HADMÉRNÖK

IX. Évfolyam 2. szám - 2014. június

KISS István Csaba
csikiss@gmail.com

BEHATOLÁSJELZŐ RENDSZER BIZTONSÁGI SZINTJÉT BEFOLYÁSOLÓ TÉNYEZŐK

Absztrakt

Korunk beruházásai szinte kivétel nélkül tartalmaznak vagyonvédelmi rendszereket. Ezen belül az elektronikai jelzőrendszerekkel szemben támasztott igények évről évre nőnek. A tervezett, vagy már telepített rendszerek biztonsági szintjének megfelelő ismerete, esetleg számszerű meghatározása sokat segít az üzemeltetőnek. Figyelembe véve, hogy a biztonság sok esetben meghatározó szemponttá vált, a biztonsági szintet jelző számszerű érték megkönnyíti a rendszer minősítését. Ennek a kutatásnak az első lépése, hogy a szerző áttekinti a behatolásjelző rendszereknél a biztonsági szintet befolyásoló tényezőket.

Nowadays, almost every investment includes property protection systems. In particular, the requirement for electronic signaling systems is growing from year to year. The proper knowledge of the security level of designed or installed systems, help to the operator make a decision. Considering that security has become an essential aspects, the numerical value indicating the security level facilitates characterization of the system. The first step of this research is that the author gives an overview of intrusion detection systems, factors affecting the level of security..

Kulcsszavak: *behatolásjelző, biztonsági szint, többkörös védelem ~ intrusion detection, security level, multi-circuit protection*

BEVEZETÉS

A katonai és polgári objektumok elektronikai vagyonvédelmi rendszerei alapvetően az épület fizikai kialakítására, falazat, nyílászárók, födém, stb. épül. A fizikai kialakítás a maga mechanikai védelmével képezi az alapját az objektum több irányú védelemének, amit a jelzőrendszerek kiegészítenek. A napjainkban használt klasszikus elektronikai jelzőrendszerek a következő funkciókat valósítják meg:

- Behatolásjelző rendszer célja, a jogosulatlan behatolás észlelése és annak jelzése az élőerős szolgálat, vagy a hatóságok felé.
- Tűzjelző rendszer feladata, az objektumban esetleg keletkező tűz minél korábbi észlelése, egy vagy több tűzjellemző detektálása alapján. Az észlelt tűzet, a rendszer jelzi, értesíti a szakszolgálatot, ill. automatikus beavatkozásokat indíthat, mint például tűzgátló ajtók zárása, liftvezérlés, vagy akár megkezdheti a terület automata oltását is.
- CCTV, vagy más néven biztonsági kamerarendszer, segíti az objektumban a mozgások, események követését, a terület áttekintését. A felvételek rögzítésével visszakereshetők a történések, nagyban segítve ezzel a felderítési, ill. bizonyítási eljárásokat.
- Beléptető rendszer feladata az objektumba való bejutás. ill. a területen történő mozgások szabályozása. A kialakított beléptetési pontokon azonosítást végez, ellenőrzi áthaladás jogosultságát és engedélyezi, vagy tiltja az áthaladást.

A felsoroltakon kívül e témakörbe tartoznak az olyan speciális alrendszerek, mint a járőrök mozgását dokumentáló járőrellenőrző rendszer, vagy a bolti lopások csökkentését célzó áruvédelmi rendszerek.

A kutatásom célja a fenti rendszerek biztonsági szintjének számszerű meghatározása. Erre eddig nem került sor. Tény, hogy az elektronikai jelzőrendszerek elterjedése növekvő tendenciát mutat, és a tulajdonosok, üzemeltetők jogos igénye, hogy az egyre összetettebb rendszerekről, azok képességeiről egy világos, jól értelmezhető számszerű jellemzőt kapjanak.

Jelen cikkben az elsőként említett behatolásjelző rendszerek felépítését, struktúráját, biztonsági szintjét meghatározó jellemzőket, előírásokat tekintem át. Rámutatok azokra a tényezőkre melyeket figyelembe kell venni, ha számszerűen szeretnénk jellemezni a védelmi szintet.

BEHATOLÁSJELZŐ RENDSZER FELÉPÍTÉSE

A behatolás jelző rendszerek elsődleges célja az élőerős védelem értesítése az illetéktelen behatolásról, behatolási kísérletről. A megfelelően tervezett és telepített rendszer, a mechanikai védelem eszközeire közvetlenül ráépülő érzékelői segítségével, már a mechanikai védelem megsértésének kezdetén helyszíni hang- és fényjelzőkkel, illetve távjelzéssel - a távfelügyeleti központon keresztül, vagy közvetlenül - értesíti az élőerős védelmet.

