontos, hogy minden kulcsfontosságú megállapítás szerepeljen benne. Az összefoglalásnak legalább az alábbiakat tartalmaznia kell (de nem kell ezekre korlátozódnia):

- az értékel t informatikai termék vagy rendszer neve és azon összetevőinek a felsorolása, amelyek az értékelés tárgyát képezték, a fejlesztő neve és a verzió;
- az informatikai biztonsági értékelő szervezet neve;
- az értékelés befejezésének dátuma;
- a jelentés eredményeinek rövid ismertetése:
  - garanciászint (alap, fokozott vagy kiemelt);
  - funkcionalitás;
  - az értékel t informatikai termékre vagy rendszerre vonatkozó fenyegetések és szervezetbiztonsági szabályzatok;
  - speciális konfigurációs követelmények;
  - feltételezések az üzemeltetési környezetre vonatkozóan;
  - (felelősség) elhatárolódások.
7.3.2 AZONOSÍTÁS

Az értékelt informatikai terméket vagy rendszert egyértelműen azonosítani kell. A szoftver verzió számot, minden alkalmazott szoftver javítócsomagot, hardver verzió számot és periféria készüléket (pl. printerek) azonosítani kell, és jegyzékbe kell venni. Ez lehetőséget biztosít az értékelt informatikai termék vagy rendszer teljes azonosításához szükséges címkézésre és leíró információk elhelyezésére.

7.3.3 BIZTONSÁGI SZABÁLYZAT

A biztonsági szabályzat fejezetnek az informatikai termék vagy rendszer biztonsági szabályzatát kell tartalmaznia. A biztonsági szabályzat az informatikai terméket vagy rendszert biztonsági szolgáltatások gyűjteményeként ismerteti. A biztonsági szabályzat ismertetése azokat a szabályzatokat vagy szabályokat tartalmazza, amelyeknek az informatikai terméknek vagy rendszernek meg kell felelnie, vagy amelyeket érvényre kell juttatnia.

7.3.4 FELTÉTELEZÉSEK ÉS HATÓKÖR

Ebben a fejezetben annak a környezetnek és/vagy konfigurációnak a biztonsági vonatkozásait kell leírni, amelyben való felhasználásra szánták az informatikai terméket vagy rendszert. A fejezet arra szolgál, hogy érthetően tisztázza az értékelés hatókörét azokkal a fenyegetésekkel kapcsolatban, amelyek nincsenek számításba véve. Ennek alapján a felhasználók megalapozott döntést hozhatnak az informatikai termék vagy rendszer használatával járó kockázatokról.

A fejezetben ismertetni kell a felhasználás módját, a környezetre vonatkozó feltételezéseket és az értékelés hatókörének tisztázását azokra a fenyegetésekre nézve, melyeket az értékelés során nem vettek figyelembe.

A környezetre vonatkozó feltételezések

Annak érdekében, hogy az értékelés során egy vonatkoztatási alapot lehessen megadni a termékre vagy rendszerre, bizonyos feltételezéseket kell tenni arra a környezetre, amelyben az informatikai terméket vagy rendszert használni fogják. Ez az alfejezet dokumentálja az informatikai termékre vagy rendszerre az értékelés során tett valamennyi környezeti feltételezést.
A felhasználásra vonatkozó feltételezések

Annak érdekében, hogy az értékelés során egy vonatkoztatási alapot lehessen megadni a termékre vagy rendszerre, bizonyos feltételezéseket kell tenni a termék vagy rendszer használatára. Feltételezni kell például a megfelelő telepítést és konfigurálást, a minimálisan kielégítendő hardver feltételeket, stb. Ez az alfejezet dokumentálja az informatikai termék vagy rendszer felhasználására az értékelés során tett valamennyi feltételezést.

Az értékelés hatóköre

Ez az alfejezet egyrészt az informatikai termékre vagy rendszerre vonatkozó azon fenyegetéseket sorolja fel és írja le, amelyeket a termék értékelő biztonsági funkciói nem vesznek számításba. Előfordulhat, hogy egy kliens feltételezi bizonyos fenyegetésekről, hogy azzal az informatikai termék vagy rendszer számol, pedig valójában nem. Ez az oka annak, hogy a számításba nem vett (releváns) fenyegetéseket is fel kell sorolni. Ez az alfejezet határozza meg azokat az esetleges biztonsági funkciókat is, melyek nem képeztek tárgyát az értékelésnek.

