A MABISZ BELÉPTETŐ RENDSZEREKKEL SZEMBEN TÁMASZTOTT VIZSGÁLATI KÖVETELMÉNYEI

A beléptető rendszer felügyeli, ellenőrzi és dokumentálja a védett objektumban történő mozgásokat. A beléptető rendszer akadályozza és/vagy jelzi a jogosulatlan áthaladási, ill. belépési kísérleteket.

A beléptető rendszer részei:

- beléptető terminál;
- beléptető vezérlőegység;
- a terminálok között, valamint terminálok és a központi egység közötti adatátviteli hálózat;
- azonosító eszköz, amely a felismeréshez szükséges adatokat tartalmazza.

1. A RENDSZER ALKOTÓ ELEMEIVEL SZEMBEN TÁMASZTOTT KÖVETELMÉNYEK

a. A beléptető terminál

Az azonosító eszközön kódolt formában tárolt információ, vagy valamilyen, emberre jellemző tulajdonság alapján azonosítja az adott személyt, aki számára a rendszer a jogosultságnak megfelelően engedélyezi, vagy tiltja az adott beléptető ponton történő áthaladást.

A beléptető terminálok részei

- A felismerő egység olyan eszköz, amely memorizált információ, vagy egy azonosító eszközön kódolt formában tárolt információ, vagy valamilyen emberre jellemző tulajdonság alapján azonosítja az adott személyt. (Pl. beléptető pont olvasó, billentyűzet stb.)
- A feldolgozó egység feladata a felismerő egység által azonosított személy jogosultságának megfelelő engedélyezési, ill. tiltási utasítások kiadása. A feldolgozó egység feladata továbbá, az illetéktelen, és az erőszakos behatolási kísérletek jelzésére szolgáló berendezés vezérlő jeleinek előállítása.
- A beléptető pont interfész feladata, hogy vezérlő jeleket szolgáltasson a beléptető pont forgalmát szabályozó elektromechanikus eszköz számára (pl. ajtó, forgókar, zsiliprendszer stb.), amely képes akadályozni a védett területre történő illetéktelen bejutási kísérletet.

A beléptető terminálok alapvető tulajdonságai védelmi szintjüknek megfelelően (az M magas biztonsági szintű, a K közepes biztonsági szintű, az A alacsony biztonsági szintű rendszer):

Tulajdonságok	M	K	A
A beléptető terminálnak autonóm módon tárolnia kell a belépési jogosultság megállapításához szükséges összes adatot.	✓	✓	✓
Tudás alapú azonosítás a belépő személy által megjegyzett adatok szerint (pl. jelszó, számkód, stb.).			✓
Azonosítás kódolt azonosító eszköz, vagy biometrikus adatok alapján.		✓	
Azonosítás az előző módszerek közül legalább kettő együttes alkalmazásával.	✓		
Érzékelni és a felügyeleti központ felé jeleznie kell az erőszakos behatolási kísérleteket.	✓	✓	
Érzékelni és a környezetének jeleznie kell a jogosulatlan behatolási	✓	✓	✓

kísérleteket.			
Idő szerinti jogosultságkezelés.	✓	✓	
Elektromechanikus áteresztő berendezéseket tudjon vezérelni.	✓	✓	✓
Legyen benne eseménynaplózási lehetőség,	✓	✓	
Hálózati feszültség kimaradás esetén a beléptető pont eseménynaplójának adatait (min. 2000) legalább a táblázatban feltüntetett, a védelmi szintnek megfelelő ideig képes legyen megőrizni.	120 h	60 h	24 h
Lehetőség a központi üzemmódból a kapcsolat megszakadása esetén autonóm üzemmódba történő automatikus átkapcsolásra.	✓	✓	
Mind mechanikai, mind elektronikus védelemmel rendelkezzen kiiktatás, rongálás, illetéktelen adatlekérdezés és adatmegsemmisítés ellen (szabotázsvédelem).	✓	✓	
Saját szünetmentes tápellátás (hálózat, akkumulátor)	✓	✓	

b. A rendszer felügyeletét ellátó központi egység:

A beléptető rendszer felügyeleti központjának alapvető tulajdonságai védelmi szintjüknek megfelelően (az M magas biztonsági szintű, a K közepes biztonsági szintű, az A alacsony biztonsági szintű rendszer):

Tulajdonságok	**M**	**K**	**A**
A terminálokról érkező jeleket értelmezi, és megjeleníti.	✓	✓	
A terminálokról érkező riasztó jelzéseket érzékeli, és a környezetének kijelzi.	✓		
A központi egységen keresztül lehet a rendszerbe táplálni azokat az információkat, melyek a jogosultság eldöntésére szolgálnak	✓	✓	
Legyen képes a munka-, vasár- és ünnepnapok megkülönböztetett kezelésére.	✓	✓	
Rendelkezzen valós idejű órával.	✓	✓	
Legyen benne eseménynaplózási lehetőség, és az eseménynaplóban rögzített adatokhoz csak az arra megfelelő jogosultsággal rendelkező személyek férhessenek hozzá.	✓	✓	
Az eseménynapló adatait a rendszergazda által meghatározott ideig képes legyen tárolni.	✓		
Valamennyi, a rendszerben történő kapcsolatmegszakadás kerüljön naplózásra.	✓	✓	
Legyen képes a terminálok távolról történő programozására	✓	✓	
Mind mechanikai, mind elektronikus védelemmel rendelkezzen kiiktatás, rongálás, illetéktelen adatlekérdezés és adatmegsemmisítés ellen (szabotázsvédelem).	✓		
Szünetmentes tápellátás (hálózat, akkumulátor).	✓	✓	
A központ legyen képes felügyelni más vagyonvédelmi rendszereket.	✓		

c. A terminálokat a központtal és egymással összekötő adatátviteli hálózat feladatai:

- A terminálok és a központ, valamint a terminálok egymás között kiépített hálózat feladata, hogy a beléptetési pontokról érkező jelzéseket továbbítsa.
- A hálózatot védőcsőben, az illetéktelen hozzáféréstől védetten kell telepíteni.

- A kiépített hálózatnak a külső EMC zavarokkal szemben magas fokú védelemmel kell rendelkeznie.
- Az esetleges kötéseket csak szabotázsvédett kötődobozokban lehet megoldani.

d. A beléptetéshez szükséges adatokat hordozó eszköz:

A személyazonosításra használt eszközök tulajdonságaik szerint az alábbi három csoportba sorolhatók.

- Tudás alapú azonosítás esetén (amit a személy tud, pl. egy személyazonosító kód, amelyet egy billentyűzeten keresztül lehet betáplálni a központi vagy a helyi jelfeldolgozó egységbe), a felhasználók száma a lehetséges kódok egy ezreléke lehet. A minimális kódszám 10.000.
- Birtoklás alapú azonosítás esetén (amivel a személy rendelkezik, pl. valamilyen kártya, vagy eszköz, ami egy bemeneti egységen keresztül a belépőre jellemző adatokat képes szolgáltatni a jelfeldolgozó egységnek) az azonosítási mód legalább 1.000.000 variációt tegyen lehetővé.
- Biometrikus, élettani alapú azonosítás esetén (mérhető, az egyénre jellemző biológiai tulajdonságok, amelyeket a felismerő egységen keresztül a jelfeldolgozó egység felismerni és azonosítani tud), az azonosítási mód legalább 10.000 variációt tegyen lehetővé.