Egy behatolás jelző rendszer

- érzékelőket,
- helyi jelzésadókat,
- központot,
- kezelőegységeket,
- tápegységeket,
- kiegészítő/bővítő modulokat,

– az eszközöket összekötő helyi kommunikációs hálózatot tartalmaz. A helyi kommunikációs hálózat általában vezetékes kialakítású, de egyre inkább terjednek a vezeték nélküli, rádiós megoldások. [3]

Behatolás jelző rendszerek érzékelői

A behatolás jelző rendszer érzékelőit hagymahéj-szerű elrendezésben, „védelmi körökben", több rétegben helyezzük el. Az egyes védelmi körök a

- kültéri védelem,
- felület (héj) védelem,
- térvédelem,
- tárgyvédelem,
- személyvédelem.

A *kültéri védelem érzékelői* mozgás, rezgés, nyomásváltozás, elektromos tér változás és egyéb érzékelési módokon működő eszközök. Ezeknél az eszközöknél fokozottan figyelembe kell venni a környezeti jellemzők hirtelen, nagymértékű változásának lehetőségét, emiatt az eszközök telepítésekor a megfelelő IP[1] védettségét, valamint szükség esetén fűtésüket-hűtésüket is biztosítani kell.

A *felületvédelem („héjvédelem") érzékelői* biztosítják a védendő objektum falazatán, padozatán, mennyezetén, nyílászáróin, üvegportáljain át történő behatolási kísérletek érzékelését[2]. A nyitható ablakokat, ajtókat nyitásérzékelővel kell ellátni, az üvegfelületek betörésének jelzésére üvegtörés érzékelőket kell telepíteni, a nem megfelelő mechanikai szilárdságú falszerkezeteket falbontás érzékelőkkel kell védeni.

A *térvédelem érzékelői* a passzív infravörös, a mikrohullámú (Doppler elv[3]), az ultrahangos és a kombinált mozgásérzékelők a védendő objektumon belül történő mozgások jelzését biztosítják.

A *tárgyvédelem érzékelői* a védendő objektumon belül elhelyezkedő védendő tárgyak, illetve tároló eszközök megközelítését, elmozdítását, nyitását, rongálását jelzik.

A személyvédelem eszközei a védendő objektumon belül dolgozók személyi biztonságát szolgálják. Ezek az eszközök támadás esetén lehetőséget biztosítanak csendes riasztás aktiválására. [2]

Helyi jelzésadók

Céljuk a környezet és a helyi élőerős védelem figyelmének hang- és/vagy fény-jelzéssel történő felhívása a behatolási-, rablási kísérletre, támadásra. [6]

Kezelőegységek

A behatolás jelző rendszerek kezelőegységei biztosítják a felhasználó/telepítő és a behatolás jelző rendszer közötti kapcsolatot. Lehetővé teszik a kezelői beavatkozást, a rendszer üzemállapotainak átváltását, működési paramétereinek megváltoztatását, átprogramozását, megjelenítik a rendszer és a rendszer elemeinek állapotait. [7]

---

[1] Az IP (Ingress Protection) jelentése behatolás elleni védelem, az elektronikát védő tokozás (készülékház) környezeti behatások elleni védettségét jelzik vele. Az IP besorolást az IEC 60529 szabvány írja le, amelyet gyakorlati tesztek alapján határoztak meg. Az első számjegy a szilárd testek elleni, a második a vízzel szembeni védettségre vonatkozik. A magasabb szám mindkét esetben jobb védettséget jelent.

[2] A felületvédelem eszközeinek követelményeit az MSZ EN 50131-2-6, és 2-7 szabványsorozat tartalmazza. [4], [5]

[3] A közeledő vagy távolodó testről visszaverődő hullámok hullámhossza (és frekvenciája) megváltozik; ezt alkalmazzuk a Doppler elven működő érzékelőknél a mozgás érzékelésére.

A vezetékes rendszerek kezelőegységei adatbuszon, vagy a „kezelői buszon” keresztül kommunikálnak a behatolás jelző központtal. Az adatátvitel a kezelőegységek esetében nem szabványosított, gyártó-specifikus egyedi protokollokkal történik.

Kiegészítő/bővítő modulok

A behatolásjelző központok tipikusan moduláris felépítésűek, azaz adatbuszon keresztül fogadják a legkülönbözőbb bővítő modulokat. Ezek jellemzően bemeneti/kimeneti bővítő modulok, kommunikációs modulok, segédtáp és egyéb speciális modulok.