7.3.5 SZERKEZETI LEÍRÁS

Ez a fejezet az informatika termék vagy rendszer és legfőbb összetevői magas szintű tervét írja le. A fejezet célja a fő összetevők szerkezeti elkülönülésének a jellemzése.

7.3.6 DOKUMENTÁCIÓ

Ez a fejezet az informatikai termékre vagy rendszerre vonatkozó azon dokumentációknak a teljes felsorolását adja meg, amelyeket a fejlesztő a termékkel együtt átad a fogyasztónak. Fontos, hogy minden lényeges dokumentum verziószámmal legyen ellátva. A dokumentációknak legalább felhasználói, adminisztrátori és telepítési útmutatót tartalmaznia kell. Az adminisztrációs és telepítési útmutatót tartalmazhatja ugyanaz a dokumentum is.

7.3.7 AZ INFORMATIKAI TERMÉK VAGY RENDSZER TESZTELÉSE

Ez a fejezet ismerteti mind a fejlesztői, mind az értékelői teszteleseket, körvonalazva a tesztelés megközelítésmódját, konfigurálását, mélységét és eredményeit.
7.3.8 AZ ÉRTÉKELT KONFIGURÁCIÓ

Ez a fejezet az informatikai terméknek vagy rendszernek az értékelés során meglévő konfigurációját dokumentálja. Általában az adminisztrátori vagy a telepítési útmutató adja meg a szükséges részleteket az informatikai termék vagy rendszer helyes konfigurálására. Az informatikai terméket vagy rendszert sokféle módon lehet konfigurálni a felhasználási környezettől, valamint a szervezet adott termékkel vagy rendszerrel érvényre juttatandó biztonsági szabályzatától függően.

Ez a fejezet a pontos beállítási és konfigurálási részleteket írja le, ezek megválasztásának magyarázatával együtt. További üzemeltetési megjegyzések és megfigyelések is csatolhatók. Ez a fejezet különösen fontos, mivel ez nyújt vonatkoztatási alapot az értékelő termék telepítéséhez.

7.3.9 AZ ÉRTÉKELÉS EREDMÉNYEI

Ez a fejezet dokumentálja azokat a garancia követelményeket, amelyeket az informatikai termék vagy rendszer teljesít. Ezen követelmények részletes leírása, és annak részletezése, hogy a termék vagy rendszer hogyan teljesíti ezeket, a biztonsági előirányzatban található.

7.3.10 ÉRTÉKELŐI MEGJEGYZÉSEK ÉS JAVASLATOK

Ez a fejezet arra szolgál, hogy kiegészítő információkat közöljön az értékelés eredményeiről. Ezek a megjegyzések/javaslatok összegezhetik az értékelés során az informatikai termékre vagy rendszerre feltárt hiányosságokat, vagy megemlíthetik a különösen fontos tulajdonságokat.

7.3.11 MELLÉKLETEK

A mellékletek arra szolgálnak, hogy körvonalazzanak minden olyan kiegészítő információt, amely hasznos lehet a jelentés olvasóközönsége számára, de logikailag nem illik az ismertetés előző fejezetéibe (pl. egy biztonsági szabályzat teljes leírása).
7.3.12 BIZTONSÁGI ELŐIRÁNYZAT

A biztonsági előirányzatot csatolni kell a tanúsítási jelentéshez. Ugyanakkor a csatolt biztonsági előirányzat változatban az üzleti titkot képező (pl. szabadalmaztatott) műszaki információk kihagyhatók vagy átfogalmazhatók.

7.3.13 FOGALMAK ÉS RÖVIDÍTÉSEK

Ez a rész a jelentés olvashatóságához járul hozzá, meghatározva azokat a betűszavakat és fogalmakat, amelyeknek jelentése nem nyilvánvaló.

