Óbudai Egyetem

Doktori (PhD) értekezés

Elektronikus megfigyelő-, és ellenőrző rendszerek objektumorientált kialakítása különös tekintettel a biztonsági kockázatok rendszerére

Horváth Tamás

Témavezető: Prof. Dr. Kovács Tibor

Biztonságtudományi Doktori Iskola

Budapest, 2018.

Szigorlati Bizottság:

Elnök:

Prof. Dr. Berek Lajos egyetemi tanár

Tagok:

Dr. Simon Ákos ny. egyetemi docens

Dr. Kiss Sándor ny. egyetemi docens

Nyilvános védés bizottsága:

Elnök:

Prof. Dr. Berek Lajos egyetemi tanár

Titkár:

Dr. Hanka László adjunktus

Tagok:

Prof. Dr. Simon Ákos ny. egyetemi docens

Dr. Kiss Sándor ny. egyetemi docens

Dr. habil. Farkas Tibor egyetemi docens

Bírálók:

Dr. Nagy Rudolf

Dr. Takács Szabolcs

Nyilvános védés időpontja

2018.

TARTALOMJEGYZÉK

BEVEZETÉS

Valamennyi, a biztonságtechnikát gyakorlatban művelő szakember számára – akár tervező, akár a kivitelezés folyamatában közvetlenül résztvevő - jelentős kihívást jelent az ipari vagy kereskedelmi létesítmények/intézmények fizikai védelmi rendszerének és biztonsági kockázatainak az értékelése. Ezek az elemzések a tervezés meghatározó alappillérei.

A dinamikusan változó biztonsági kockázatok és a környezeti feltételek a már meglévő védelmi rendszerek rendszeres és eseti felülvizsgálatára, auditjára kényszerítik a tulajdonosokat és az üzemeltetőket. Ezeket a mértékadó gazdasági társaságok, nemzeti és üzleti szempontból érzékeny adatokkal tevékenykedő vállalatok végre is hajtják. Minthogy azonban nem rendelkeznek egy egységesen elfogadott irányelv-rendszerrel, ennek hiányában kénytelenek a biztonsági szakemberek javaslataiban megbízni, így viszont nehezen ellenőrizhetők számukra a kockázatarányos védelmi igények. Ugyanezen elveknek megfelelő egységes szabványok, valamint a tervezési elvek hiánya a szakemberek számára is nehézséget jelentenek, mert igen gyakran csak magyarázkodásnak tűnő vitakörnyezetben tudják a szakmai érveiket indokolni. Az üzemeltető szakemberek számára a vállalati biztonságért felelős munkatársak sem tudnak megfelelő szakmai érveket találni az egyes fejlesztésekre. Így fordulhat elő, hogy adott vállalati vezetők a pillanatnyi gazdasági érdekek mentén döntenek igen gyakran a biztonság rovására.

Disszertációmban arra vállalkozom, hogy az egyes fizikai védelmi fejlesztési, tervezési és üzemeltetési folyamatban résztvevők számára egy átfogó, érthető, a biztonságtechnikában jól használható, átlátható kockázatértékelési módszert dolgozzak ki. Ennek segítségével egy adott létesítmény/intézmény aktuális biztonsági kockázatainak értékelését követően egyértelműen láthatók lesznek azok a veszélyek, amelyeket kezelni kell. A kockázatértékelés folyamán a kockázatkezelés tekintetében megfogalmazódnak támpontok, amelyek segíthetik a biztonsági területen tevékenykedő szakembereket.

A kockázatértékeléssel foglalkozó fejezetben hat létesítmény biztonsági kockázatait magában foglaló értékelést végre is hajtok. Ezek valós adatokra épülnek, így azok üzleti és biztonsági szempontokból érzékeny információnak számítanak.

Értekezésem második részében egy általam kidolgozott és összeállított feltételrendszer tanulmányozható: ezt - minimális követelményként - célszerű követni az egyes biztonsági kockázatú létesítmények esetében.

A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

Szakmai pályafutásom jelentős részében biztonságtechnikai rendszerek tervezésével, telepítésével, fejlesztésével és üzemeltetésével foglalkoztam.

Munkáim során azt tapasztaltam, hogy a különböző biztonsági kockázatú létesítményekben telepítendő, illetve telepített biztonságtechnikai berendezések (behatolásjelző; beléptető és *videó megfigyelő rendszerek*) alkalmazhatóságának értékelése jelenleg nem egységesen megoldott. Kérdés, hogy ezek a rendszerek megfelelnek-e a szakmai-megbízói elvárásoknak, egyúttal képesek-e a létesítmények biztonsági kockázatainak kezelésére. Természetesen lehetőség van különböző biztonsági auditok elkészítésére, de az ellenőrzések, felülvizsgálatok - főként biztonságtechnikai szempontból - nem azonos alapról indulnak. Ennek oka, hogy nem állnak rendelkezésre általános érvényű objektum-specifikus tervezési, és kivitelezési alapelvek. Egy egységes elvrendszer kidolgozása meghatározó támogatást biztosít mind a megbízói, mind a tervezői oldal számára már az elvárások szintjén is. Ugyanakkor jelentős segítség a megbízói oldal üzemeltetői számára a biztonsági kockázatok aktualizálásából adódó esetleges módosítások, biztonságtechnikai fejlesztések, azok irányai és részletei meghatározásában is.

Mind a szakemberek, mind a Megbízók számára alapvető támogatást jelent egy, a biztonsági kockázatokkal arányos minimális követelményrendszer kidolgozása, amely egyértelműen meghatározza az elvárt védelmi, biztonságtechnikai rendszerkövetelményeket. Ezen a terülten jelenleg nincsenek megfogalmazott elvárások, kialakítási elvek, miközben az angol nyelvű szakirodalomban találhatunk különböző „best practices – jó megoldások” elnevezésű útmutatókat, amelyek esetenként jól fogalmazzák meg azokat a biztonsági kockázatkezelési igényeket, melyekkel egy-egy létesítmény üzemeltetése során foglalkozni kell.

KUTATÁSI ELVEK ÉS MOTIVÁCIÓK

Értekezésem megírásában fontos alapelvnek tekintettem, hogy a gyakorlati életben is jól használható, egységes rendszert dolgozzak ki, amelynek segítségével mind a szakemberek, mind az igénybe vevők (felhasználók) érthető és gyakorlatias szempontok szerint legyenek képesek dolgozni, mindemellett pedig áttekintsem a jelenleg elérhető, témához kapcsolódó legfrissebb tudományos eredményeket és a sajátjaimat ezek rendszerébe illesszem.

A munkámból adódóan, hosszú évek óta kerülök szembe azzal a problémával, hogy a biztonságtechnikával foglalkozó szakemberek, a megbízásaik során vagy nem készítenek, vagy nem kapnak az adott létesítmény biztonsági kockázatait értékelő irányadó dokumentációt, amely pedig tervezéskor szükséges. Amennyiben mégis akad ilyen, akkor az általában az elkészítés időpontjában lehetett aktuális és nélkülözi a könnyen „up-to-date" szinten tartás lehetőségét (az elkészített tervek, iránymutatások „kőbevésettek" és rugalmatlanok). Ipari és kereskedelmi létesítmények esetén igen gyakran még egy megalapozott objektumvédelmi tervet sem lehet fellelni, főként akkor, ha arra semmilyen hatósági rendelkezés nincs, vagy nem volt.

A kutatásom egyik fő motivációja az, hogy azon létesítmények számára, amelyek esetében a biztonsági kockázatok azt megkövetelik, egy jól követhető és használható kockázatértékelési módszert és ahhoz közvetlenül kapcsolódó biztonságtechnikai rendszerkialakítási elvet fogalmazzak meg, valamint az általam szolgáltatott rendszer és értékelési javaslat kellő rugalmassággal le tudja követni a piaci igényeket, elvárásokat.

További motivációt jelentett számomra az a lehetőség, hogy egy, a nemzetközi piacon is tevékenykedő nagyvállalat környezetében az általam kialakított követelményrendszer tesztelhető és bevezethető lehet.

Nem feledkezhetem meg arról sem, hogy a kutató munkám során összeállított rendszer informatikai támogatással akár piaci termékké is fejleszthető, hiszen a követelményrendszer adatbázisba szervezhető, szükség esetén bővíthető.

KUTATÁSI CÉLOK

A különböző biztonsági kockázatú létesítményekben telepítendő biztonságtechnikai rendszerek pontos meghatározásához szükséges egy jól alkalmazható, biztonsági kockázatokon alapuló besorolási rendszer kidolgozása. Olyan komplex rendszeré, amely a gyakorlatban támogatást nyújt mind a megbízó, mind a tervező, kivitelező, illetve a rendszer alkalmasságát vizsgáló személyek, szervezetek számára.

További célom a disszertációm elkészítésével, hogy megalkossak egy objektumorientált[1] tervezési és kivitelezési elvrendszert, amely jól követhető alkalmazási normákat jelent a felhasználók széles köre számára.

[1] Az objektumorientált szakkifejezés valójában azon tervezési elvek összességét jelenti, amely az adott létesítmény fizikai védelmi rendszerét a biztonsági kockázatok szerint testre szabja.

AZ ÉRTEKEZÉSEMBEN ELÉRNI KÍVÁNT EREDMÉNYEK

a. Létrehozni egy olyan, a biztonsági kockázatokat értékelő módszert, amely elsősorban a biztonságtechnikai rendszerek tervezéséhez ad támogatást.

A létező kockázatértékelési módszerek közül olyan módszer kiválasztásának van létjogosultsága, amely a megbízó és a megbízott számára is könnyen követhető, jelentős véleményeltérésre okokat nem szolgáltat. Az elsődleges szempontok között kell szerepelnie a generális látásmódnak, amely az adott létesítményeket struktúrában vizsgálja, és a tágabb környezet, társadalmi beágyazódottság ugyanakkora súllyal jelenik meg az értékelésben, mint a belső működési struktúra, személyi feltételek és a minősített adatállomány, vagy a specifikus informatikai hálózat.

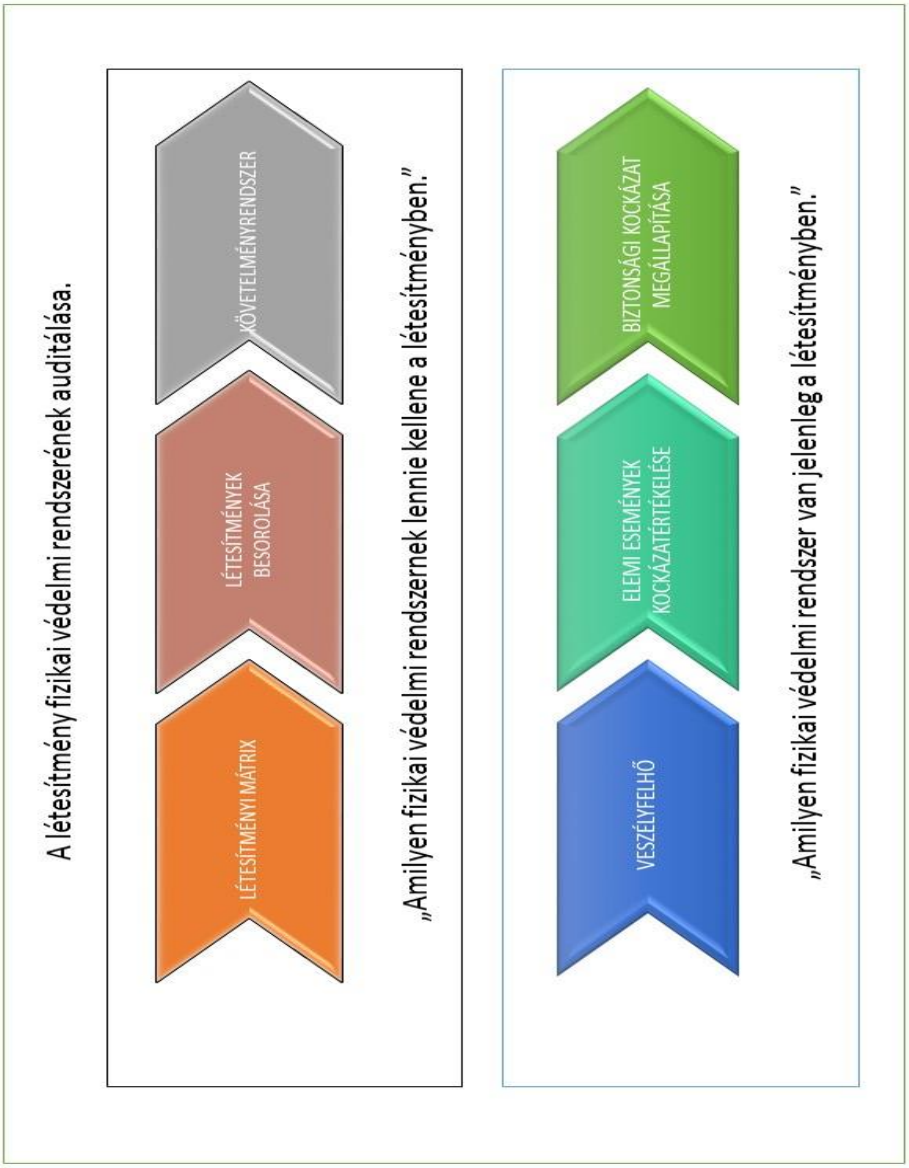
b. Az egyes létesítmények biztonsági kockázatok alapján történő besorolása egy olyan rendszerbe, amelyben ezek biztonsági kockázatai megjelennek egy létesítményi együttható formájában.

A biztonsági kockázatok alapján történő létesítmény-besorolás egységes módszere jelenleg nem létezik. Az elszigetelt, egyedi kockázatértékelések nem teszik összehasonlíthatóvá az egyes létesítmények biztonsági kockázatait, így a biztonságtechnikai rendszerek kivitelezésére felhasznált pénzügyi erőforrások felhasználása sem hatékony.

Egy adott létesítmény biztonsági besorolása jelentős támogatást biztosíthat más biztonsági szakterület (például a munkavédelem) számára is. Létesítményi jellemzőként figyelembe véve a besorolást a nagyvállalatok esetében a munkavédelmi tevékenység összehasonlíthatóvá válhat a különböző veszélyességi környezetben tevékenykedő társaságok esetén is.

c. Megalkotni egy objektív, a biztonsági kockázatokra épülő tervezési segédletet, amely támogatást adhat a biztonságtechnikai rendszerek tervezéséhez, kialakításához.

Egy felhasználóbarát tervezési segédletet mind a megbízó, mind a megbízott könnyen értelmez, a tervezett költségvetés tételeinek ellenőrzése ezáltal áttekinthetővé válik.



1. ábra: A létesítményi kockázat meghatározásának magas szintű folyamata[2]

[2] Létesítményi mátrix: egy adott létesítményre jellemző biztonsági kockázatok értékének meghatározásához használható mátrix. Veszélyfelhő: Az adott létesítmény fizikai védelmi rendszerét, annak működését veszélyeztető kockázatok. Mindkét fogalmat a későbbiekben részletesen tárgyalom.

KUTATÁSI MÓDSZEREK

A napi munkám során biztosított számomra az MVM Magyar Villamos Művek Zrt., illetve az MVM Csoport (17 tagvállalat) egyes létesítményeinek és erőművei objektumvédelmi terveinek egyedi tanulmányozása, valamint az erőművek fizikai védelmi rendszereinek, biztonsági kockázatainak meghatározására irányuló módszerek megismerése.

A primer kutatás során áttekintettem azokat a fellelhető szakkönyveket, amelyek a számomra releváns információkkal szolgálhattak a téma feldolgozásában.