A JELZŐRENDSZER BIZTONSÁGI SZINTJÉT BEFOLYÁSOLÓ MŰSZAKI TÉNYEZŐK

A CENELEC TC 79 Riasztórendszerek Műszaki Bizottság által készített a rendszerkövetelményekről szóló MSZ EN 50131-1 szabványban megtalálható a behatolásjelző rendszerre vonatkozó biztonsági fokozatok ismertetése. A szabvány négy biztonsági fokozatot jelöl meg. Az egyes a legalacsonyabb, a négyes a legmagasabb biztonsági szintnek felel meg. A szakmában gyakran Grade_1-től, Grade_4-ig emlegetik e fokozatokat. A szabvány az alább tárgyalt, biztonsági szintet befolyásoló tényezőket elemzi, ill. fogalmaz meg követelményeket velük szemben. [8]

Funkcionális követelmények

Ez alatt a behatolásjelzés és a támadásjelzés feldolgozását, valamint az egész rendszerre kiterjedő szabotázsérzékelést kell érteni. Részletesen foglalkozik a szabvány azzal, hogy a különböző hibákat milyen biztonsági besorolású szintű rendszernek kötelező érzékelni. Lásd 1. táblázat

Hibák	**1. fokozat**	**2. fokozat**	**3. fokozat**	**4. fokozat**
Érzékelők	K	K	K	K
Támadásjelző eszközök	K	K	K	K
Elsődleges tápáramforrás	K	K	K	K
Másodlagos tápáramforrás	K	K	K	K
Összeköttetések	K	K	K	K
Riasztásátviteli rendszerek	K	K	K	K
Figyelemfelhívó eszközök	K	K	K	K
Egyéb hibák	V	V	V	V
Jelmagyarázat: A hibafelismerés K= kötelező V=választható				

1. táblázat.

Egyéb funkciók címén foglalkozik a mozgásérzékelők kitakarás érzékelésével (3. és 4. fokozatnál előírás). Üzemeltetői szempontból fontos, hogy a kezelő legyen világos, áttekinthető, erre a szabvány is utal. A hozzáférési prioritást tekintve, a szabványban négy felhasználói hozzáférési szint van definiálva. Lásd 2. táblázat

Funkciók	Hozzáférési szintek			
	1.	2.	3.	4.
Élesítés	K	K	K	K
Hatástalanítás	K	K	K	K
Riasztás visszaállítás	K	K	K	K
Riasztás funkciók ellenőrzése	K	K	K	K
Eseménynapló lekérdezés	K	K	K	K
Tiltás/kizárás/felülbírálás	K	K	K	K
jogosultsági kódok cseréje	K	K	K	K
2. szintű felhasználói kódcsere	V	V	V	V
helyszíni paraméterek cseréje	K	K	K	K
Alapprogram módosítása	K	K	K	K
Jelmagyarázat:	E= engedélyezett NE=nem engedélyezett			

2. táblázat.

A rendszerben az azonosítást végző jogosultsági kódokkal szemben támasztott követelményeket a 3. táblázat tartalmazza.

	2.,3. és 4. hozzáférési szinten az eltérő kombinációk minimális száma			
	1. biztonsági fokozat	2. biztonsági fokozat	3. biztonsági fokozat	4. biztonsági fokozat
Logikai kulcs	1000	10000	100000	1000000
Mechanikai kulcs	300	3000	15000	50000

3. táblázat.

A különböző biztonsági szinteknél, meghatározták azokat a feltételeket, amikor a rendszer egészének, ill. egy részének élesítését meg kell akadályozni. Lásd 4. táblázat

Az élesítés megakadályozás feltételei	1. fokozat	2. fokozat	3. fokozat	4. fokozat
Behatolásjelző érzékelő aktív	K	K	K	K
Támadásjelző eszközök aktív	K	K	K	K
Mozgásérzékelő kitakart állapotban	V	V	K	K
Mozgásérzékelő érzékelési tartomány csökkenés	V	V	V	K
Behatolásjelző érzékelő hiba	V	K	K	K
Szabotázs állapot	V	K	K	K
Összeköttetések hiba	V	K	K	K
Elsődleges tápáramforrás hiba	V	K	K	K
Másodlagos tápáramforrás hiba	V	K	K	K
Riasztásátviteli rendszerek hiba	V	K	K	K
Figyelemfelhívó eszközök hiba	K	K	K	K
Egyéb hibák	V	K	K	K
Jelmagyarázat:	K= kötelező V=választható			

4. táblázat.

A rendszer lehetőséget ad, az automatikus élesítés akadályozás felülbírálatára, a megfelelő hozzáférési szintű kóddal rendelkező felhasználó számára.