7.3.14 FELHASZNÁLT DOKUMENTUMOK

Ez a fejezet a jelentés szerkesztéséhez forrásanyagként felhasznált összes hivatkozott dokumentációt sorolja fel. Többek között tartalmazhatják a következőket:

- követelmények, módszertan, séma dokumentáció;
- műszaki hivatkozások dokumentációja;
- az értékelés során felhasznált fejlesztői dokumentáció.
7.4 A MIBÉTS KERETÉBEN KIADOTT TANÚSÍTVÁNYOK

7.4.1 INFORMATIKAI TERMÉK ÉRTÉKELÉSÉHEZ KAPCSOLÓDÓ MIBÉTS TANÚSÍTVÁNYOK

Egy MIBÉTS keretén belül végzett informatikai termékértékelés tanúsításával keletkezett, a tanúsító szervezet által jóváhagyott tanúsítványnak a következő információkat kell tartalmaznia:

- a termék neve;
- a termék gyártója;
- a termék típusa;
- verziószám vagy a kiadás száma;
- a biztonsági előirányzatnak való megfelelés;
- az értékelő szervezet megnevezése;
- az értékelés garanciaszintje (alap, fokozott vagy kiemelt);
- értékelési platform (opcionális);
- a tanúsítvány azonosítója;
- a tanúsítási jelentés azonosítója;
- a kibocsátás dátuma.

7.4.2 KIEGÉSZÍTŐ NYILATKOZAT ÉS SÉMAJELZÉS INFORMATIKAI TERMÉK ESETÉN

Egy MIBÉTS keretén belül végzett informatikai termékértékelés tanúsításával keletkezett, a tanúsító szervezet által jóváhagyott tanúsítványnak tartalmaznia kell az alábbi nyilatkozatot is:

Az értékelést a Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma rendelkezéseivel összhangban folytatták le, és az értékelő szervezet értékelési jelentésében rögzített következtetései összhangban állnak a szolgáltatott bizonyítékokkal.

Ez a tanúsítvány az informatikai terméknél csak a jelen tanúsítványban felsorolt verzióira és kiadásaira érvényes, az értékelő konfigurációs esetén, valamint a teljes tanúsítási jelentéssel együtt.
Ezzel a tanúsítvánnyal a tanúsító szervezet vagy bármely más szervezet, amely elismeri vagy hatályba lépteti ezt a tanúsítványt, nem hagyja jóvá az informatikai terméket, és nem vállal sem kimondott, sem hallgatólagos garanciát érte. Bizonyos valószínűséggel megmarad a kihasználható sebezhetőség feltáratlanságának maradvány kockázata. Ez a valószínűség alap garanciaszint mellett nagyobb, fokozott garanciaszintnél kisebb, kiemelt garanciaszint mellett pedig a legkisebb.

7.4.3 INFORMATIKAI RENDSZER ÉRTÉKELÉSÉHEZ KAPCSOLÓDÓ MIBÉTS TANÚSÍTVÁNYOK

Egy MIBÉTS keretén belül végzett informatikai rendszerértékelés tanúsításával keletkezett, a tanúsító szervezet által jóváhagyott tanúsítványnak a következő információkat kell tartalmaznia:

- a rendszer neve;
- a rendszert alkotó termékek;
- a rendszert alkotó termékek gyártói;
- a termékek típusa;
- a termékek verziószáma vagy a kiadás száma;
- a biztonsági előírásoknak való megfelelés;
- az értékelő szervezet megnevezése;
- az értékelés garanciaszintje (alap, fokozott vagy kiemelt);
- értékelési platform (opcionális);
- a tanúsítvány azonosítója;
- a tanúsítási jelentés azonosítója;
- a kibocsátás dátuma.

7.4.4 KIEGÉSZÍTŐ NYILATKOZAT ÉS SÉMAJELZÉS INFORMATIKAI RENDSZER ESETÉN

Egy MIBÉTS séma keretén belül végzett informatikai rendszerértékelés tanúsításával keletkezett, a tanúsító szervezet által jóváhagyott tanúsítványnak tartalmaznia kell az alábbi nyilatkozatot is:

Az értékelést a Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma rendelkezéseivel összhangban folytatták le, és az értékelő szervezet értékelési
jelentésében rögzített következtetései összhangban állnak a szolgáltatott bizonyítékokkal.