Kutatási munkámat a szekunder fázisban kiterjesztettem a szakkönyvek mellett a szakirodalmi hivatkozások felkutatására. Ennek során elsősorban az Internetes minősített szakanyagokat és természetesen magát a hivatkozott publikációkat tekintettem át, majd a nagyobb külföldi könyvforgalmazók szakkönyv kínálatát, illetve a szakmai tevékenységem során ismertté vált társaságok nyilvánosan fellelhető anyagait.

A szakmai publikációk és szakkönyvek felkutatása és tanulmányozása mellett lehetőségem volt - a kockázatértékelési módszerek között válogatva - a fizikai védelmi rendszerek számára jól használható módszert kiválasztanom és bemutatnom a társaságunk által szervezett szakmai ülésen, a kritikus infrastruktúra fizikai védelmének gyakorlati megvalósításáról tárgyban „Üzemeltetői Biztonsági Terv[3], de a gyakorlatban hogyan?” címmel.

A tercier kutatási szakaszban, lehetőségem volt a nem publikus, az üzleti szempontból érzékeny adatokat tartalmazó, az MVM Magyar Villamos Művek Zrt. vállalatcsoportban érvényben lévő szabályozási rendszert is áttanulmányozni.

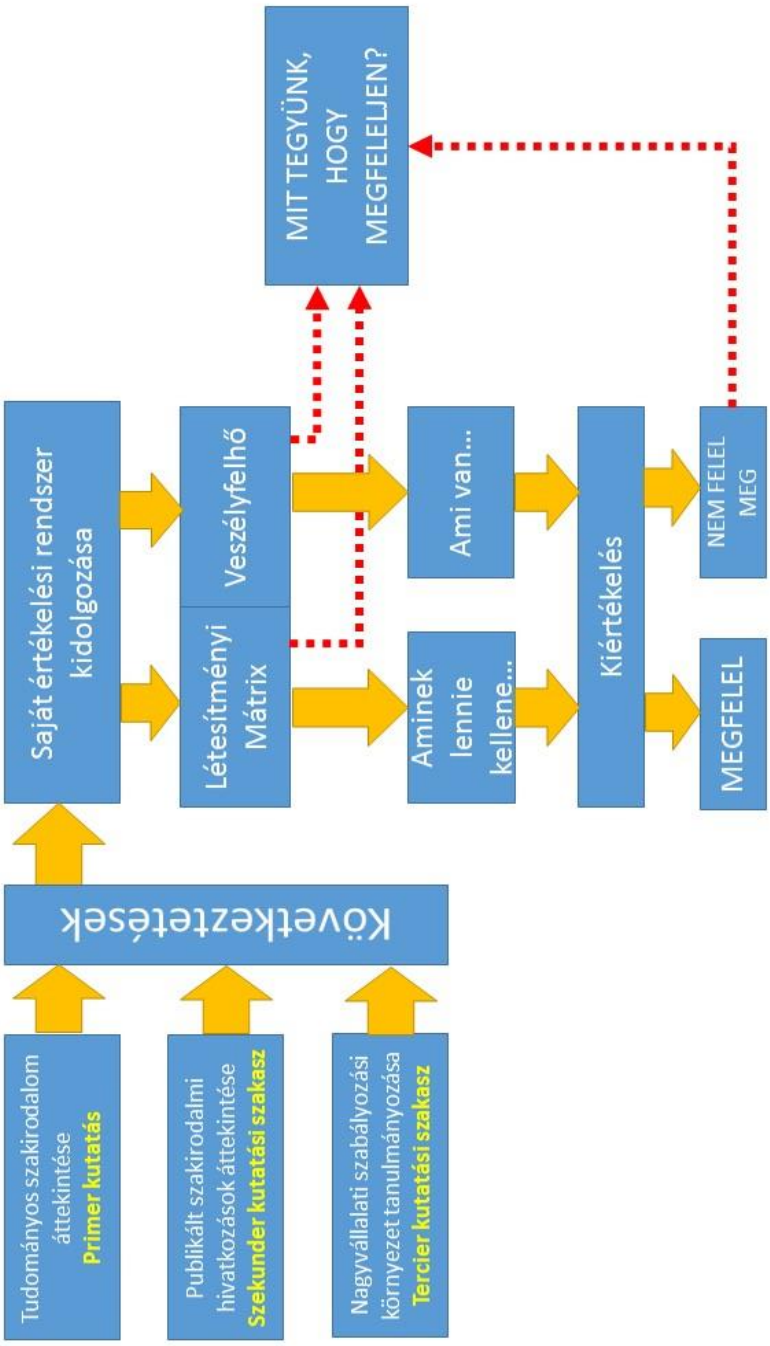
Az 1. ábra mutatja azt a módszertani koncepciót, magas szintű folyamatot, amelyet az értekezésem, kockázatértékelési módszerem kidolgozása során követtem. A 2. ábrán összefoglaltam a teljes módszertani útmutató, melyet az általam megalkotott kockázatértékelési módszer kidolgozása során a disszertációmban követtem a kutatási munkától a vizsgált fizikai védelmi rendszer megfelelőségig, vagy meg nem felelőségig.

[3] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (Lrtv.) az a jogszabály, amely az Üzemeltetői Biztonsági Terv tartalmi követelményeit tárgyalja.

Vizsgálataim során a „normál” üzemi működés mellett az ún. „minősített időszakban” történő fizikai védelmi rendszerek üzemeltetési körülményeinek meghatározása a biztonsági kockázatok változásának függvényében az, amely lehetőséget biztosít a disszertációm elkészítése során végzett kutató munka folytatására.

A kutatási periódust 2017. november 15-én lezártam.

A dőlten szedett fogalmak definíciója a Fogalomtár a fizikai biztonság témaköréhez fejezetben, a mellékletek után található.



2. ábra: A kiértékelési munka és az auditációs munka.

ÁLTALÁNOS MEGGONDOLÁSOK

Szakmai tevékenységem során nagyszámú fizikai védelmi rendszertervezésben, kivitelezésben vettem részt, esetenként tervezőként, esetenként a kivitelező társaság szakmai vezetőjeként, illetve projektmenedzserként. Tapasztalataimra alapozva néhány, jelen disszertációmhoz kapcsolódó, az objektumorientált megfigyelő és ellenőrző rendszerről - a titoktartási kötelezettségeket követve -, egyfajta rövidített követelményi listát adok közre. Teszem mindezt azért, hogy az általam elképzelt és paraméterezett fizikai védelmi rendszerek jobban érthetők legyenek.

A tárgyalt létesítménytípusok esetében saját szakmai tapasztalataimat osztom meg, kitüntetett figyelmet szentelve a nemzeti minősített adatok kezelésének[4], amely elsődlegesen egy atomerőmű fizikai védelmi rendszerének, annak irányadó paramétereinek meghatározásakor jöhet szóba.

Természetesen valamennyi, egyéb létesítmény fizikai védelmi rendszerére vonatkozó információ üzletileg fontos, érzékeny adatnak számít, így konkrétumokat nem, de pontos tervezési elveket, üzemeltetői igényeket meg tudok határozni és arról van is lehetőségem értekezni.

Vagyonvédelem vs fizikai védelem

Fontosnak tartom kiemelni azt a különbséget, amely a fizikai védelmi és a személy-, és vagyonvédelmi rendszerek között áll fenn.

Személy-, és vagyonvédelmi rendszerekről akkor beszélhetünk, ha a biztonsági rendszerek tervezésének és kialakításának az elsődleges célja az adott létesítmény/intézmény vagyonának, az ott dolgozó személyek – esetlegesen az üzemeltető, vagy tulajdonos által meghatározott munkavállalók – védelme. Ezen esetekben nem beszélünk a létesítményben/intézményben alkalmazott technológiáról, míg a fizikai védelem esetén már a létesítményben alkalmazott technológiát is védenünk kell az illetéktelen személyek – behatolók/támadók – tevékenységétől.

Ezt a kritériumrendszert erősíti, és egyben kibővíti Mary Lynn Garcia meghatározása a fizikai védelmi rendszer tekintetében:

[4] Forrás: 2009. évi CLV. törvény a minősített adat védelméről, valamint a 190/2011 (IX.19.) Kormány rendelet az atomenergia alkalmazása körében a fizikai védelmi és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről

"…a physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks." - A fizikai védelmi rendszer integrálja az embereket, eljárásokat és védelmi berendezéseket, létesítményeket az eltulajdonítás, szabotázs és egyéb rosszindulatú támadások ellen. [1]

Ezen egyszerűnek tűnő különbség miatt - amely bonyolult struktúrájú rendszerkialakításhoz is vezethet - van igen nagy jelentősége az értekezésem első részében taglalt tervezési stratégiának (Elrettentés/Meghiúsítás).

Az alkalmazott technológia védelme esetén érdemes megjegyezni, hogy a támadók, behatolók jól kategorizálhatók a fenyegetettség jellege, mértéke szerint. Ezen kategorizálásnak azért lehet fontos szerepe, mert az ellenük való védekezés módjait, lehetőségeit is előre meghatározhatóvá teszi. Példaként az alábbi sematikus kategorizálás támogathatja a kockázatkezelési módszerek kiválasztását:

1. Terrorista. Célja a rombolás, nem anyagi érdekek motiválják, esetenként jól felkészült és felszerelt, valamint sérülés, halál okozása is lehet a járulékos vesztesége (*collateral damage*) cselekedetének.
2. Bűnöző. Célja a haszonszerzés, eszközei korlátozottabbak, de erőszak alkalmazása, valamint halálos következményekkel járó cselekedetek sem kizártak.
3. Vandál. Célja a károkozás és általában nem az anyagi haszonszerzés, kevéssé felszerelt és képzett, személyek elleni erőszakos cselekményeket követ el.
4. Belső elkövető, szabotőr. Célja lehet a bosszú, a károkozás és az anyagi haszonszerzés, általában jól képzett, hiszen belső információkkal rendelkezik, esetenként az első két kategóriával anyagi haszonszerzés reményében együttműködhet, a biztonsági rendszer működésével tisztában lehet, sőt maga is lehet a biztonsági személyzet vagy a vezetés tagja, összejátszhat a beszállítókkal, alvállalkozókkal. Az ellene való védekezés, rendkívül bonyolult és sok nehézséget is okozhat.

A belső elkövető (angol szóhasználatban „*insider*") szerepe kiemelkedően fontos lehet a magas és a fokozott biztonsági kockázatú létesítményi kategóriában, ugyanis a károkozás felmérhetetlen. Gondoljuk csak azt el, ha egy belső elkövető egy terroristatámadást készít elő és támogat egy atomerőműben. Nem kérdés, hogy a károkozásuk együttes hatása beláthatatlan következ-

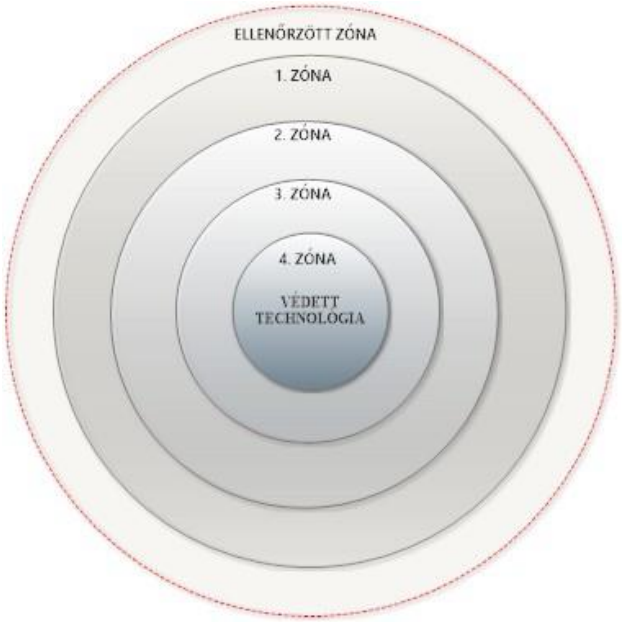
ményekkel járhat akár egy egész régió vagy akár kontinens számára is. Ezen okok miatt a Nemzetközi Atomenergia Ügynökség fizikai védelmi szabályrendszerében (NNS13[5]) kiemelkedő szerepe van a belső elkövető felderítésének, és ha szükséges tevékenysége megakadályozásának [2].

Nincsenek a villamos erőművekben kialakítandó fizikai védelmi rendszerre vonatkozó egységes szabályok. Azokat az üzemeltető biztonsági szakterületnek, szervezetnek kell meghatároznia. Nagyvállalati környezetben, ahol holdingszerű a működés, az anyavállalat biztonsági szervezete megalkotja a teljes vállalatcsoportra érvényes szabályozórendszert, amely alapvetően a minimális követelményrendszert, mint belső szabványt jelenti. Minden tagvállalatnak ehhez kell alkalmazkodnia, implementálva az anyavállalat által megalkotott, és szabályokba, utasításokba foglalt elvárásokat.

Mélységi védelem

A személy-, és vagyonvédelem, illetve a fizikai védelem tekintetében mélységi védelemnek nevezzük azokat az adminisztratív és biztonságtechnikai módon kialakított védelmi határokat, amelyek segítségével biztosítani lehet egy adott létesítmény/intézmény területén belül, hogy a védett, vagy védeni kívánt értékekhez történő illetéktelen hozzáférés csak többlépcsős, a védett irányban növekvő hatékonyságú biztonsági intézkedések mellett legyen lehetséges. Ebben kiemelkedően fontos, hogy az egyes biztonsági zónák (3. ábra) közötti átjárás mind fizikailag, mind elektronikusan, csak ellenőrzött körülmények között történhessen meg.

[5] IAEA Nuclear Security Series No.13; angol rövidítése: NNS13



3. ábra: A mélységi védelem struktúrája.

A mélységi védelem lényegét Maria Lynn Garcia az alábbiak szerint határozza meg: „*A well-designed system provides protection-in-depth, minimizes the consequence of component failures, and exhibits balanced protection*[6].”- Egy jól tervezett rendszer mélységi és kiegyensúlyozott védelmet biztosít, minimalizálva a rendszerelemek meghibásodásának következményeit. [3].

Biztonsági zóna

Biztonsági zónának nevezzük a védett létesítmény azon területi, funkcionális egységét, amely biztonsági kockázati szempontból egy egységnek tekinthető. A bevezetésre szánt védelmi intézkedések egységes egészet alkotnak, miközben illeszkednek az egész védett létesítmény komplex, mélységi védelmi elvek alapján kialakított rendszerébe.

[6] Garcia, Mary Lynn: Design and Evaluation of Physical Protection Systems (Kindle Locations 403-404). Elsevier Science. Kindle Edition.

Objektumorientált kialakítás

Az „Idegen szavak és kifejezések” szótára szerint a kialakítás a legjobb hatásfokra törekvést jelenti, amely a disszertációm témáját tekintve is egyértelmű.

A fizikai védelem területén objektumorientált kialakításnak nevezhetjük azokat az intézkedéseket, biztonságtechnikai megoldásokat, amelyek koherens egységet alkotva, az adott létesítmény/intézmény biztonsági kockázatainak körültekintő értékelésén alapulnak. A létesítmény/intézmény létrehozásának és működtetésének célját, a valós biztonsági kockázatokat szem előtt tartva, annak biztonságos működését a lehető legjobban támogatják.

Megfigyelő-, és ellenőrző rendszerek

Minden olyan biztonságtechnikai rendszert, amelynek feladata egy adott létesítmény/intézmény személy-, és vagyonvédelmének, illetve fizikai védelmének biztosítása és a biztonsági kockázatok kezelésének támogatása: e definíciónak megfelelően határozom meg az adott létesítmény biztonsági kockázatainak szempontjából releváns behatolásjelző, beléptető és videó megfigyelő rendszerek tervezését, kialakítását.