Az élesítés megakadályozás felülbírálása	1. fokozat	2. fokozat	3. fokozat	4. fokozat
Behatolásjelző érzékelő aktív állapotában	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint
Támadásjelző eszközök aktív állapotában	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint
Mozgásérzékelő kitakart állapotban	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint
Mozgásérzékelő érzékelési tartomány csökkenés állapotában	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint
Behatolásjelző érzékelő hiba	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint
Szabotázs állapot	2. hozzáférési szint	2. hozzáférési szint	3. hozzáférési szint	3. hozzáférési szint
Összeköttetések hiba	2. hozzáférési szint	2. hozzáférési szint	3. hozzáférési szint	3. hozzáférési szint
Elsődleges tápáramforrás hiba	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint
Másodlagos tápáramforrás hiba	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint	3. hozzáférési szint
Riasztásátviteli rendszerek hiba	2. hozzáférési szint	2. hozzáférési szint	3. hozzáférési szint	3. hozzáférési szint
Figyelemfelhívó eszközök hiba	2. hozzáférési szint	2. hozzáférési szint	3. hozzáférési szint	3. hozzáférési szint
Egyéb hibák	2. hozzáférési szint	2. hozzáférési szint	2. hozzáférési szint	3. hozzáférési szint

5. táblázat.

A rendszer hatástalanítására vonatkozóan a belépési késleltetés maximális idejét 45 másodpercben jelöli meg. A visszaállítási jogosultságot is korlátozza, azaz csak a 2. vagy 3. hozzáférési szinttel rendelkező kezelő végezhet visszaállítást. Ennél szigorúbb feltételhez 3. hozzáférési szinthez köti a szabotázs, ill. a hibaüzenet törlését a Grade_3 és Grade_4 rendszerekben.

A kizárás, vagy az elterjedt angol kifejezéssel, bypass funkciót Grade_1. és Grade_2. esetén 2. vagy 3. szintű hozzáféréshez kötik, míg ennél magasabb biztonsági fokozatú rendszereknél csak a 3. szintű hozzáféréssel rendelkező felhasználónak engedélyezi.

Nem ismertetem, de részletesen tárgyalja a szabvány a kijelző/kezelő egységen látható jelzések engedélyezését/tiltását a különböző rendszerállapotok (hatástalanított/éles/ riasztásiállapot/hibaállapot stb.) szerint, a különböző biztonsági szintű rendszerekre lebontva.

Mint a bevezetőben láttuk, a behatolásjelző rendszereknek elsődleges feladata a behatolás, ill. támadás esetén történő jelzés, amit helyi hang- fényjelzővel és/vagy távfelügyeleti átjelzéssel oldhatunk meg. A helyi figyelemfelhívó eszköz lehet távtáplált, ami biztonsági szempontból a gyengébb megoldás, ill. saját tápellátású, azaz belső akkumulátoros változat. A távfelügyeleti kommunikátor egység, melyet a szabvány riasztásátviteli rendszernek nevez és ATS4 rövidítéssel használ, lehet egy, vagy több átviteli utat használó eszköz. Így beszélhetünk fő, vagy elsődleges ATS-ről és az átviteli biztonságot növelő párhuzamos utat biztosító kiegészítő, vagy másodlagos ATS-ről. Az egyes ATS-ek teljesítőképességét öt paraméter szerint csoportosították.

Ezek:

- Átviteli időtartam várható értéke
- A maximális átviteli idő

[4] ATS: Alarm Transmission System, riasztásátviteli rendszer

- Jelentési időköz (ilyen sűrűn kell tesztelni az átvitelt)
- Helyettesítési biztonság (az átviteli csatorna jogosulatlan helyettesítése elleni védelem)
- Információ biztonság (az átvitt jelzés olvasása és/vagy módosítása elleni védelem)

Ezen követelmények szerint hat csoportot definiáltak ATS1-től ATS6-ig, ahol a ATS6 a legmagasabb követelmény szintet jelenti.5

Ezek a helyi, ill. távfelügyeleti jelző eszközök, több különböző kombinációban tehetnek eleget az egyes biztonsági szintek előírásainak. Ezeket a kombinációkat a 6. táblázat-ban egyes opciók jelölik.

Értesítés eszköze	**1. fokozat**			**2. fokozat**				**3. fokozat**				**4. fokozat**			
	opciók			**opciók**				**opciók**				**opciók**			
	A	B	C	A	B	C	D	A	B	C	D	A	B	C	D
Távtáplált hangjelző	2	V	V	2	V	V	V	2	V	V	V	2	V	V	V
Saját táplálású hangjelző	V	1	V	V	1	V	V	V	1	V	V	V	1	V	V
Fő ATS	V	V	ATS 1	ATS2	ATS2	ATS 2	ATS 3	ATS 4	ATS 4	ATS 4	ATS 5	ATS 5	ATS 5	ATS 5	ATS 6
Kiegészítő ATS	V	V	V	V	V	ATS 1	V	V	V	ATS 3	V	V	V	ATS 4	V
Jelmagyarázat	V = választható, de nem kötelező														

6. táblázat.