Ez a tanúsítvány csak az informatikai rendszert alkotó termékek jelen tanúsítványban felsorolt verzióira és kiadásaira érvényes, az értéktől konfigurációk esetén, valamint a teljes tanúsítási jelentéssel együtt.

Ezzel a tanúsítvánnyal a tanúsító szervezet vagy bármely más szervezet, amely elismeri vagy hatályba lépteti ezt a tanúsítványt, nem hagya jóvá az informatikai rendszert, és nem vállal sem kimondott, sem hallgatólagos garanciát érte.

Bizonyos valószínűséggel megmarad a kihasználható sebezhetőség feltáratlanságának maradvány kockázata. Ez a valószínűség alap garanciaszint mellett nagyobb, fokozott garanciaszintnél kisebb, kiemelt garanciaszint mellett pedig a legkisebb.

A felsorolt információkon túl minden MIBÉTS keretén belül kiadott, a tanúsító szervezet által jóváhagyott tanúsítványon a 7.5 alféjezetben megadott sémajelet is el kell helyezni.
7.5 A MIBÉTS SÉMA JELZÉSE (LOGO)
HIVATKOZÁSOK


## RÖVIDÍTÉSEK JEGYZÉKE

<table>
<thead>
<tr>
<th>Abbr</th>
<th>Magyar jelentés</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC</td>
<td>Common Criteria (közös szempontok)</td>
</tr>
<tr>
<td>CCRA</td>
<td>Common Criteria Recognition Arrangement (Megállapodás a Közös szempontok szerinti tanúsítványok elfogadására az informatikai biztonság területén)</td>
</tr>
<tr>
<td>CEM</td>
<td>Common Evaluation Methodology (közös értékelési módszertan)</td>
</tr>
<tr>
<td>EAL</td>
<td>Evaluation Assurance Level (értékelési garanciaszint)</td>
</tr>
<tr>
<td>MIBÉTS</td>
<td>Magyar informatikai Biztonsági Értékelési és Tanúsítási Sémá (séma)</td>
</tr>
<tr>
<td>NAT</td>
<td>Nemzeti Akkreditáló Testület</td>
</tr>
</tbody>
</table>
MEGHATÁROZÁSOK

Értékelési jelentés: az a dokumentum, amely bemutatja az értékelés eredményeit és az értékeléssel kapcsolatos egyéb információkat. [8]

Értékelési módszer: egy eljárás, amely leírja a konkrét termék összetevők, illetve az egész termék vonatkozásában alkalmazott konkrét mérés vagy ellenőrzés eredményeinek elérése érdekében az értékelő által végrehajtandó tevékenységet. [8]

Értékelési nyilvántartás: az értékelési folyamat által végrehajtott összes tevékenység és az értékelési folyamat révén elért összes eredmény dokumentált, objektív bizonyítéka. [8]

Értékelési specifikáció: az értékelési folyamat hatókörének és módszertanának meghatározása. [8]

Értékelés kérelmezője (megbízó): az a személy, illetve szervezet, amely egy értékelést kér. [8]

Értékelő szervezet (értékelő): az értékelést végrehajtó szervezet. [8]

Szoftvertermék (termék): egy felhasználó számára leszállításra szánt számítógép programok, eljárások és az esetleg kapcsolódó dokumentáció és adatok egy sorozata. [9]

Szoftvertermék fejlesztő (fejlesztő): az a személy, illetve szervezet, amely egy szofterverterméket legyárt. [8]

Szoftvertermék értékelés (értékelés): műszaki művelet, amely egy szoftervertermék egy vagy több jellemzőjére vonatkozó felmérésnek egy meghatározott eljárás szerinti végrehajtásából áll. [8]


Tanúsító szervezet (tanúsító): olyan szervezet, amely egy informatikai termék vagy rendszer biztonsági megfelelőségének tanúsítására jogosult, egy a MIBÉTS módszertan alapján végrehajtott értékelés eredménye alapján.