A fizikai védelmi rendszerek tervezése, kivitelezése – alapvető menedzselése – az Egyesült Államok Belügyminisztériuma szerint:
“A managing physical security resource is a holistic process which includes strategic planning, identifying goals and performance objectives, as well as justifying and applying a realistic budget for a comprehensive security program.” – A fizikai védelemmel kapcsolatos feladatok menedzselése egy olyan holisztikus folyamat, amely magában foglalja a stratégiai tervezést, a célok és teljesítések objektív azonosítását csakúgy, mint egy valódi, reális költségvetés összeállítását egy mindenrészletre kiterjedő biztonsági program számára. [4]

A fenti kitételből is nyilvánvaló, hogy egy fizikai védelmi rendszer komplexitása több, különböző szakember szoros együttműködését igényli ahhoz, hogy a szervezeti célok, a biztonsági kockázatok kezelésébe bevont védelmi rendszerek valóban helyszínre szabottan, objektumorientált megvalósításban kerüljenek kialakításra.

Személyes tapasztalatom szerint - melyet egy speciális továbbképzésen[7] szerezett ismeretek is megerősítettek - a „tengerentúli”, elsősorban az Amerikai Egyesült Államokban tevékenykedő szakemberek szemléletében fontos szerepet játszik, hogy egy videó megfigyelő rendszer alapvetően a *behatolásjelző rendszer* része. Feladata a beérkező jelzések valóságtartalmának, hitelességének ellenőrzésére szolgál, természetesen más szempontok szerint tervezett és kialakított rendszerek is léteznek, például: személyek, gépjárművek mozgásának nyomon követése a létesítményen belül, gépjármű parkolók ellenőrzése, technológiai rendszerek ellenőrzése, melyek esetében is érvényes cél a biztonsági kockázatok kezelése, illetve azok támogatása).

A hazai gyakorlatban használatos rendszerezés a következő: megfigyelő és ellenőrző rendszereknek nevezzük azokat a biztonságtechnikában felhasznált eszközöket, berendezéseket, illetve ezek integrált egységét, amelyek egy adott létesítmény biztonsági kockázatainak kezelésével támogatják a létesítményben végzett folyamatok biztonságos végzését, függetlenül attól, hogy azok társadalmi, gazdasági, vagy direkt módon biztonsági tevékenységet jelentenek-e.[8] Ezen rendszerek alapesetben:

1. Behatolásjelző rendszerek.
2. Beléptető rendszerek.
3. Videó megfigyelő rendszerek.
4. Egyedi védelmi megoldások.

[7] IAEA International Training Course on the Physical Protection of Nuclear Material and Nuclear Facilities (2016. november 11-22.), Albuquerque, NM, USA

[8] Saját meghatározás, amely megfogalmazás a tapasztalatom szerint a legszélesebb körben határozza meg a megfigyelős és ellenőrző rendszerek gyakorlati jelentését.

1. TUDOMÁNYOS ELŐZMÉNYEK

A biztonságra törekvés nem új keletű igény és tevékenység az emberiség történetében. Már az ősi Egyiptomban, időszámításunk előtt 3150-ben tettek konkrét vagyonvédelmi intézkedéseket a vízforrások védelme érdekében. A kutak körül árkokat ástak, melyeket vízzel töltöttek fel annak érdekében, hogy védjék azokat a behatolóktól, a károkozóktól. [5]

1.1. Történeti háttér

Szinte hihetetlen, de az első elektromágneses elven működő behatolásjelző berendezés szabadalmi bejelentése 1853. június 21-ére datálódik. A bejelentő egy bizonyos Augustus Russel Pope bostoni feltaláló volt.

Pope berendezése egy elektromos áramkör zárására reagált: az ajtókat és az ablakokat párhuzamos áramkörként önálló egységekként csatlakoztatták. Ha az ajtót, vagy az ablakot kinyitották, és az elektromos áramkör záródott, az áram hirtelen történő megindulása rendszer egyik csatlakoztatott elektromágnesének behúzását okozta. Az elektromágneses rezgéseket egy kalapáccsal továbbították, amely csengőt ütögetett. Pope találmányának különleges tulajdonsága az volt, hogy a riasztást nem lehet kikapcsolni az ablakok vagy ajtók egyszerű lezárásával: az ajtó felett lévő falra szerelt kapcsolórugó ebben az esetben is megszakította az áramot, hogy a csengő folyamatosan működjön. [6]

Egy másik meghatározó mérföldkő a biztonságtechnikai rendszerek tekintetében a központi felügyeleti állomás ötlete, amely Edward A. Calahan nevéhez fűződik. Ebben Calahan 50 szomszédjának házában elhelyezett vészhívót egy rendszerré kapcsolta össze. [5]

A biztonságtechnika, mint fogalom egyik legkomplexebb meghatározása - véleményem szerint - a következő: „Biztonságtechnikának nevezzük tehát a műszaki tudományok azon területét, amelynek feladata a különféle objektumok, rendszerek biztonságának növelése, az embert érő káros hatások és a vagyon kár kockázatának csökkentése, igénybe véve ehhez műszaki, szervezési, egészségügyi, gazdasági intézkedéseket és eszközöket…” [7]. A definíció önmagában is mutatja, hogy a biztonságtechnikával foglalkozó szakemberek számára jelentős kihívás az a tény, hogy munkavégzésük során interdiszciplináris tudásháttérrel, nagy odafigyeléssel kell eljárni - széles körben áttekintve a különböző tudományágak követelményeit.

A XX. század második fele gyors fejlődést hozott a biztonságtechnikai, elsősorban a behatolásjelző rendszerek területén. A mérnökök az 1970-es években integrálták az első *mozgásérzékelő*t a behatolásjelző központjaikhoz. Az ezt követő években a gyors fejlesztések mellett a rendszerek szabványosítása is megindult (elsősorban az Egyesült Államokban).

A biztonságtechnikai rendszerek másik jelentős komponense a video-megfigyelő rendszerek fejlődése természetesen sokkal később kezdődhetett. Miközben maga a technológia az 1940-es években érte el az alkalmazhatósági szintet, a mindennapi gyakorlatban csak a múlt század 70-es éveiben jelent meg először. [8]

A biztonságtechnikai rendszerek, rendszerelemek fejlődése az elmúlt évtizedben eddig nem ismert sebességgel ment végbe. A sürgető technológiai változások igényével naponta szembesülünk, azonban a fejlődés sok-sok megoldandó újabb műszaki, esetenként a fizika határait feszegető problémát vet fel. Az IT/ICT[9] technológia az elmúlt közel 20 évben „beszivárgott" a biztonságtechnikai rendszerek szinte valamennyi területére. Ez nagy kihívások elé állítja a biztonsági szakterületen tevékenykedő szakembereket. A nehézséget alapvetően az okozza, hogy a fejlett védelmi rendszerek tervezésekor, kiépítésekor az informatikai hálózati ismeretek már nem kerülhetők meg, ezért a szakemberek továbbképzése elengedhetetlen.

Jelentős feladatnak tekinthető, hogy az *IP alapú rendszer*ek tervezésekor az egyes kábelek hossza már nem szabadon választott, azaz nem a szükségletek szerinti. „…LAN rendszerek tervezésénél alapvető szabály a hálózati végpontok távolsága. Réz alapú összeköttetés esetén ez maximálisan 100 m lehet. Amennyiben nagyobb távolságban kell biztosítanunk az átvitelt, két lehetőségünk van: első lépésként repeatere[10]-ket kapcsolhatunk a rendszerünkhöz (maximálisan négyet). Ha ez a távolság kevés, akkor az *optikai kábel*lel és médiakonverterrel[11] megvalósított hálózatot kell előtérbe helyezni…"[9]

Érdekes az alábbi gondolat, amelyet a szakmában ismert munkatárs kissé keserűen jegyzett meg egy szakmai egyeztetés alkalmával: „a digitális rendszerek, informatikai hálózatok megjelené-

[9] IT/ICT: Information Technology/Information Communication Technology: Információ Technológia/Információ- és Kommunikációtechnológia
[10] Repeater: jelismétlő, a csillapított jelek újragenerálására használt hálózati készülék.
[11] Médiakonverter: olyan átalakító, amely az informatikai hálózat optika platformját réz alapúra konvertálja.

sével együtt az „igazi” videó képek eltűntek, helyette a valós képről az elemi képfelvevő elemeket követően már csak egy néhány matematikai algoritmus által előállított kép jelenik meg az operátorok *monitor*jain…”.

Az állítás bármennyire igaz, a digitális jelfeldolgozásnak, az IT hálózatok megjelenésének rendkívül nagy jelentősége van a biztonságtechnikai világ környezetében is. Az egyes alrendszerek integrálhatósága ugrásszerűen megnőtt. Ezek működtetésével különböző egyéb rendszerek irányában történő átjárás, vezérlés is elérhetővé vált a rendszeren belül. Az ún. „front-end[12]” alkalmazások lényegesen több alrendszert integrálhatnak, ezzel az operátorok, vezetők döntését szélesebb körben támogatják.

Mi a megoldás? – tehetnénk fel a kérdést, amire kézenfekvő a válasz: a szakemberek továbbképzésére sokkal jelentősebb hangsúlyt kell fektetni. „…Az IP alapú kommunikációt alkalmazó eszközök és rendszerek visszavonhatatlanul megjelentek a vagyonvédelmi alkalmazásokban. Az egyszerű, néhány kamerás irodaitól, az összetett repülőtéri rendszerekig megfelelő eszközválaszték áll a tervezők és telepítők rendelkezésére. Az első feladat a biztonságtechnikai szakembereknek megismerni magát a technológiát: az hogyan működik, milyen lehetőségeket kínál, melyek a korlátai. A második - és valószínűleg a fontosabb -: újragondolni, mi mindent nyújthat egy ilyen rendszer a felhasználónak...” [10]

Az analóg videó technológia alkalmazások már sok évvel ezelőtt elérkeztek a fejlődésük technológiailag elérhető felső határához. A továbblépéshez új utakat kellett keresni - felhasználva a kor technikai fejlődését. Így kézenfekvő megoldás volt az IT-ipar eredményeinek felhasználása. A hatalmas számítástechnikai fejlődés a műszaki tudományok minden területén jelentős változást hozott. A mikroprocesszorok számítási teljesítményének, valamint az operatív és háttértárak korábban elképzelhetetlen tároló kapacitásának, csakúgy, mint az adott számítási feladathoz szükséges energiafelhasználásnak a jelentős csökkenése figyelhető meg. Az integráltság, az egyes integrált áramkörökben használható ún. „vonalszélesség[13]” elképesztő csökkenése új lehetőségeket teremtett a biztonságtechnikai igények fokozódó kielégítésére.

[12] Front-end alkalmazásnak nevezzük azt a számítógép programot, amelyet a felhasználó közvetlenül használ egy rendszer üzemeltetéséhez.
[13] A vonalszélesség a félvezető gyártásban használt fogalom, amely gyakorlatilag a félvezető lapkára felvitt félvezető elemek közötti „kábelezést” jelenti. Az ezeken a „kábeleken” folyó áram, így annak a vastagsága jelentősen befolyásolja az integráltsági fokot, azaz az alkatrészsűrűséget.

A videotechnika fejlődésével a behatolásjelző rendszerek gyártói is igyekeznek lépést tartani, az IT/ITC infrastruktúra ezen a területen is láthatóan megjelent. A távjelzések *távfelügyelet*i központ nélküli továbbítása az egyes tulajdonosok, üzemeltetők részére, hanem a mobil alkalmazások megjelenése is egy más dimenzióba emelte a lakossági és az üzleti környezetben működtetett behatolásjelzők üzemeltetését.

A vagyonvédelmi, illetve a fizikai védelmi rendszerek tekintetében a *beléptető rendszer*ek fejlődése nem tekint vissza több száz, vagy akár több ezer évre (ellentétben a behatolásjelző rendszerekkel). Annak érdekében, hogy ellenőrzött beléptetést lehessen kialakítani, meg kellett születniük a különböző mechanikai és elektronikus rendszerelemeknek, úgymint zárak, ajtók, vezérlők, stb. Az elektronikus beléptető rendszerek gyakorlati alkalmazásának megkezdése a múlt század 60-as éveire tehető. [11] Az első rendszerek tervezésnek és telepítésének okai között „az elveszett kulcs problémája" is jelentős szerepet játszott minden olyan jól értelmezhető előny mellett, mint a jogosultsági rendszer alkalmazhatósága, jelentések automatikus elkészítése, stb. Ezekben az első rendszerekben az ún. PIN (Personal Identification Number[14]) kódok felhasználása volt a meghatározó. A további fejlődés hozta magával a mágnescsíkok, beépített elektronikus áramkörök (chip) megjelenését, majd a technológia továbblépésével, a 70-es években megkezdődött az érintés nélküli belépőkártyák (proximity cards[15]) használata (4. ábra).

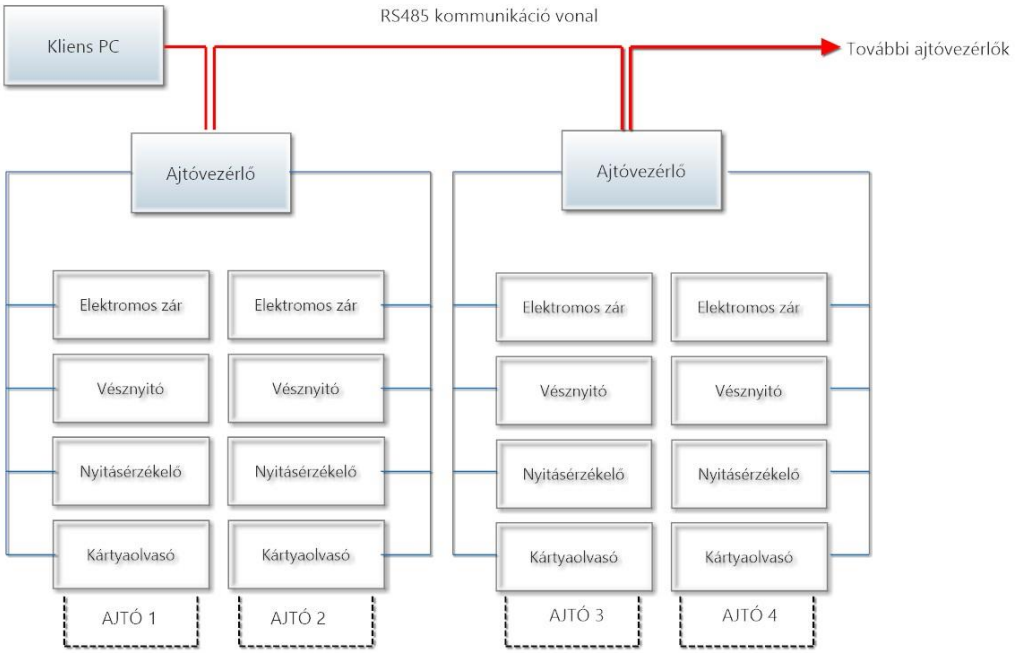
A fejlődés során kialakultak azok a telepítési elvek, amelyek megfelelő iránymutatássá váltak a szakemberek számára.

Példaként néhány ilyen fontos szabály, rendező elv:

- Az *ajtóvezérlő* dobozát, lehetőleg rejtett módon és *szabotázsvédett* kivitelben kell telepíteni.
- A *vésznyitó* minden esetben a védett oldalon kerüljön felszerelésre.
- Biztonsági szempontból - elektronikus zár, vagy tartómágnes alkalmazása esetén - a feszültség elvételére nyitó beállítást kell alkalmazni, de a szünetmentesítéshez szükséges akkumulátor-kapacitást gondosan, a helyszín ismeretében kell kiszámítani.