Fontos megjegyezni, hogy a figyelemfelhívó eszköz működését le szabad tiltani, pl. egy támadásjelző aktiválásánál (csendes riasztás). Ha egy rendszerben van hang- fényjelző és ATS is, akkor a hangjelző működését maximum 10 percig késleltethetjük, sőt az indítás elhagyható, ha távfelügyeletről az ATS-en nyugtázás érkezett.

A hangjelző működési ideje minimum 90 másodperc, maximum 15 perc lehet. Megjegyzem még, hogy a hálózati kimaradás átjelzése maximum egy óra hosszat késleltethető.

Szabotázs elleni védelem

A behatolásjelző rendszernél a szabotázs elleni védelem azt jelenti, hogy a részegységek el vannak látva olyan eszközzel, ami meggátolja a belső elemekhez való hozzáférést, manipulálást. A szabotázsvédelemre vonatkozó követelmények a rendszer biztonsági fokozatától és attól függenek, hogy az adott részegység a felügyelt téren belül, vagy kívül van.

Általánosságban elmondható, tehát minden biztonsági szintre igaz, hogy a CIE/ACE/SPT/WD/PS[6] eszközöket mindig el kell látni szabotázsvédelemmel. A támadásjelzőket és az érzékelőket a 2. fokozattól fölfelé, a kötődobozokat a 3. fokozattól kötelező szabotázs ellen védeni. A szabotázsvédelemnek mind élesített, mind hatástalanított állapotban működnie kell. Azt hogy milyen események minősülnek szabotázsnak a 7. táblázat tartalmazza.

[5] A teljesítőképességi követelményeket részletesen az EN 50136-1-1 tartalmazza

[6] CIE: Control and Indicating Equipment, vezérlő és kijelző eszköz. ACE: Ancillary Conrtol Equipment, kiegészítő vezérlő. SPT: Supervised Premises Transcecier, felügyelt rádiós átjelző. WD: Warning Device, figyelemfelhívó eszköz. PS: Power Supply, tápegység

Szabotázsesemények	1. fokozat	2. fokozat	3. fokozat	4. fokozat
Egyszerű eszközzel történő kinyitás	K	K	K	K
Vezeték nélküli eszköz eltávolítása a felszerelési helyről	V	K	K	K
Vezetékes eszköz eltávolítása a felszerelési helyről	V	V	K	K
Behatolás a figyelemfelhívó eszközbe	V	V	V	K
Behatolás a CIE/ACE/SPT eszközbe	V	V	V	K
Érzékelő érzékelési irányának megváltoztatása	V	V	K	K
Jelmagyarázat: K= kötelező V=választható				

7. táblázat.

A fentieken túl a 4. biztonsági fokozatú rendszernél elvárás, hogy akár élesített, akár hatástalanított állapotú, a részegységek helyettesítését érzékelje és szabotázsnak tekintse. Időkorlátot is szabtak a helyettesítés érzékelésére. 4. fokozatnál 10 másodpercen belül érzékelnie kell a helyettesítést. Bár a 3. fokozatnál nincs kötelezően előírva az érzékelés, de ha tudja a rendszer, akkor ott 100 másodperc ez az időkorlát.

Rendszerelemek közötti összeköttetés vizsgálat

A biztonsági követelmények közül talán legnehezebb, az elemek közötti összeköttetés követelményrendszerének a megfogalmazása. Általánosságban elmondhatjuk, hogy a rendszer elemei között a kommunikáció legyen gyors és biztonságos. az összeköttetéseket úgy kell tervezni, hogy a lehető legkisebb legyen a jelzések és üzenetek késedelmének, módosulásának, helyettesítésének vagy elvesztésének lehetősége. Ezért legyen szó vezetékes, vagy vezeték nélküli behatolásjelző rendszerről, a részegységek közötti összeköttetéseket ellenőrizni, figyelni kell.

A megfigyelés célja, hogy kimutassák, hogy eleget tesz-e az összeköttetés a rendelkezésre állás követelményeinek. Vezetékes rendszereknél természetesnek vesszük az összeköttetések folyamatos rendelkezésre állását, de a manapság egyre terjedő rádiós rendszereknél energia ellátási okok miatt az összeköttetés megfigyelése időszakos. Tehát legyen szó vezetékes, vagy rádiós rendszerről a 8. táblázat meghatározza, mennyi lehet a leghosszabb megengedett időtartam, ameddig egy összeköttetés nem áll rendelkezésre. Ha egy összeköttetés a megengedett időn túl nem áll rendelkezésre, szabotázs vagy hibajelzést kell létrehozni, a 11. táblázat első sora szerint.