[14] Personal Identification Number (rövidítéssel: PIN) kód egy olyan személyi azonosító szám, amely egyedileg, az adott eszköz használója részére kerül generálása.
[15] Proximity card: egy olyan, elsősorban személy azonosításra felhasználható kártya, amelyben a kártyaolvasóból nyert energiát felhasználó elektronikus áramkör került elhelyezésre - akár egyedileg programozott azonosítóval.

- Kiemelt figyelmet kell biztosítani az esetleges azonosító kártya nélküli bejutás kizárására, tekintettel arra, hogy „kényszerített nyitás” státusz üzenetre intézkedési kényszerbe kerül az őrszolgálat (miközben valaki akár jogosan kulccsal jutott be például a pénztárba).



4. ábra: Kártyás beléptető rendszerstruktúra.[16] [12]

A fizikai védelem, illetve a videó megfigyelő rendszerek talán legjobban áhított eszköze a *hőkamera*. Ezek egyre elérhetőbbé válnak egy szélesebb körű piaci szektor számára is. Egyremásra jelennek meg a különböző képességekkel felruházott hőkamerás megfigyelőállomások, amelyek videó analitikai támogatással a fizikai védelmi rendszerek rendkívül hasznos, meghatározó elemei lehetnek.

A fejlődés – pozitív hatásai mellett – új kihívást is jelent a biztonságtechnika területén tevékenykedő szakemberek, vállalkozások számára. Egy eleddig kevésbé ismert tudomány területére is be kell merészkedniük, megismerkedve az „Informatikai hálózatok” néhány, a biztonságtechnika által is felhasznált területével. Ma már nem csenghet ismeretlenül a szakemberek

[16] Az általánosabb értelmezés érdekében az eredeti rajz alapján került megrajzolásra.

számára a menedzselhető *switch*[17], router[18], gateway[19], alhálózati maszk, vagy a DNS[20] elnevezés sem.

Az IP-alapú rendszerek megjelenése óta az IT ipar fejlődése, azok eredményei azonnal megjelennek ezen a szakterületen is. A biztonságtechnikai rendszerekkel foglalkozó szakemberek folyamatos képzése ma rendszeres feladat a hálózattervezés, építés és konfiguráció területén. A leggondosabban kiválasztott kamerák, rögzítő berendezések, hálózati elemek esetén nagy hiba, ha az átviteli csatorna eszközeinek helyes konfigurációja elmarad. Így fordulhat elő, hogy a felhasznált magas kvalitású eszközalkalmazás ellenére az állandó lefagyások, csomagütközések miatt gyakorlatilag használhatatlan rendszer épül. Szintén kiemelt jelentősége van az elméleti háttérismeretek gyakorlati alkalmazásának: egészen biztosan hibás döntés egy Digitális Videó Rögzítő (*DVR*) beállításnál a H.264,[21] illetve napjainkban, a biztonságtechnikában is megjelenő H.265[22] tömörítés használata, ha tudjuk, hogy a beépített mikroprocesszor számítási kapacitása alacsony.

Az előzőekben rögzített technológiai környezetben megvalósításra kerülő fizikai védelmi rendszerek tervezési és kivitelezési feltételrendszereit alapjaiban határozzák meg az adott létesítmény biztonsági kockázatai. Ezek mind a tervezői, mind a megrendelői oldalon relevánsak, amelyeknek optimális kezelésére a védelmi terveknek megoldásokat kell találni. A létesítményt, a gazdasági társaságot, esetleg intézményt fenyegető kockázatokat értékelni kell annak érdekében, hogy azok kezelésére hatékony, ár/érték arányában megfelelő megoldásokat alkalmazzunk. [13]

„…A kockázatértékelés egyfajta tervezési alapfenyegetettséget dolgoz ki, amely a tervezési folyamat alapját képezi biztosítva, hogy a tervezési folyamat a biztonsági kockázatokra megfelelő válaszokat adjon. A kockázatértékelés területén széleskörű lehetőségek és módszerek vannak, amelyek közül a biztonságtechnikai tervezők számra kiválasztható az optimális megoldás a vállalat biztonsági stratégiájának, gazdasági céljainak megvalósításához legjobban illeszkedő fizikai védelmi rendszerek kidolgozásához…” [13]

---

[17] Switch: hálózati kapcsoló
[18] Router: útválasztó
[19] Gateway: átjáró
[20] Az informatikai hálózatok építőelemei
[21] H.264 egy, a videotechnikában elterjed tömörítési eljárás
[22] H.265 szabványban rögzített, akár 7680·4320 felbontást is támogató tömörítési eljárás

1.2. Jogszabályi környezet

A biztonságtechnikai rendszerek alkalmazására szinte alig vannak jogszabályok. Néhány, a szakmai területünket érintő szervezetre, hatóságra vonatkozó előírás, rendelet, állásfoglalás létezik, amelyekben e szakirányban irányadó megfogalmazásokat találunk. Felsorolás-szerűen:

1) A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól kiadott jogszabály (2005. évi CXXXIII. törvény)
2) A rendőrségi törvény 42.§ és 42/A.§ (1994. évi XXXIV. törvény a Rendőrségről)
3) A rendőrségi térfigyelést szabályozó intézkedés (38/2001 ORFK Intézkedés)
4) Pénzváltó helyek kamerái (297/2001. (XII.27.) Korm. Rendelet a pénzváltási tevékenységről)
5) Közterület-felügyeletre vonatkozó jogszabály (1999. évi LXIII. törvény a Közterület-felügyeletről)
6) 2003. évi CXXXIII. törvény a társasházakról
7) A személyszállítási szolgáltatásokról szóló 2012. évi XLI. törvény
8) 2004. évi I. törvény a sportról (54/2004. (III.31.) Korm. Rendelet a sportrendezvények biztonságáról)
9) Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása a munkahelyen alkalmazott elektronikus megfigyelőrendszer alapvető követelményeiről

Disszertációmban nem kerülhetem meg az Európai Parlament és a Tanács (EU) 2016/679 rendeletét (2016. április 27.), amely a személyes adatok védelmét emelte a középpontba. Fizikai-, és/vagy vagyonvédelmi rendszerek tervezése során eddig is kiemelt figyelmet kellett fordítani az adatkezelési és adatfeldolgozási folyamatok kialakítására, hasonlóan az adatkezelés és feldolgozás szigorú célhoz kötöttségi elvére. Az új jogszabály hatálybalépésével fokozottabb és az adatvédelmi garanciákat közvetlenebb módon biztosító szabályozás lép életbe. Ezzel kapcsolatban elegendő, ha csak megemlítem az adatvédelmi felelős személy megjelenését, aki jelentős támogatást nyújthat a szakemberek számára a szükséges rendszerkialakítás adatvédelmében.

A beléptető-, és videó megfigyelő rendszerek tervezőit és üzemeltetőit is érintő jogszabályi változásokhoz történő alkalmazkodás nem kis feladatot ró a szűkebb értelemben vett szakterület művelőire is. Izgalmas és egyben nagy erőforrás-igényű változás az üzemeltető hatóságok előtti bizonyítási kötelezettsége arra vonatkozóan, hogy az általa üzemeltetett rendszerek az adatvédelmi jogszabályoknak megfelelnek.

A 2018. május 25-től már hazánkban is alkalmazandó jogszabály alapján az esetlegesen bekövetkezett incidenseket kötelező lesz jelenteni, emellett új jogokat is biztosít az ügyfelek számára. Személy szerint nincs kétségem afelől, hogy a változások követéséhez jelentős pénzügyi forrásokat kell allokálni.

Véleményem szerint az új adatvédelmi törvénnyel véget érhet a ma még esetenként megtalálható barkácsolt, nem szakszerűen, vagy nem a szakemberek által kialakított biztonságtechnikai rendszerek időszaka. Ez kétségtelenül kedvező hatással lesz a közeljövő szakmai tevékenységére és önmagára a szakterület fejlődésére is.

Fontos eleme lesz az adatvédelmi tevékenységnek az adatközpontok fizikai kialakítása, valamint az adatközpont geolokációjának meghatározása. Ennek értelmében a személyes adatok tárolása, azok védelme az Európai Unióban érvényes szabályozásnak kell, hogy megfeleljen (azaz az adatközpontnak az Európai Unió területén kell lennie annak érdekében, hogy a személyes adatok védelme garantálható legyen).

1.3. Szabványok, ajánlások

A biztonságtechnika területén már léteznek kidolgozott szabványok, de szinte kivétel nélkül minden szabvány termékszabvány, azaz az egyes rendszerelemekkel szemben támasztott követelményeket részletezi.

Az érvényben lévő szabványokat (1. táblázat), illetve az azokat körülvevő értelmezési, felhasználási nehézségeket is áttekintve megállapítható, hogy a szabványokkal kapcsolatos környezet nem egyszerű. A szabványok egy része kizárólag idegen nyelven (elsősorban angol, valamint német és francia nyelveken) érhető el, amely nehézséget okozhat a biztonságtechnikai rendszerek tervezőinek, kivitelezőinek.

A szabványokról történő elemzések közé be kell illeszteni egy műszaki előírást (Technical Specification – TS), amely olyan normatív dokumentum[23], amelyet nemzeti szinten nem kötelező nemzeti szabványként bevezetni.

[23] Magyar Szabványügyi Testület állásfoglalásából átvéve, melyet Személy-, Vagyonvédelmi és Magánnyomozói Kamara (képviselte: Móré Attila) kérésére adott ki 2015. május 29-én.

Legfontosabb biztonságtechnikai szabványok szakterületenként, tervezők, telepítők, karbantartók és üzemeltetők részére			
Szakterület	**Szabvány megnevezése**	**Szabvány száma**	**Szabvány nyelve**
Behatolás- és támadásjelző rendszerek	Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 1. rész: Rendszerkövetelmények 13.310 Bűnözés elleni védelem Megjelenés dátuma: 2011-01-01	**MSZ EN 50131-1:2011**	magyar
	Riasztórendszerek. Behatolás- és támadásjelző rendszerek. 7. rész: Alkalmazási irányelvek 13.310 Bűnözés elleni védelem Megjelenés dátuma: 2010-01-01	**MSZ CLC/TS 50131-7:2010**	magyar
Videó-megfigyelő rendszerek	Videó-megfigyelőrendszerek biztonsági alkalmazásokhoz. 1-1. rész: Rendszerkövetelmények. Általános előírások (IEC 62676-1-1:2013)	**MSZ EN 62676-1-1:2014**	angol
	Videó-megfigyelőrendszerek biztonsági alkalmazásokhoz. 4. rész: Alkalmazási irányelvek (IEC 62676-4:2014)	**MSZ EN 62676-4:2015**	angol
Beléptető rendszerek	Riasztórendszerek és elektronikus biztonsági rendszerek. 11-1. rész: Elektronikus beléptető rendszerek. A berendezésekre és készülékekre vonatkozó követelmények (IEC	**MSZ EN 60839-11-1:2013**	angol
	Riasztórendszerek és elektronikus biztonsági rendszerek. 11-2. rész: Elektronikus beléptető rendszerek. Alkalmazási irányelvek (IEC 60839-11-2:2014)	**MSZ EN 60839-11-2:2015**	angol
Segélyhívó rendszerek	Riasztórendszerek. Segélyhívó rendszerek. 1. rész: Rendszerkövetelmények 13.320 Vészjelző és figyelmeztetőrendszerek Megjelenés dátuma: 2002-12-01	**MSZ EN 50134-1:2002**	magyar
	Riasztórendszerek. Segélyhívó rendszerek. 7. rész: Alkalmazási irányelvek 13.320 Vészjelző és figyelmeztetőrendszerek Megjelenés dátuma: 2006-09-01	**MSZ CLC/TS 50134-7:2006**	magyar
Riasztásátviteli rendszerek	Riasztórendszerek. Riasztásátviteli rendszerek és berendezések. 1. rész: A riasztásátviteli rendszerek általános követelményei	**MSZ EN 50136-1:2012**	angol
	Riasztórendszerek. Riasztásátviteli rendszerek és berendezések. 2. rész: A felügyelt létesítményi adó-vevő berendezés (SPT) követelményei	**MSZ EN 50136-2:2014**	angol
	Riasztórendszerek. Riasztásátviteli rendszerek és berendezések. 3. rész: A riasztásfogadó központi adó-vevő berendezés (RCT) követelményei	**MSZ EN 50136-3:2014**	angol
	Riasztórendszerek. Riasztásátviteli rendszerek és berendezések. 4. rész: A riasztásfogadó központokban alkalmazott riasztásmegj	**MSZ CLC/TS 50136-4:2008**	magyar
	Riasztórendszerek. Riasztásátviteli rendszerek és berendezések. 7. rész: Alkalmazási irányelvek	**MSZ CLC/TS 50136-7:2007**	magyar
Riasztásfogadó központok	Riasztásfogadó központ. 1. rész: Helyszín-megválasztási és építészeti követelmények	**MSZ EN 50518-1:2014**	angol
	Riasztásfogadó központ. 2. rész: Műszaki követelmények	**MSZ EN 50518-2:2014**	angol
	Riasztásfogadó központ. 3. rész: A működés folyamata és követelményei	**MSZ EN 50518-3:2014**	angol

1. táblázat: A legfontosabb szabványok a biztonságtechnika területén.

Természetesen a szakterületre vonatkozó szabványok köre az 1. táblázatban látható felsoroláshoz képest jóval tágabb, a megnevezett szabványok a szakmagyakorlók számára gyakorlatilag nélkülözhetetlenek.

A Magyar Szabványügyi Testület MB816 (Műszaki Bizottság, Riasztórendszerek) szakbizottsága, amelynek a tevékenységi területe átfogja a biztonságtechnika területének meghatározó részét, úgymint betörés-, és behatolásjelzők, segélyhívók, vészjelző- és figyelmeztető eszközök, a hozzájuk tartozó jelzésátviteli és egyéb eszközök és ezek rendszerei. A Bizottság jelentős

erőfeszítést tesz annak érdekében, hogy a Magyarországon és Európában is érvényben lévő szabályozást ismertté tegye - minimálisan a szakemberek részére.

Az 1. táblázatból jól látható, hogy 2011-et követően a legfontosabb szabványok nem magyar nyelvűek, amely tény nem segíti a Magyarországon tevékenykedő szakemberek munkáját. A munkavégzéshez elegendő szakmai angol nyelvtudás nem elégséges, mert sok pontatlan értelmezéshez vezet.

A biztonságtechnikában a teljes körű jogszabályi támogatás, illetve környezet csak a tűzjelző rendszerek tervezésében, létesítésben van érvényben. A biztonságtechnika más területén léteznek előírások, ajánlások, néhol szabványok, amelyek nem komplex jogszabályi hátteret, de azért megbízható körülményeket biztosítanak a szakember munkájához. A területen belül a biztonságtechnikai rendszerek alkalmazási lehetőségei, előírásai szabványban rögzítettek. E szabványok ugyan nem kötelezően betartandók, de az abban előírtak teljesítése ajánlott mind a tervezők, mind a kivitelezők részére, az attól való eltérés csak a jobb műszaki megoldások irányában történhet.

Disszertációmban nem foglalkozom a tűzvédelemmel kapcsolatos berendezésekkel, azok tervezési, kivitelezési követelményeivel, tekintettel arra, hogy az a biztonságtechnikai szakterület egyetlen olyan része, amely teljes egészében lefedett törvényi szintű előírásokkal, konkrét tervezési szempontokkal, feltételrendszerrel.[24]

1.3.1. A MABISZ termék-megfelelőségi ajánlása

A jogszabályi környezet tárgyalásánál nem feledkezhetünk meg a Magyar Biztosítók Szövetségének (MABISZ) Ajánlásáról sem, amely irányadó a biztonságtechnikai szakemberek számára.

Magyarországon a MABISZ Betöréses lopás-, és rablásbiztosítás technikai feltételei [14] (Ajánlás) figyelembevételével célszerű olyan biztonságtechnikai berendezéseket telepíteni,

[24] 1996. évi XXXI. törvény A tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról (a törvény az alapja közel 40 különböző jogszabálynak, köztük az 54/2014. (XII. 5.) BM Rendeletnek az Országos Tűzvédelmi Szabályzatról).

amelyek a biztosítók számára is elfogadottak. Az Ajánlások megfelelő szakmai háttérrel kidolgozott javaslatok, amelyek jelentős támogatást nyújthatnak a szakmagyakorlók számára.

1.4. A fejezet összegzése – következtetések

Az első fejezetben általam megállapítottakból jól látható, hogy a biztonságtechnikai rendszerekre vonatkozó kiépítési elvek nem rögzítettek. A tűzvédelmi rendszereken kívül az egyéni biztonságtechnikai rendszerekre vonatkozó tervezési és telepítési alapelveket ipari környezetben nem, vagy csak társasági szinten saját használatra fogalmazták meg. Ennek – véleményem szerint – elsősorban az az oka, hogy nincs egy általánosan kialakított, jól követhető szabályrendszer. Másodsorban okolható a szakterületre jellemző – esetenként indokolt, máskor operatív érdekekkel nem magyarázható – titkolódzás/titoktartás.

A terület jelenlegi jogszabályi környezete az alulszabályozottsággal küzd. Magára a biztonságtechnikai rendszerek tervezésére, építésére, azoknak konkrét technikai paramétereire nem vonatkoznak jogszabályok. Mint azt a fejezetben kifejtettem: léteznek ugyan a szakmai területet érintő szervezetre, hatóságra vonatkozó előírások, rendeletek, állásfoglalások, azonban ezek csupán e szakirányban irányadó megfogalmazások.

Elengedhetetlen a tervezési, kivitelezési folyamat szakmaiságának érdekében annak mielőbbi jogszabályi lefedése. A létesítményt, a gazdasági társaságot, esetleg intézményt fenyegető kockázatokat értékelni kell azért, hogy azok kezelésére hatékony, ár/érték arányban megfelelő megoldásokat tartalmazzon. A folyamat jogszabályi hátterének a védelmi tervektől kezdve, a tervezési alapfenyegetettség meghatározásán át, egészen a felhasznált anyagok, eszközök alapjellemzőjéig ki kell terjednie. Egészen addig kell a jogszabályi háttérnek hatnia, hogy fizikai védelmi rendszer építését csakis megfelelő szakirányú végzettséggel, erkölcsi bizonyítvánnyal lehessen végezni. Magának a képzettségnek évenkénti ráképzését is szükséges megoldani.

Az adott technológiai környezetben megvalósításra kerülő fizikai védelmi rendszerek tervezési és kivitelezési feltételrendszereit alapjaiban határozzák meg az adott létesítmény biztonsági kockázatai. Ennek értelmében szükségszerű kockázatértékelést végezni minden fizikai védelmi rendszer kiépítése előtt. Ez mind a tervezői, mind a megrendelői oldal tekintetében elengedhetetlen. A kockázatértékelés alapján megállapított veszélyek optimális kezelésére a védelmi terveknek kell hatékony, és egyben költséghatékony megoldásokat találni.

Mindezek érdekében elengedhetetlen egy egységes elvrendszer kidolgozása, amelynek mentén tematikusan, követhető elvek alapján, szigorúan objektumorientáltan kidolgozható az optimális megoldás a különböző biztonsági kockázatú vállalatok egyedi biztonsági stratégiájának megalkotásához. Ezzel egységes, ellenőrizhető, folyamatosan aktualizálható rendszert szolgáltatunk a gazdasági célok megvalósításához legjobban illeszkedő fizikai védelmi rendszerek tervezéséhez.

2. MEGFIGYELŐ-, ÉS ELLENŐRZŐ RENDSZEREK TERVEZÉSE

Ebben a fejezetben a célom az, hogy megfogalmazzam azokat a tervezési alapelveket, amelyek a szakemberek munkájában és az adott létesítmény védelmének kialakítása szempontjából meghatározóak. Ezen elvek ismerete elengedhetetlen a szakszerű tervezési munka, illetve egyáltalán a teljes, komplex védelmi koncepció kidolgozása érdekében.

2.1. Az objektumorientált megfigyelő-, és ellenőrző rendszer

A megfigyelő-, és ellenőrző rendszerek tervezési stratégiája esetenként jelentősen eltér – elsősorban az angolszásszal összehasonlítva – a külföldi, illetve a magyar gyakorlatban. Ez a különbség a szemléletmódból következik. Lényegében a magas, vagy fokozott biztonsági kockázatok közepette működtetett létesítmények esetében Magyarországon az „elrettentés" stratégiáját követjük, miközben angolszász környezetben a „meghiúsítás" stratégiája az előírás.

A videó megfigyelő rendszerek tervezése nem választható el a behatolásjelző rendszerek tervezésétől. Napjaink lendületes informatikai fejlődése, a hardver elemek teljesítményének kiugró növekedése és az ezzel szinte egyidejű méretcsökkenése egyre inkább lehetőséget teremt a CCTV[25] rendszerek detektálási lehetőségeinek jobb kihasználására. A videoanalitikai fejlesztések legfőbb iránya is ez, akkor is, ha ez (még) nem alternatívája a behatolásjelző berendezések alkalmazásnak.

A disszertációm témájául választott objektumorientált megfigyelő-, és ellenőrző rendszerek a gyakorlati életben szinte mindig megvalósulnak, amikor a megbízó kérésére a szakemberek egy-egy komplex biztonságtechnikai rendszert terveznek. A kialakítandó rendszert minden esetben az adott intézmény környezetéhez, a megbízó által megjelölt igények szerint építik fel. A gyakorlati életben azonban ezt a folyamatot csak igen kevés esetben előzi meg egy racionális, minden részletre kiterjedő kockázatértékelés, holott ez mindkét fél számára jelentős könnyebbséget, a feladat jobb megértését, következésképpen magasabb szintű szakszerűséget biztosíthatna. Jelen munkámban – mindkét fél tevékenységét segítve – ezt folyamatot kívánom támogatni.

[25] CCTV: Close Circuit Television (Zártláncú Televíziós Hálózat, amely elnevezést a biztonságtechnikában gyakran használjuk a videó megfigyelő rendszer elnevezés helyett).

2.1.1 Elrettentés, mint tervezési elv

Az elrettentés, mint tervezési stratégia alapvetően abból indul ki, hogy olyan biztonsági rendszert építsünk, amely megjelenésében, műszaki paramétereiben, technológiai szintjében erőt és sérthetetlenséget sugároz.

Az esetleges támadó a rendszer látványától, a részére megszerezhető információkból azt a következtetést vonja le, hogy úgysem lesz képes végrehajtani a tervezett támadást, így attól önszántából eláll. Magyarországon alapvetően ezt a stratégiát követjük, amely bizonyos esetekben célravezető lehet, de semmiképpen sem az optimális megoldás figyelembe véve a finanszírozási költségeket.

Ez a tervezési elv viszonylag jól beválhat megfelelő megbízói és tervezői felügyelet mellett olyan rendszerek esetében, amelyek személy-, és vagyonvédelmi célból, lakossági, valamint kisméretű kereskedelmi létesítmények számára kerülnek kiépítésre.

2.1.2 Meghiúsítás, mint tervezési elv

A meghiúsítás tervezési elvét alapvetően a fizikai védelmi rendszerek esetében célszerű alkalmazni, amely abban tér el a személy-, és vagyonvédelmi célú biztonsági rendszerektől, hogy a létesítményben üzemeltetett technológia védelme is feladat.

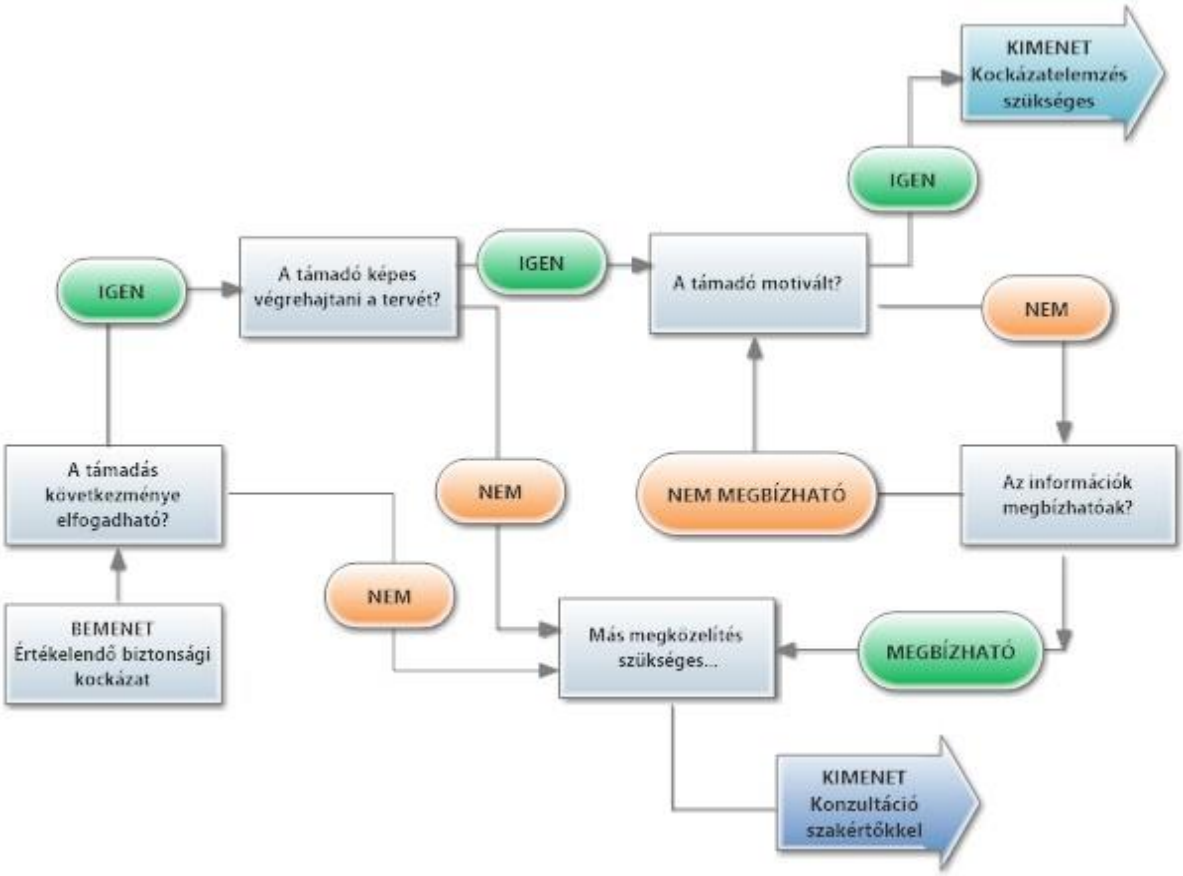
A meghiúsítás, mint a tervezési stratégia egyik meghatározó eleme az ún. „Tervezési Alapfenyegetettség[26]" meghatározása (5. ábra). A biztonsági kockázatokat, a létesítmény működtetésével kapcsolatos veszélyeket ebben a dokumentumban kell összegezni és nem csak az elveket, hanem a konkrét veszélyforrásokat is meg kell nevezni. A szemléletmód szépségét és érdekességét az adja, hogy a dokumentum összeállítója meghatározza, hogy milyen valószínűséggel kell az illetéktelen behatolást érzékelni, illetve milyen valószínűséggel képes a reagáló erő az illetéktelen behatoló szándékát, illetve cselekményét meghiúsítani. [2]

Természetesen a jelzett adatok meghatározásához hosszú út vezet. A dokumentum összeállításának külön szabályrendszere van, amely nincs jelen értekezésem fókuszában, de abban kapcsolódik ahhoz, hogy szcenárió-elemzéssel meg kell határozni a fenyegetéseket, és a biztonsági

[26] Tervezési Alapfenyegetettség: Design of Basic Threat (DBT)

kockázatokat. Részletes választ kell adni valamennyi veszély esetén a miért (motiváció), mit (szándék), hogyan (képesség) kérdésekre.

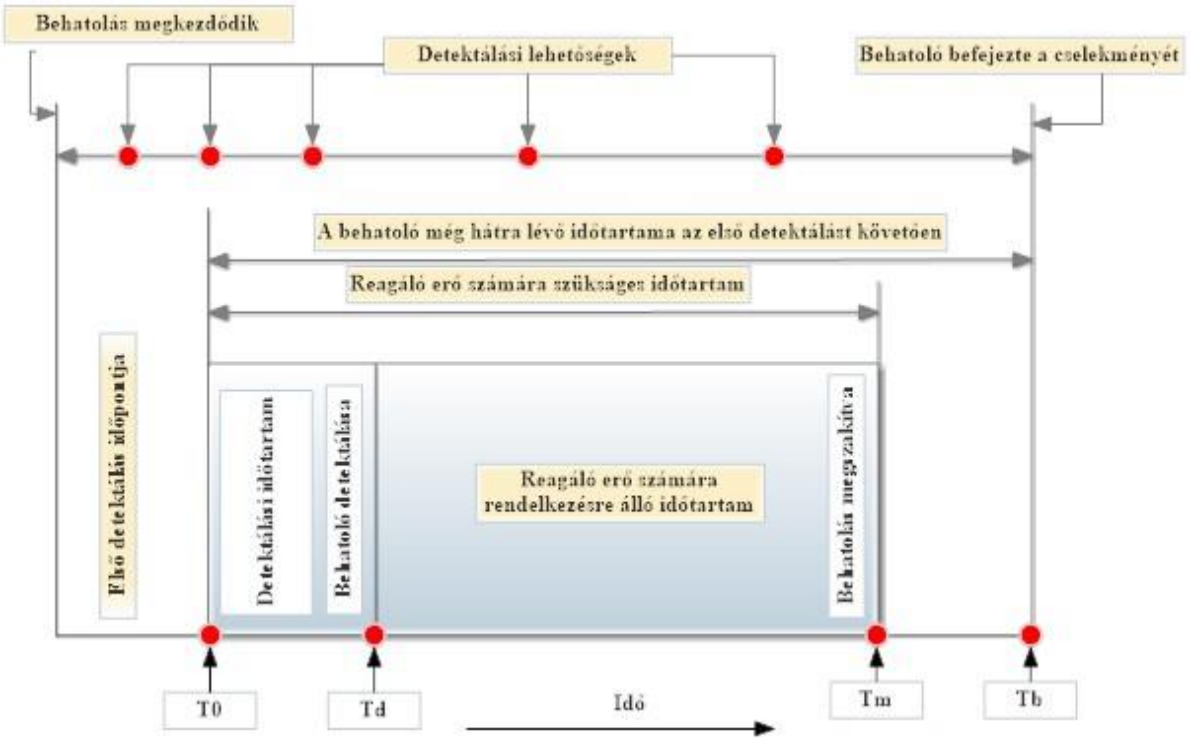
Ezt a meghiúsítás stratégiát találhatjuk meg a behatolásjelző rendszerek tervezőivel és telepítőivel, valamint a távfelügyeleti szolgáltatókkal való együttműködésben is.



5. ábra: A Tervezési Alapfenyegetettség meghatározásának folyamata.

A meghiúsítás, mint tervezési stratégia alapvetően a fizikai védelmi rendszer tervezése esetén kiemelkedő hatékonyságú, olyan jól követhető és működő módszer, amelynek széleskörű alkalmazását hazánkban is célszerű lenne bevezetni. [15]

.



6. ábra: Behatoló és a védelmi rendszer idődiagram.