	1. fokozat	2. fokozat	3. fokozat	4. fokozat
A rendelkezésre nem állás leghosszabb megengedett időtartama	100 s	100 s	100 s	10 s

8. táblázat.

Az 1. 2. fokozatú behatolásjelző rendszereknél megengedett a rendelkezésre állás indirekt ellenőrzése, azaz az átviteli közeget figyelem meg, hogy kimutassam annak rendelkezésre állását a jelzések továbbítására (tipikusan rádiós rendszereknél használják).

A rendelkezésre álláson túl, az összeköttetés épségét folytonosan 9. táblázatban meghatározottnál nem nagyobb időközönként ellenőrizni kell.

1. Ha a rendszer azonosított hibaállapotban van, és e-miatt nem tudja ellenőrizni a kommunikációt, erről hibaüzenetet kell létrehozni a 11. táblázat második sora szerint.
2. Ha a rendszerben nincs azonosított hiba, de nem tudja ellenőrizni a kommunikációt, erről szintén hibaüzenetet kell létrehozni a 11. táblázat harmadik sorának megfelelően.

	1. fokozat	2. fokozat	3. fokozat	4. fokozat
A rendszeres kommunikációs jelzések vagy üzenetek között megengedett leghosszabb időköz	240 perc	120 perc	100 s	10 s

9. táblázat.

A rendszerben a legutolsó ellenőrző jelzés, vagy üzenet óta eltelt idő az élesítés folyamatát is befolyásolhatja. Meg kell akadályozni az élesítést, ha az eltelt idő meghaladja a 10. táblázatban a különböző biztonsági szintekre meghatározott értéket.

	1. fokozat	2. fokozat	3. fokozat	4. fokozat
A megengedett legnagyobb időköz a legutolsó jelzés vagy üzenet vétele után	60 perc	20 perc	60 s	10 s

10. táblázat.

A 4. biztonsági fokozatú rendszereknél, külön előírás van a kommunikáció biztonságára. Ezen a biztonsági szinten a rendszernek kell tartalmazni olyan eszközt, ami a jelzések és üzenetek késedelmét, módosulását, helyettesítését vagy elvesztését, 20 másodpercen belül kimutatja. Erről a 11. táblázat utolsó sora szerint hiba vagy szabotázsjelzést, vagy üzenetet kell létrehozni.

Követelmények	1. fokozat	2. fokozat	3. fokozat	4. fokozat
Összeköttetések megfigyelése	Sz vagy H	Sz vagy H	Sz	Sz
Rendszeres kommunikáció 3.3. a)	H	H	H	H
Rendszeres kommunikáció 3.3. b)	Sz vagy H	Sz vagy H	Sz	Sz
A kommunikáció biztonsága	Sz vagy H	Sz vagy H	Sz	Sz
Jelmagyarázat: Sz=szabotázs H=hiba (-jelzés vagy üzenet)				

11. táblázat.

A biztonsági fokozattól függően a behatolásjelző rendszernek a 13. táblázatban meghatározott eseményeket naplózni kell. Az eseménytár méretére a 12. táblázat ad útmutatást. Egy bejegyzésnek tartalmaznia kell az esemény megnevezését, idejét, dátumát.

Memória kapacitás és megőrzés	1. fokozat	2. fokozat	3. fokozat	4. fokozat
A naplózható események legkisebb száma	V	250 esemény	500 esemény	1000 esemény
Memóriatartalom megőrzési ideje tápellátás kiesése után legalább	V	30 nap	30 nap	30 nap
Jelmagyarázat: V=választható				

12. táblázat.