A meghiúsítási tervezési stratégia az 6. ábrán látható idődiagramból indul ki. Ehhez a környezethez lehetséges fizikai védelmi terveket készíteni, illetve a teljes rendszert kialakítani. Fontos megjegyezni, hogy a behatoló első detektálását követően a behatolásjelző rendszer jelzésének ellenőrzését követően kezdődhet meg a reagáló erők (készenléti erők tevékenysége. „*The PPS*[27] *must provide detection and enough delay for the response force to stop the adversary from successfully completing their tasks*" – A fizikai védelmi rendszernek biztosítania kell az érzékelést és az elegendő késleltetést a reagáló erők számára, annak érdekében, hogy azok megállítsák a behatolót a feladata sikeres végrehajtása előtt. [1]

[27] PPS: Physical Protection System (Fizikai Védelmi Rendszer)

Az idődiagram pontos megértéséhez szükségesek az abban megjelölt időpontok értelmezése, melyek a következők:

T_0: A behatolás detektálásának első időpontja (azzal célszerű számolni, hogy az első detektálási lehetőség bármilyen, akár műszaki okból, meghiúsul, vagy a behatoló olyan gyorsan képes mozogni az általa választott behatolási útvonalon, hogy csak a 2. detektálási pontnál lesz érzékelve).

T_d: A behatolás tényének megerősítési időpontja. Ez azt jelenti, hogy a behatoló által kiváltott riasztási jelzéseket, a behatolás tényét a monitor helyiségben szolgálatot teljesítő munkatársnak ellenőriznie kell elsősorban a CCTV rendszer kameráival. Ez az az időpont, amikor a reagáló erők részére a riasztás szóbeli paranccsal (titkosított csatornákat alkalmazó rádió adó-vevővel) kiadható. A reagáló erők számára ez lesz a tevékenységük megkezdésének elő pillanata.

T_m: A behatoló tevékenységének megszakításának időpillanata. Ebből látható, hogy a reagáló erők számára T_m-T_d időtartam áll rendelkezésre a sikeres meghiúsításra, azaz a behatoló a tevékenységét nem tudta befejezni, a célját nem érte el.

T_b: Az az időpillanat, amikor a behatoló befejezte a tevékenységét, a célját elérte. A reagáló erő tevékenysége nem volt megfelelő, elkésett, vagy be nem fejezett beavatkozás.

A behatolásjelző rendszer detektálásának ellenőrzése CCTV rendszerrel történik, ezért kiemelten fontos az egyes létesítményekben telepítendő videó megfigyelő rendszerek tervezése és kivitelezése. Az esetlegesen bekövetkezett események videotechnikai dokumentálása a későbbi elemzések szakszerű és szabályszerű végrehajtása érdekében alapvető fontosságú (ugyancsak nagy jelentősége van az esetlegesen megindított büntetőeljárásban való hiteles és értékelhető bizonyító erejű felvételek produkálási képességének), így a megfigyelő rendszerek felhasználásának komplexitása azt meghatározó biztonságtechnikai rendszerré emeli.

Napjainkban egyre inkább fejlődik a *videoanalitika* területe, amely merőben új és lényeges lehetőségeket biztosít a CCTV rendszerek felhasználásának (gondoljunk itt elsősorban az emberi viselkedést, a fizikai folyamatokat elemző *kamera*rendszerek alkalmazására).

2.1.3 A behatoló detektálásának valószínűsége

A létesítmény fizikai védelmi rendszerének alapvető, meghatározó részei a létesítmény határán telepítésre kerülő kültéri biztonságtechnikai rendszerek. A reagáló (készenléti) erők felkészülése és eredményes beavatkozása érdekében szükséges késleltetést elsődlegesen a létesítmény jogi határán lévő, megfelelően masszív kialakítású kerítés adja, míg annak fedővédelmét szolgáló, azaz a behatoló első detektálását biztosító védelmi berendezés a telepítendő kerítésvédelmi rendszer.

A kerítésvédelmi rendszerek technológiailag is sokszínűek. Valamennyi megvalósított kerítésvédelmi rendszer esetében szükségünk van azonban egy alapadatra, mégpedig az illetéktelen behatoló detektálásának valószínűségére, amely az adott védelmi rendszerre jellemző. Ezt a valószínűségi adatot jó esetben a gyártó megadja. Ezek az adatok egy adatbázisban rögzítésre kerültek és természetesen kellően nagyszámú és módszerű behatolási kísérlettel teszteltek, illetőleg abból meghatározottak. Az adatok, amelyeket az Egyesült Államokban biztosítani kell a tervező részére, beszerezhetők az Energia Hivataltól (Department of Energy - DOE). A már korábban említett egyesült államokbeli tanfolyamon, vizsgafeladat keretében, ennek az adatbázisnak egy részét meg is ismerhettem. [15]

A tervezett fizikai védelmi rendszer esetében a behatoló első detektálásának valószínűsége (P_D) kiszámításához szükségünk van a tervezett rendszerben telepítésre szánt minden egyes biztonságtechnikai rendszer detektálási valószínűségére (P_{D1}, …, P_{Dn}). Ezek alapján az első detektálási valószínűség [15]:

$$P_D = 1 - (1 - P_{D1})\cdot(1 - P_{D2})\cdot \ \dots \ \cdot(1 - P_{Dn})$$

ahol

P_{D1} : az első érzékelő rendszer detektálási valószínűsége (adatbázisból);
P_{D2} : a második érzékelő rendszer detektálási valószínűsége (adatbázisból);
P_{Dn} : az „n”-dik érzékelő rendszer detektálási valószínűsége (adatbázisból).

A P_D = 0,8…0,9 közötti valószínűség (Tervezési Alapfenyegetettség dokumentumban, atomerőművek esetében a helyi hatóság által meghatározott érték) eléréséhez bizonyos esetben már három önálló, más-más érzékelési technológiát biztosító rendszer telepítése elegendő.

Tipikus detektálási valószínűségi érték például a *rezgésérzékelő*kkel telepített kerítésvédelmi rendszerre: P_{D1} = 0,5).

2.2. Általános meggondolások

Az értekezésem eddig tárgyalt részeiből egyértelmű, hogy egy biztonsági rendszer tervezése és kialakítása során kiemelt figyelmet kell fordítani az adott létesítményt fenyegető veszélyekre, a biztonsági kockázatokra. Minden esetben fontos tisztázni, hogy mit szeretnénk megvédeni és a védendő vagyont, technológiát, esetlegesen személyeket milyen veszélyek fenyegetik.

Az elmúlt évtizedekben szerzett szakmai tapasztalatom egyik legfontosabb felismerése volt, hogy a biztonsági szakterület az adott létesítmény működtetését támogató szakterület. Ezen ténynek tudomásul vételével egy reális nézőpontból leszünk képesek a biztonsági szakterület funkcióit, működtetését szemlélni. Az adott létesítmény fizikai védelmét biztosító valamennyi beépített biztonságtechnikai rendszerrel, *élőerős védelem*mel, szabályzataival, rezsimintézkedéseivel együtt is támogató szakterület, nem pedig önmagáért a biztonságért kialakítandó, kialakított rendszer.

Ezeket a gondolatokat szem előtt tartva a gazdasági társaságok biztonságért felelős szakemberei sokkal hitelesebb, elfogadhatóbb módon képesek a biztonsági kérdéseket menedzselni és a biztonságtechnikai rendszereiket megépíteni, és üzemeltetni.

A disszertációm egyik témáját képező videó megfigyelő rendszereket, önmagukban ritkán célszerű kiépíteni. Ez a megállapításom abból a korábban tárgyalt tervezési stratégiából következik, amely a meghiúsítás/elrettentés közötti különbségeken alapul. Amennyiben a meghiúsítást, mint tervezési elvet alkalmazzuk, a CCTV rendszer alapvetően a behatolásjelző berendezés része (azért kerül telepítésre, hogy a behatolást érzékelő, arról jelzést továbbító eszközök jeleit lehetőleg késlekedés nélkül, ellenőrizni és kiértékelni lehessen). Ez a tervezési elv nem csak a létesítményben létrehozott reagáló (készenléti) erő számára fontos (a korai riasztás – az egyes fizikai akadályok által biztosított késleltetésekkel – elegendő időt biztosít a behatolót semlegesítő tevékenység megkezdéséhez és sikeres végrehajtásához), hanem az élőerős őrzést biztosító szolgálat létszámát is képes optimális szinten tartani – ez pedig lényeges gazdasági szempont.[28]

Mindezek mellett egy CCTV rendszer tervezése és üzemeltetése nemcsak a behatolásjelző rendszer részét kell, hogy képezze. Fontos követelmény, hogy a teljes létesítmény területén –

[28] 2017-ben egy 24 órás biztonsági őr státusz fenntartása akár 15-20 millió forint is lehet évente.

építményeken belül, és azokon kívül is – történő mozgást (az adott létesítmény biztonsági kockázatainak függvényében) a megfelelő módon és lefedettséggel tudja ellenőrizni. Elengedhetetlen feltétel továbbá, hogy a kamerák által biztosított képeket az esetleges későbbi felhasználás érdekében archiválni lehessen – természetesen szigorúan a jogszabályoknak, belső előírásoknak megfelelően.

Videó megfigyelő rendszer tervezése során a rosszul megadott prioritások és igények meghatározásakor a kivitelezési költségek aránytalanul magasak lehetnek, amely sem egy felelős tervezőnek, sem a megbízónak nem lehet az érdeke.

2.3. A fejezet összegzése – következtetések

Az objektumorientált tervezés, mint elvárás, az adott létesítmény működésének és biztonsági kockázatainak teljes körű ismeretét igényli. A tervezési stratégia tekintetében mindkét alapelv (elrettentés és meghiúsítás) szerinti tervezési munka elvégezhető, de jól bizonyított, hogy a „meghiúsítási stratégia" lényegesen nagyobb pontossággal írja le egy-egy biztonsági rendszer (fizikai és védelmi) működését, valamint a rossz-szándékú behatoló tevékenységének a megakadályozását.

A biztonsági szakterület az adott létesítmény működtetését támogató szakterület - valamennyi beépített biztonságtechnikai rendszerrel, élőerős védelemmel, szabályzataival, rezsimintézkedéseivel együtt. Ennek funkciói, működtetése reális és koncepciózus tervezést követel. Mindezek következtében változik a biztonságtecnikai rendszer telepítésére vonatkozó alapindok is. A biztonságtechnikai rendszer nem egy önmagáért a biztonságért kialakítandó struktúra.

Egyértelműen megalapozott tehát az az igény, hogy egy adott létesítmény, gazdasági társaság biztonságos működését támogató fizikai védelmi rendszer tervezésekor és kivitelezésekor legyenek jól kidolgozott és világosan megfogalmazott kritériumok, amelyeket követve egy olyan megbízható rendszer hozható létre, amely figyelembe veszi az adott környezet veszélyeit, de nem túlméretezett a meglévő biztonsági kockázatokhoz képest.

3. KÜLÖNBÖZŐ BIZTONSÁGI KATEGÓRIÁJÚ LÉTESÍTMÉNYEKBEN TELEPÍTENDŐ BIZTONSÁGTECHNIKAI RENDSZEREK ALAPKÖVETELMÉNYEI

Ebben a fejezetben az általam meghatározott alapkövetelményeket, minimálisan kialakításra javasolt vagyonvédelmi és fizikai védelmi javaslatokat rögzítem az egyes létesítmények biztonsági kategóriába történő besorolása függvényében, biztonsági kategóriánként.

Ezek rendre: Fokozott, Magas, Közepes, Alacsony biztonsági kockázatú létesítményeket. Meghatározom, továbbá a létesítmények fizikai biztonsági attribútumát és foglalkozom továbbá az egyedi védettségű zónákkal is.

3.1. Fokozott Biztonsági Kockázatú Létesítmény (FBKZ)

Az egyes létesítmények, amelyekben a legmagasabb biztonsági kockázatú tevékenység folyik, magától értetődően a legmagasabb szintű fizikai védelemmel kell ellátni. Tekintettel kimagasló biztonsági kockázatra olyan veszélyek bekövetkezésére is készülni kell, amelyek bekövetkeztét a biztonsági kockázatokat értékelő szakértői csoport aktuálisan (historikus adatok nem lévén) magas hatásúnak, de alacsony eséllyel bekövetkezőnek tart. Ezek azok a veszélyek, amely a tervezési alapfenyegetettségről készülő dokumentum összeállításakor is kiemelt figyelmet kapnak.

A minimál követelmények meghatározásakor, a fizikai védelmi rendszer összeállításának követnie kell a biztonsági kockázatokat, ugyanakkor kiegyenlített védelmet kell biztosítania a teljes védelmi rendszer, valamennyi alrendszere, rendszereleme tekintetében. Ezzel a feltétellel lesz biztosítható az adott létesítmény biztonsági kockázataival, a védendő tevékenységgel arányos, ergo gazdaságosan kialakítható védelem.

3.1.1 Élőerős védelem

- az élőerős védelmet ellátó biztonsági szervezet számára egy recepciós/ügyfélfogadó pultot, illetve annak a műszaki, támogatási hátterét biztosító helyiséget kell kialakítani; (1, lásd 2. táblázat)
- a biztonsági őrség számára a szükséges kommunikációs eszközöket, azok használatának lehetőségét, a tevékenységük ellátásához szükséges egyéb, a szolgálatot biztosító társasággal egyeztetve, technikai, és egészségügyi körülmények meglétét kell biztosítani; (2)

- az élőerős védelem létszámát úgy kell meghatározni, hogy az a gépkocsibejárónál, az épület főbejáratánál, illetve a külső területeken a járőrözést is képes legyen ellátni; (3)
- a biztonsági őrség mellett a recepcióban dolgozó munkatársakat is foglalkoztatni kell, ahol a vendég fogadása, vendégkártyákkal történő ellátása kerül megszervezésre; (4)
- a létesítményben nem állandó belépőkártyával rendelkező személyek kizárólag kísérettel együtt mozoghatnak; (5)
- a létesítmény területén a rendszeres járőrözést biztosítani kell, amelyet őrjárat ellenőrzővel dokumentálni is szükséges. (6)

3.1.2 Mechanikai védelem

Kerítés

- létesítményhatáron legalább 250 cm magas, zártszelvényből készült, hegesztett kerítés telepítése szükséges; (1)
- a kerítéseken történő átmászást akadályozó mechanikai elemeket kell telepíteni; (2)
- a személy-, és gépkocsi bejárók számára a kerítés anyagával azonos mechanikai szilárdságú, nyitható/zárható kapuk felszerelése elengedhetetlen; (3)
- a záró/nyitó szerkezetek kialakításánál a hosszú távú, nagy igénybevételű terhelésekre kell felkészülni; (4)
- a gépkocsi bejáratoknál sorompót kell telepíteni, amelyet rendszám-felismerővel, illetve a munkatársak számára kiadott belépőkártyával kell vezérelni; (5)
- mind a személy-, mind a teherkapuknál kaputelefon beépítése szükséges;
- a kapuk távoli nyitását biztosítani kell. (6)

Falak, falazatok

- az épületfalazatok kialakításánál különleges biztonsági követelmények nincsenek.

Zárszerkezetek, zárbetétek

- a létesítményben csak minősített zárszerkezetek használhatók legalább 5 perces áttörésgátlással; (8)
- a létesítményben megerősített, és tanúsítvánnyal is rendelkező zárbetétek használhatók legalább 5 perces áttörésgátlással; (9)

– a zárbetétek felszerelésénél a kisebb, mint 4 mm-es túllógás megengedett a nem védett oldalon. (10)

Nyílászárók

– a létesítményben telepítendő nyílászáróknak több ponton kell záródniuk. (11)

3.1.3 Elektronikus védelem

Videó megfigyelő rendszer

– valamennyi kültéri bejárónál, illetve az épületekbe történő belépési pontoknál kamera elhelyezése szükséges; (1)
– a kamerák egy része által biztosított képeknek alkalmasnak kell lenniük a belépni szándékozók, illetve a belépett személyek azonosítására; (2)
– a kamerák másik részének továbbítania kell egy jól kiértékelhető képet a belépési pontokról, illetve az azok közvetlen környezetében történő eseményekről; (3)
– további kamerákat kell telepíteni a létesítményhatárok, épület falazatok ellenőrzésére oly módon, hogy a létesítményben tartózkodó személyek, és gépjárművek mozgása kitakarás-mentesen követhető legyen; (4)
– a kamerák telepítésénél biztosítani kell, hogy a létesítmény területén történő mozgásuk során az egyes személyek, gépkocsik azonosíthatók legyenek; (5)
– a videofelvételeket jogszabályok/belső szabályozás szerinti időtartamra archiválni kell. (6)
– a biztonsági őrségnél legalább 2 videó megfigyelő munkaállomást, 2 monitorral (munka és spot monitorok) kell elhelyezni, ahonnan az előképek, és az archivált anyagok is megtekinthetők. (7)

Behatolásjelző rendszer

– behatolásjelző rendszert kell kiépíteni a zónába tartozó épületekben; (8)
– a telepítendő behatolásjelző rendszerrel az épületek földszintjén és I. emeletén teljes körű védelmet kell kialakítani, a II. emelettől felfelé az épületfolyosókat, a lépcsőfordulókat szükséges teljes körű *térvédelem*mel ellátni; (9)
– a kerítés fedővédelméről gondoskodni kell egy kerítésvédelmi rendszer segítségével; (10)

- amennyiben *fedővédelem* nem alakítható ki, akkor a kerítés belső oldalán védőtávolságot kell meghatározni, amely területet mikrohullámú területvédelemmel kell ellátni; (11)
- a rendszer állapotát olyan távfelügyeleti szolgálat részére kell átjelezni, ahol kivonuló szolgálat is van; (12)
- a központi egység legalább 16 *partíció*-kezelést tegyen lehetővé. (13)

Beléptető rendszer

- a létesítményben kialakított kártyás beléptető rendszerrel kompatibilis beléptető rendszert kell telepíteni, amely az Egységes Beléptető Rendszer része; (14)
- a személyforgalom ellenőrzésére fémkereső kapuk telepítése szükséges; (15)
- a rendszert véletlen-generátoros személykiválasztó berendezéssel szükséges kiegészíteni, amely jelzésére az adott személy csomagja átvizsgálásra, a személy alkohol szonda használatára kötelezhető; (16)
- kétirányú belépési pontokat kell telepíteni az épületek bejáratainál; (17)
- kétirányú belépési pontokat kell kiépíteni az egyes épületrészek, folyosószakaszok bejáratainál; (18)
- az épületbe, az ellenőrzött területre történő első belépéshez a megszemélyesített proximity kártya mellett PIN kód is szükséges; (19)
- a gépkocsi bejáratnál rendszám-felismerő rendszert kell telepíteni; (20)
- az egyes épületeken belüli mozgás kártyákkal történő azonosítás mellett is lehetséges; (21)
- az épületen belül kialakított, fokozott biztonságot igénylő helyiségek zárásához, valamint a kulcsok biztonságos tárolásához hidegbélyegzővel felülbélyegzett kulcsdobozt, esetlegesen speciális kulcsszéfet kell használni (felvételi jogosultság meghatározása és a kiadás dokumentálása mellett); (22)
- beléptető rendszer kezelését legalább 3 munkaállomásnál biztosítani szükséges (recepció, porta és biztonsági munkatárs irodája). (23)

3.2. Magas Biztonsági Kockázatú Létesítmény (MBKL)

3.2.1 Élőerős védelem

- az élőerős védelmet ellátó biztonsági szervezet számára egy recepciós/ügyfélfogadó pultot, illetve annak a műszaki, támogatási hátterét biztosító helyiséget kell kialakítani;
- a biztonsági őrség számára a szükséges kommunikációs eszközöket, azok használatának lehetőségét, tevékenységük ellátásához szükséges egyéb technikai, és egészségügyi körülmények meglétét biztosítani szükséges;
- az élőerős védelem létszámát úgy kell meghatározni, hogy az a gépkocsibejárónál, az épület főbejáratánál, illetve a külső területeken a járőrözést is képes legyen biztosítani;
- a biztonsági őrség mellett recepcióban dolgozó munkatársakat is kell foglalkoztatni, ahol a vendég regisztrálása, fogadása, vendégkártyákkal történő ellátása megoldható;
- a létesítményben nem állandó belépőkártyával rendelkező személyek kizárólag kísérettel együtt mozoghatnak.

3.2.2 Mechanikai védelem

Kerítés

- a létesítményhatáron legalább 250 cm magas, 4 mm átmérőjű acélhuzalból, vagy zártszelvényből készült, hegesztett kerítés telepítése szükséges;
- a személy- és gépkocsi bejárók számára a kerítés anyagával azonos mechanikai szilárdságú, nyitható/zárható kapuk felszerelése elengedhetetlen;
- a záró/nyitó szerkezetek kialakításánál a hosszú távú, nagy igénybevételű terhelésekre kell felkészülni;
- a gépkocsi bejáratoknál sorompót kell telepíteni, amelyet rendszám-felismerővel, illetve a munkatársak számára kiadott belépőkártyával kell vezérelni;
- mind a személy-, mind a teherkapuknál kaputelefon beépítése szükséges;
- a kapuk távoli nyitását biztosítani kell.

Zárszerkezetek, zárbetétek

- a létesítményben használhatók nem megerősített zárszerkezetek;

– a létesítményben nem megerősített, de tanúsítvánnyal is rendelkező zárbetétek használhatók;
– a zárbetétek felszerelésénél a kisebb, mint 4 mm-es túllógás megengedett a nem védett oldalon.

Falak, falazatok

– az épületfalazatok kialakításánál különleges biztonsági követelmények nincsenek.

Nyílászárók

– a létesítményben telepítendő nyílászárók nem kell, hogy több ponton záródjanak.

3.2.3 Elektronikus védelem

Videó megfigyelő rendszer

– valamennyi kültéri bejárónál, illetve az épületekbe történő belépési pontoknál kamera elhelyezése szükséges;
– a kamerák egy része által biztosított képeknek alkalmasnak kell lennie a belépni szándékozók, illetve a belépett személyek azonosítására;
– a kamerák másik része továbbítson jól látható képet a belépési pontok, illetve azok közvetlen környezetében történő eseményekről;
– további kamerákat kell telepíteni a létesítményhatárok, épületfalazatok ellenőrzésére oly módon, hogy a létesítményben tartózkodó személyek, és gépjárművek mozgása kitakarás-mentesen követhető legyen;
– a videofelvételeket jogszabályok/belső szabályozás szerinti időtartamra archiválni kell.
– a biztonsági őrségnél legalább 2 videó megfigyelő munkaállomást, 2 monitorral (munka és spot monitorok) kell elhelyezni, ahonnan az előképek, és az archivált anyagok is megtekinthetők.

Behatolásjelző rendszer

– behatolásjelző rendszert kell kiépíteni a zónába tartozó épületekben;
– telepítendő behatolásjelző rendszerrel az épületek földszintjén és I. emeletén teljes körű védelmet kell kialakítani, a II. emelettől felfelé pedig az épületfolyosókat, a lépcsőfordulókat szükséges teljes körű térvédelemmel ellátni;
– a rendszer állapotát olyan távfelügyeleti szolgálat részére kell átjelezni, ahol kivonuló szolgálat is van;

– a központi egység legalább 8 partíció kezelését tegye lehetővé.

Beléptető rendszer

– a létesítményben kialakított kártyás beléptető rendszerrel kompatibilis beléptető rendszert kell telepíteni, amely az Egységes Beléptető Rendszer része;
– kétirányú belépési pontokat kell telepíteni az épületek bejáratainál;
– kétirányú belépési pontokat kell kiépíteni az egyes épületrészek, folyosószakaszok bejáratainál;
– az épületbe, az ellenőrzött területre történő első belépéshez a megszemélyesített proximity kártya mellett PIN kód is szükséges;
– az egyes épületeken belüli mozgás kártyákkal történő azonosítás mellett is lehetséges;
– a gépkocsi bejáratnál rendszám-felismerő rendszert kell telepíteni;
– a beléptető rendszer kezelését legalább 3 munkaállomásnál biztosítani szükséges (recepció, porta és biztonsági munkatárs irodája).

3.3. Közepes Biztonsági Kockázatú Létesítmény (KBKL)

3.3.1 Élőerős védelem

– az élőerős védelmet ellátó biztonsági szervezet számára egy recepciós/ügyfélfogadó pultot, illetve annak a műszaki, támogatási hátterét biztosító helyiséget kell kialakítani;
– a biztonsági őrség számára a szükséges kommunikációs eszközöket, azok használatának lehetőségét, a tevékenységük ellátásához szükséges egyéb technikai és egészségügyi feltételeinek meglétét biztosítani szükséges.

3.3.2 Mechanikai védelem

Kerítés

– a létesítményhatáron legalább 250 cm magas drótkerítés telepítése szükséges, amelyen roncsolás-mentes áthaladás nem lehetséges;
– a személy-, és gépkocsi bejárók számára a kerítés anyagával azonos mechanikai szilárdságú, nyitható/zárható kapuk felszerelése elengedhetetlen;

- a záró/nyitó szerkezetek kialakításánál a hosszú távú, nagy igénybevételű terhelésekre kell felkészülni;
- mind a személy-, mind a teherkapuknál kaputelefon beépítése szükséges;
- a kapuk távoli nyitására lehetőséget kell biztosítani.

Falak, falazatok

- az épületfalazatok kialakításánál különleges biztonsági követelmények nincsenek.

Zárszerkezetek, zárbetétek

- a létesítményben nem megerősített zárszerkezetek, zárbetétek is használhatók;
- a zárbetétek felszerelésénél a kisebb, mint 4 mm-es túlnyúlás megengedett a védett oldalon.

Nyílászárók

- a létesítményben telepítendő nyílászárók nem kell, hogy több ponton záródjanak.

3.3.3 Elektronikus védelem

Videó megfigyelő rendszer

- valamennyi kültéri bejárónál, illetve az épületekbe történő belépési pontnál kamera elhelyezése szükséges;
- a kamerák egy része által biztosított képeknek alkalmasnak kell lenniük a belépni szándékozók, illetve a belépett személyek azonosítására;
- a kamerák másik része továbbítson jól kiértékelhető képet a belépési pontok, illetve azok közvetlen környezetében történő eseményekről;
- további kamerákat kell telepíteni a létesítményhatárok, épület falazatok ellenőrzésére;
- a videofelvételeket jogszabályok/belső szabályozás szerinti időtartamra archiválni kell.
- a biztonsági őrségnél legalább 2 videó megfigyelő munkaállomást, 2 monitorral (munka és spot monitorok) kell elhelyezni, ahonnan az előképek, és az archivált anyagok is megtekinthetők.

Behatolásjelző rendszer (*csapdaszerű védelem*)

- behatolásjelző rendszert kell kiépíteni a zónába tartozó épületekben;

- telepítendő behatolásjelző rendszert az épületek földszintjén, I. emeletén teljes körű védelmet kell kialakítani, a II. emelettől felfelé pedig az épületfolyosókat, a lépcsőfordulókat teljes körű térvédelemmel kell ellátni;
- a rendszer állapotát olyan távfelügyeleti szolgálat részére kell átjelezni, ahol kivonuló szolgálat is van;
- a központi egység legalább 8 partíció kezelését tegye lehetővé.

Beléptető rendszer

- a létesítményben kialakított kártyás beléptető rendszerrel kompatibilis beléptető rendszert kell telepíteni, amely az Egységes Beléptető Rendszer része;
- kétirányú belépési pontokat kell telepíteni az épületek bejáratainál
- a beléptető rendszer kezelését legalább 2 munkaállomásnál biztosítani szükséges (porta és biztonsági munkatárs irodája).

3.4. Alacsony Biztonsági Kockázatú Létesítmény (ABKL)

3.4.1 Élőerős védelem

- A kategóriában nem szükséges.

3.4.2 Mechanikai védelem

Kerítés

- létesítményhatáron minimálisan fonott, 1,5 m magas drótkerítés telepítése szükséges;
- a személy-, és gépkocsi bejárók számára a kerítés anyagával azonos mechanikai szilárdságú, nyitható/zárható kapuk felszerelése elengedhetetlen;
- a záró/nyitó szerkezetek kialakításánál a hosszú távú, nagy igénybevételű terhelésekre kell felkészülni;
- mind a személy-, mind a teherkapuknál kaputelefon beépítése szükséges;
- a kapuk távoli nyitására lehetőséget kell biztosítani.

Falak, falazatok

- épületfalazatok kialakításánál különleges biztonsági követelmények nincsenek.

Zárszerkezetek, zárbetétek

- a létesítményben nem megerősített zárszerkezetek, zárbetétek is használhatók;

– a zárbetétek felszerelésénél a kisebb, mint 4 mm-es „túllógás” megengedett a nem védett oldalon.

Nyílászárók

– a létesítményben telepítendő nyílászárók nem kell, hogy több ponton záródjanak.

3.4.3 Elektronikus védelem

Videó megfigyelő rendszer

– valamennyi kültéri bejárónál, illetve az épületekbe történő belépési pontoknál kamera elhelyezése szükséges;
– a kamerák egy része által biztosított képeknek alkalmasnak kell lenniük a belépni szándékozók, illetve a belépett személyek azonosítására;
– a kamerák másik része továbbítson tiszta képet a belépési pontok, illetve az azok közvetlen környezetében történő eseményekről;
– a videofelvételeket jogszabályok/belső szabályozás szerinti időtartamra archiválni kell.
– a vezénylő épületben legalább egy videó megfigyelő munkaállomást, 2 monitorral (munka és spot monitorok) kell elhelyezni, ahonnan az előképek, és az archivált anyagok is megtekinthetők.

Behatolásjelző rendszer (csapdaszerű védelem)

– behatolásjelző rendszert kell kiépíteni a zónába tartozó épületekben;
– a telepítendő behatolásjelző rendszert az épületek földszintjén, I. emeletén csapdaszerűen kell kialakítani, azaz a bejáratokat, illetve az épületfolyosókat teljes körű térvédelemmel kell ellátni;
– a rendszer állapotát olyan távfelügyeleti szolgálat részére kell átjelezni, ahol kivonuló szolgálat is van.

Beléptető rendszer

– a létesítményben kialakított kártyás beléptető rendszerrel kompatibilis beléptető rendszert kell telepíteni, amely az Egységes Beléptető Rendszer része;
– kétirányú belépési pontokat kell telepíteni az épületek bejáratainál;
– a beléptető rendszer kezelését legalább egy munkaállomásnál biztosítani szükséges.

3.5. Létesítmények fizikai biztonsági attribútuma

A 3.1, 3.2, 3.3. és 3.4. fejezetek alapján határozom meg a következőben a létesítmények fizikai biztonsági attribútumát.

Létesítmények fizikai biztonsági attribútuma	"A" Élőerős védelem	"B" Mechanikai védelem	"C" Elektronikus védelem
Alacsony Biztonsági Kockázatú Létesítmény (ABKL)	0	0	0
Közepes Biztonsági Kockázatú Létesítmény (KBKL)	1	1	1
Magas Biztonsági Kockázatú Létesítmény (MBKL)	2	2	2
Fokozott Biztonsági Kockázatú Létesítmény (FBKL)	3	3	3

2. táblázat: Adott létesítmény védelmi tulajdonságát (attribútumát) meghatározó mátrix.