Általános funkciók	1. fokozat	2. fokozat	3. fokozat	4. fokozat
Felhasználó azonosítás élesítéskor/hatástalanításkor	V	V	K	K
Rendszer élesített/részben élesített	V	K	K	K
Rendszer hatástalanított	V	K	K	K
Támadásjelzési állapot	V	K	K	K
Támadásjelző zóna azonosítása	V	V	K	K
Behatolás riasztási állapot	V	K	K	K
Behatolásjelző zóna azonosítása	V	V	K	K
Szabotázs-riasztási állapot	V	K	K	K
érékelők egyedi azonosítása	V	V	K	K
Zóna tiltása	V	K	K	K
Zóna kizárása	V	K	K	K
Érzékelő hibajelzés	V	V	K	K
Támadásjelző hibajelzés	V	V	K	K
Elsődleges tápegység hibajelzés	K	K	K	K
Másodlagos tápegység hibajelzés	V	V	K	K
Összeköttetés hibajelzés	V	K	K	K
Riasztásátviteli rendszer hibajelzés	V	K	K	K
Figyelemfelhívó eszköz hibajelzés	V	K	K	K
Egyéb hibajelzés	V	V	V	V
Élesítés megakadályozás felülbírálása	V	K	K	K
Elsőként riasztást adó érzékelő azonosítása	V	K	K	K
Telepcsere szükséges (csak szárazelem esetén)	V	V	K	K
Felülbírált zóna/érzékelő	V	K	K	K
Időpont és dátum módosítása	V	V	K	K
Helyszínspecifikus adatok módosítása	V	V	K	K
2. szintű felhasználó cseréje egy 3. hozzáférésű szintűnek	V	K	K	K
Részegységek helyettesítésének detektálása	V	V	V	K
Jelmagyarázat: K= kötelező V=választható				

13. táblázat.

Tápellátás követelményei

A szabvány három különböző típusú tápegységet definiál. [9]

Az „A típus” amikor egy elsődleges tápáramforrás, tipikusan a hálózat, a behatolásjelző rendszer által automatikusan tölt egy másodlagos áramforrást, pl. akkumulátort.

A „B típus” annyiban különbözik, hogy a másodlagos tápáramforrást pl. akkumulátort nem a behatolásjelző rendszer tölti.

A „C típus ” amikor véges kapacitású elsődleges tápáramforrást használunk, ez tipikusan egy, vagy több nem tölthető szárazelem.

Követelményként jelentkezik, hogy a rendszer az elsődleges és másodlagos tápáramforrás közötti átkapcsolása nem befolyásolhatja a rendszer állapotát. Ha a behatolásjelző rendszerben „C típusú” tápáramforrás van, az legyen képes biztosítani a rendszer energiaszükségletét legalább egy évig, bármely használati körülmény esetén, és rendelkezzen alacsony feszültség jelzéssel. Áthidalási időtartamnak nevezzük az elsődleges tápáramforrás kiesése esetén azt az időtartamot ameddig a másodlagos tápáramforrás képes energiával ellátni a rendszert. A

minimális áthidalási időre vonatkozó előírás 1. és 2. biztonsági fokozatnál „A típusú” tápegységre 12 óra „B típusú” tápegységre 24 óra. A 3. és 4. fokozatnál „A típusú” tápegységre 60 óra „B típusú” tápegységre 120 óra, amely időtartam megfelezhető, ha a táplálás hibájáról értesítésküldés történik a távfelügyeleti központba..

Amennyiben az elsődleges tápáramforrás, jellemzően a hálózat az objektumban elsődleges kiegészítő tápáramforrással pl. automatikusan induló generátorral (szünetmentesített hálózat) rendelkezik, a behatolásjelző rendszer áthidalási időtartama 4 órára csökkenthető.

Az „A típusú” tápegységnek, újra kell tudni tölteni a másodlagos tápáramforrását, azaz az akkumulátort, legalább a maximális kapacitás 80 %-ig, a 14. táblázatban megadott időtartamon belül. Ezt nevezzük maximális újratöltési időnek.

A típusú tápegység	1. fokozat	2. fokozat	3. fokozat	4. fokozat
Maximális újratöltési időtartam	72 óra	72 óra	24 óra	24 óra

14. táblázat.

Természetesen van jó néhány olyan általános követelmény, amely az összes biztonsági fokozatba sorolt rendszerre egyaránt érvényes. Ezek az üzemeltetési, vagy a funkcionális megbízhatóságra vonatkoznak, ill. a környezetállósági követelményeket, vagy a elektromágneses összeférhetőséget taglalják. Ezeket nem részletezem, mert a biztonsági osztályba sorolást nem befolyásolják.

A BEHATOLÁSJELZŐ RENDSZER VÉDELMI KONCEPCIÓJÁNAK HATÁSA BIZTONSÁGI SZINTRE

Egy behatolásjelző rendszer biztonsági szintjét, az objektumban és a környékén elhelyezett érzékelők és a velük teljesen, vagy részlegesen lefedett védelmi körök befolyásolják meghatározó módon. A védelmi köröket a rendszer tervezésekor, a védelmi koncepció alapján alakítjuk ki. Az objektumok sokfélesége, ill. a jelzőrendszer célja, számtalan kialakítást tesz lehetővé. Az érzékelők száma, elhelyezkedése és persze milyensége, mind hatással van a biztonsági szintre. [10]

Vizsgáljuk meg részletesen a behatolás-érzékelők többkörös elrendezését. A kültéri védelem tartalmazhat elektronikai kerítésvédelmet és/vagy kültéri térvédelmet. Ezek lehetnek teljes körű, vagy részleges kialakításúak.

A következő védelmi kör az objektum felületvédelme. Itt megkülönböztethetünk funkcionálisan ki-be jutásra alkalmas nyílászárókat (ajtókat), ill. funkcionálisan közlekedésre nem alkalmas nyílászárókat, amelyek azért könnyen támadhatók (ablakok), és az objektum egyéb épületszerkezetekkel határolt részeit, mint falazat, tető és padozat. E harmadik csoport kialakításánál, vagy elhelyezkedésénél fogva, néhány kivételtől eltekintve (pl. üvegportál), relatív magas szintű mechanikai védelmet biztosít, ezek elektronikai érzékelőkkel (falbontás-érzékelővel) való ellátása csak kiemelt biztonsági szintnél szükséges.

A legáltalánosabban alkalmazott védelmi kör a beltéri térvédelem. Ez képezi szinte minden behatolásjelző rendszer alapját. Tipikus érzékelői a különböző elven működő mozgásérzékelők. Ezeket teljes körűen, teljes lefedéssel, vagy csapdaszerűen, részleges védelem kialakítására használjuk.

Az objektum jellege, kialakítása és a használat célja dönti el, hogy szükség van-e a speciális védelmi körnek számító tárgy, ill. személyvédelemre. Ha egy bankfiókot, vagy egy katonai kutatólaboratóriumot veszünk példának, akkor mindkettőre szükség van. A bankban a pénzt, a laboratóriumban a mintákat és a kutatási eredményeket páncélszekrényben tartjuk. Ennek a

jelzőrendszerbe kötött érzékelői egy külön védelmi kört képez az objektumon belül, nehezítve ezzel az illetéktelen hozzáférést.

A személyvédelemre is jó példa a fenti két objektum, hiszen a bankban a pénztárosok vannak támadásnak kitéve, a kutató laborban például a portaszolgálatot fenyegeti ilyen veszély. Az itt dolgozó személyek részére a támadásjelzés lehetőségét, mint az elektronikai jelzőrendszer személyvédelmi funkcióját biztosítani kell.

KÖVETKEZTETÉSEK, PROBLÉMAFELVETÉS

Egy elektronikai jelzőrendszer biztonsági szintje, azt a védelmi képességet fejezi ki, hogy a védett objektumban a különböző szintű fenyegetéseket milyen megbízhatósággal jelzi.

Mint láttuk a behatolásjelző rendszer az elektronikai vagyonvédelmi jelzőrendszerek egy fajtája. A konkrét rendszer által megvalósított biztonsági szintet nagyon sok tényező befolyásolja. Cikkemben megkíséreltem összegyűjteni azokat a műszaki jellemzőket, ill. a rendszer kialakítására jellemző struktúrákat, melyek alapvetően hatással vannak a biztonsági szintre

Ha ezen tényezőket számszerűen tudjuk jellemezni, akkor egy olyan eszközt kapunk, mellyel az objektumok vagyonvédelmi rendszerei a védelmi szint szempontjából, azaz biztonsági szempontból összehasonlíthatóak, mérhetőek lesznek. A további kutatásom arra irányul, hogy kidolgozzam ennek a számszerű jellemzésnek a rendszerét.

Felhasznált irodalom

[1] Tóth Levente: CCTV magyarul, BM Nyomda, 2004. Budapest

[2] Utassy Sándor Komplex villamos rendszerek biztonságtechnikai kérdései Doktori (PhD) értekezés, 2009 Budapest

[3] Alarm Systems – Combined and integrated alarm systems – Generalrequirements Final Draft CLC/FprTS 50398:2008

[4] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 2-6. rész:Nyitásérzékelők, MSZ EN 50131-2-6:2008, (angol nyelvű)

[5] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 2-7-1. rész: Üvegtörés érzékelők, MSZ EN 50131-2-7:2008,

[6] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 4. rész:Figyelemfelhívó eszközök, MSZ EN 50131-4:2009

[7] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 3. rész: Vezérlő- és kijelző berendezés, MSZ EN 50131-3:2009

[8] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 1. rész: Rendszerkövetelmények, MSZ EN 50131-1:2011

[9] Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 6. rész: Tápegységek, MSZ EN 50131-6:2006

[10] Dr. Lukács György szerkesztő: Új Vagyonvédelmi Nagykönyv, Cedit 2000 Kft, 2002. Budapest