Az 2. táblázaton tanulmányozható mátrix egy adott létesítmény aktuális fizikai védelmét értékelő, biztonsági audit során felvehető adatokból kinyerhető, jellemző számhármas. Az adott biztonsági kockázatot értékelő szakértői csoport az auditot követően az aktuális élőerős, mechanikai, elektronikai védelmi körülményeket határozhatja meg a mátrix segítségével. A biztonsági felülvizsgálatot követően a fejlesztési igények azonnal jól láthatóak a meglévő és a szükséges létesítményi paraméterek (attribútumok) figyelembe vételével. Természetesen az ideális és optimális megoldás valamennyi értékelt létesítmény/intézmény esetében az lenne, ha a fizikai védelmi fejlesztéseket követően a létesítmény a biztonsági kockázatainak megfelelő értékelést kaphatna.

Tekintsük azt a példát, amikor az optimális érték egy Magas Biztonsági Kockázatú Létesítmény (MBKL) esetében az élőerős, a mechanikai, és az elektronikus védelem megfelel az adott létesítmény biztonsági kockázati besorolásához megjelölt minimális biztonságtechnikai követelményeknek. Az audit aztán feltárja az élőerős védelem gyengeségeit, majd a vezetőség intézkedik a megoldásra (2. táblázat).

Létesítmények fizikai biztonsági attribútuma	"A" Élőerős védelem	"B" Mechanikai védelem	"C" Elektronikus védelem	ÁTLAG
Magas Biztonsági Kockázatú Létesítmény (MBKL)	2	2	2	2,00
Magas Biztonsági Kockázatú Létesítmény (MBKL)	1	2	2	1,67
Magas Biztonsági Kockázatú Létesítmény (MBKL)	1	3	2	2,00

3. táblázat: Magas Biztonsági Kockázatú Létesítmény fizikai biztonsági attribútumainak átjárhatósága.

A biztonságtechnikai fejlesztéseket követően létrejött, a visszamérés után megállapítható létesítményt jellemző számhármas (1,3,2) mutatja, hogy a korábban meghatározott minimális biztonságtechnikai követelményekhez képest magasabb szintű mechanikai védelem került kiépítésre – így a számtani átlag újra megfelelő az optimális átlagértéknek. Ez azt jelenti, hogy kiváltható az élőerős őrzés egy költséghatékonyabb megoldással.[29]

3.3. Egyedi védettségű zónák

A fizikai biztonságról beszélve nem kerülhetők meg az egyedi védettségi igényű helyiségek, építmények.

Az egyedi védettségű zónák kijelölését annak érdekében szükséges elvégezni, hogy a speciális igények a kialakított struktúrába jól beilleszthetők legyenek. Ennek megfelelően az MVM Vállalat Csoportnál az alábbi egyedi védettségű zónák kerülnek meghatározásra:

1. Pénztár (házipénztár).
2. Személyi Nyilvántartó (HR adatok kezelése).
3. Minősített Adatok Kezelés (papír alapú és elektronikus nemzeti minősített adatok tárolása).
4. Szerver helyiségek.

[29] A költségmegtakarítás igen jelentős a Magyar Villamos Műveknél, ahol az élőerős védelemben dolgozó valamennyi munkatárs esetében is elvárás a jogszabályoknak mindenben megfelelő foglalkoztatás. Egy 24 órás biztonsági őr munkakör éves teljes költsége (így a megtakarítás is egyben) elérheti a 20 millió forintot, azaz a technikai feltételek javítása jelentős költségmegtakarítást eredményezhet.

Ebben a felsorolásban lévő egyedi védettségi igényekkel rendelkező helyiségek, építmények esetében a minimális biztonságtechnikai rendszerkövetelményeket a következőkben ismertetem. Ez a meghatározás szervesen illeszkedik a létesítmények besorolásához, azok alapbesorolását mutatja meg.

A meghatározott biztonsági kockázatú létesítményen belül lehet megjelölni az egyes speciális védelmi igények szerint kijelölt helyiségek, akár építmények minimális biztonságtechnikai követelményeit.[30]

3.6.1 Pénztár (házipénztár)

Mechanikai védelem (a MABISZ ajánlások irányadók)

- legalább téglafalazat, vagy annak megfelelő mechanikai szilárdságú egyéb kiépítésű határoló falak;
- megerősített zárszerkezetek;
- minősített zárbetétek;
- több ponton záródó bejárati ajtó;
- nem nyitható ablak, amely ráccsal, vagy MABISZ ajánlással rendelkező betörés gátló fóliával védett min. 0,150 mm vastag, minősített kivitelben;
- a pénztárhelyiségben az értékeket, pénzt kizárólag minősített, értéktárolásra gyártott, a tárolandó értéknek megfelelő biztosítást garantáló értéktárolóban szabad elhelyezni;
- az értéktoló szekrénynek (páncélszekrény) a mechanikus zár mellett legalább még egy mechanikus, vagy minősített elektronikus zárral kell rendelkeznie;
- az értéktárolónak saját, a gyártó által előkészített, a biztonsági rendszerhez történő bekötést támogató szekrényelemeket kell használnia.

Elektronikus védelem

Videó megfigyelő rendszer

- a pénztár előteréről folyamatos videó felvételt kell készíteni az épület videó megfigyelő rendszer részeként;

[30] Az felsorolt biztonságtechnikai jellemzők az adott biztonsági kockázatú létesítményre szabott paramétereken felül értendők.

– a videofelvételeket jogszabályok/belső szabályozás szerinti időtartamra archiválni kell.

Behatolásjelző rendszer

– a pénztár helyiségeit akusztikus üvegtörés-érzékelővel védeni kell;
– a pénztár helyiségeinek teljes körű térvédelmét biztosítani kell duál technológiás (mikrohullámú radar, és passzív infravörös mozgásérzékelő logikai kapcsolatban és azonos érzékelő-tokozásban) mozgásérzékelővel;
– valamennyi nyílászárót rejtetten telepített *nyitásérzékelő*vel kell ellátni;
– az értéktároló szekrényre nyitás-, és rezgésérzékelőket kell telepíteni;
– „kényszerített nyitás" jelzés *hangjelzés* nélküli továbbítását a saját biztonsági szolgálat, illetve a távfelügyeleti szolgálat részére biztosítani kell;
– a munkatársak személyi védelme érdekében pánikjelzők telepítése szükséges a munkaasztalok alatt, vagy rádiós kivitelben;
– a pénztárhelyiség kezelése önálló partícióként, saját *kezelőegység*gel történjen.

Beléptető rendszer

– a pénztárhelyiségbe történő belépés belépő kártyás azonosítást követően legyen lehetséges.

3.6.2 Személyi Nyilvántartó (HR adatok tárolása)

Mechanikai védelem

– legalább téglafalazat, vagy annak megfelelő mechanikai szilárdságú egyéb kiépítésű határoló falak;
– megerősített zárszerkezetek;
– minősített zárbetétek;
– több ponton záródó bejárati ajtó;
– nem nyitható ablak, amely ráccsal, vagy MABISZ ajánlással rendelkező betörés gátló fóliával védett min. 0,150 mm vastag, minősített kivitelben;
– a nyilvántartó helyiségben az iratok lehetőleg irattárolásra gyártott, 60 perces tűzgátlást biztosító értéktárolóban kerüljenek;
– értéktároló szekrénynek a mechanikus zár mellett legalább még egy mechanikus, vagy minősített elektronikus zárral kell rendelkeznie.

Elektronikus védelem

Videó megfigyelő rendszer

- a nyilvántartó helyiségbe történő belépésekről folyamatos, a személyek azonosítását lehetővé tevő videó felvételt kell készíteni;
- a videofelvételeket jogszabályok/belső szabályozás szerinti időtartamra archiválni kell.

Behatolásjelző rendszer

- a nyilvántartó helyiséget akusztikus üvegtörés-érzékelővel védeni kell;
- a nyilvántartó helyiség teljes körű térvédelmét biztosítani kell ún. duál technológiás (mikrohullámú radar és passzív infravörös) mozgásérzékelővel;
- valamennyi nyílászárót rejtetten telepített nyitásérzékelővel kell ellátni;
- az értéktároló szekrényre nyitás és rezgésérzékelőket kell telepíteni;
- a nyilvántartó helyiség kezelése önálló partícióként, saját kezelőegységgel történjen.

Beléptető rendszer

- a nyilvántartó helyiségbe történő belépés belépő kártyás azonosítást követően legyen lehetséges.

3.6.3 Minősített Adatok Kezelés

A nemzeti minősített adatok (papír és elektronikus alapú) tárolásához külön jogszabályi környezet áll rendelkezésre, amelyben megtalálhatóak a biztonságtechnikai eszközök alkalmazási lehetőségei is. Ezen szabályozói környezet jól illeszkedik az általam kidolgozott biztonsági kockázati rendszerbe: I. osztályú biztonsági terület (minősített adat nyílt tárolása) és II. osztályú biztonsági terület (minősített adat zárt tárolása) 90/2010 (III.26) Korm. rendeletben meghatározottak szerint.

3.6.4 Szerver helyiségek

Mechanikai védelem

- legalább téglafalazat, vagy annak megfelelő mechanikai szilárdságú egyéb kiépítésű határoló falak;
- megerősített zárszerkezetek;
- minősített zárbetétek;

- több ponton záródó bejárati ajtó;
- nem nyitható ablak, amely ráccsal, vagy MABISZ ajánlással rendelkező betörés gátló fóliával védett min. 0,150 mm vastag, minősített kivitelben.

Elektronikus védelem

Videó megfigyelő rendszer

- a szerver helyiségbe történő belépésekről folyamatos, a személyek azonosítását lehetővé tevő videó felvételt kell készíteni;
- a videofelvételeket jogszabályok/belső szabályozás szerinti időtartamra archiválni kell.

Behatolásjelző rendszer

- a szerver helyiség teljes körű térvédelmét biztosítani kell duál technológiás (mikrohullámú radar és passzív infravörös) mozgásérzékelővel;
- valamennyi nyílászárót rejtetten telepített nyitásérzékelővel kell ellátni;
- a szerver helyiségek mennyezetének nedvességérzékelését lehetőleg a szerver helyiség fölötti helyiségek padlójánál kell megoldani (amennyiben az szükséges);
- a szerver helyiség kezelése önálló partícióként, saját kezelőegységgel történjen.

Beléptető rendszer

- a nyilvántartó helyiségbe történő belépés belépő kártyás és PIN kódos azonosítást követően legyen lehetséges.

Az egyedi védettségű zónák kiegészítő védelme tanulmányozható a 3. táblázatban.

Megnevezés	Az adott létesítményi biztonsági kockázati besorolását kiegészítő védelem
Pénztár	A kezelt pénz mennyiségének és a belső szabályozók függvényében.
Személyi Nyilvántartó	A hatályos adatvédelmi szabályok szerinti kialakítás.
Minősített Adatok Kezelése	Minősítésnek (EU, NATO, nemzeti) megfelelő kialakítás.
Szerver helyiségek	A futtatott alkalmazások, adatok és sérülékenység függvényében.

4. táblázat: Egyedi védettségű zónák kiegészítő védelme

3.4. A fejezet összegzése - következtetések

A biztonsági kockázatokkal arányos, kiegyenlített és koherens védelem kialakításával, a minimális követelmények megalkotásával egy olyan környezetet építettem fel, amely megfelelő szakmai ismeretek és gyakorlat esetén egy-egy létesítmény esetében támpontot ad az optimális, a meglévő biztonsági kockázatok kezelését lehetővé tevő biztonsági rendszer megtervezéshez és kialakításához. Mindezek mellett a megrendelői oldalt is támogatja a szakmai igények pontos megértésében, ugyanakkor lehetőséget biztosít számára a szükséges biztonsági költségvetés összeállításában.

A minimális követelményrendszer megalkotásával támogatni szeretném azokat a törekvéseket, amelyek a biztonsági költségek optimalizálása irányába hatnak. A személyi költségek folyamatos emelkedése, az üzemeltetőknek erre kell számítaniuk a közeljövőben is, fokozott hangsúlyt helyez a technikai megoldások előtérbe helyezésére, amellyel a biztonsági kockázatok kezelése teljes egészében megoldható, miközben az őrzött órák számát racionalizálni lehetséges.

4. A KOCKÁZATÉRTÉKELÉSRŐL

„A veszély elmúltával Isten neve is eltűnik.”[31]

A fejezetben meghatározom azokat a kockázatértékelés elvégzéshez szükséges mátrixokat, amelyekkel az általam kidolgozott rendszer megvalósítható. Részletesen levezetem az ún. Létesítményi együttható meghatározását, a „Veszélyfelhő” összeállítását és az egyes elemi veszélyek esetleges bekövetkezésének kockázatait.

A biztonsági kockázatok megfelelő értékelése kulcskérdés minden olyan környezetben, amelyben vannak védendő értékek és/vagy adatok annak érdekében, hogy a kockázatok kezelésének optimalizált módja meghatározható legyen. Az ún. optimalizált mód ebben az esetben a kockázatarányos, kiegyenlített[32] védelem kialakítását jelenti, amely szinte minden környezetben pénzügyi szempontból a legkedvezőbb megoldást jelenti. Ez abban az esetben elfogadható a megbízók, üzemeltetők számára, ha nyilvánvalóvá vált, hogy mely biztonsági kockázatokat kell kezelni. [17]

Az első feltétel a teljesen stabil auditálási rendszer megalapozása, amelyre azután az értékelési rendszer építhető, kialakítható és hitelesíthető lesz.

Fontos szempont az is, hogy egy ország közintézményei, gazdasági társaságai rendkívüli változatosságot mutatnak védelmi szempontból. Így könnyen belátható, hogy az egyes létesítmények kockázati kategóriákba sorolásával egy egységes rendszer is kialakítható.

Munkám során áttekintettem a kockázatértékelési lehetőségeket. Hazánkban jelentős – ipari környezetben is meghatározó – kockázatértékelési és kezelési tevékenységet folytató társasággal, illetve szakértőikkel több egyeztetést és konzultációt is folytattam. Ezen kutatótevékenység által egyértelművé vált számomra, hogy a biztonsági kockázatok kezelésének egy egyszerűen, jól követhető módon kialakított megoldását kell választanom, amely a nem szakavatott személyek (sok esetben maga a megrendelő) számára is érthető és követhető.

---

[31] Mahatma Gandhi (Mohandas Karamcsand Gandhi, 1869-1948)

[32] Kiegyenlített (balanced) védelem ebben az esetben azt jelenti, hogy a fizikai védelmi rendszer valamennyi elemére, alrendszerére közel azonos szintű, „egyenszilárdságú” védelmet alakítunk ki.

Áttanulmányozva a kockázatkezelésre vonatkozó nemzetközi szabványt[33] és a lehetséges kockázatkezelési módszereket, a biztonsági rendszerek tekintetében az eseményelemzés módszerének kiválasztása jó elgondolás, amely megoldás a korábban rögzített kívánalmaknak is megfelel.

Értekezésemben négy biztonsági kockázatú létesítményi kategória meghatározására, valamint a hozzátartozó biztonságtechnikai rendszerkialakítási és értékelési elvekre teszek javaslatot.

A négy biztonsági kockázatú létesítményi kategória az elektronikus információbiztonsággal kapcsolatos fizikai védelmi rendelkezések számára is megfelelő lehet. Ebbe a kockázati rendszerbe e szakterület is jól beilleszthető. Ezeknek a biztonsági kockázati szinteknek a meghatározásához egy jól érthető, követhető kockázatértékelési módszert dolgoztam ki annak érdekében, hogy az objektivitási elvek messzemenően transzparensek legyenek.

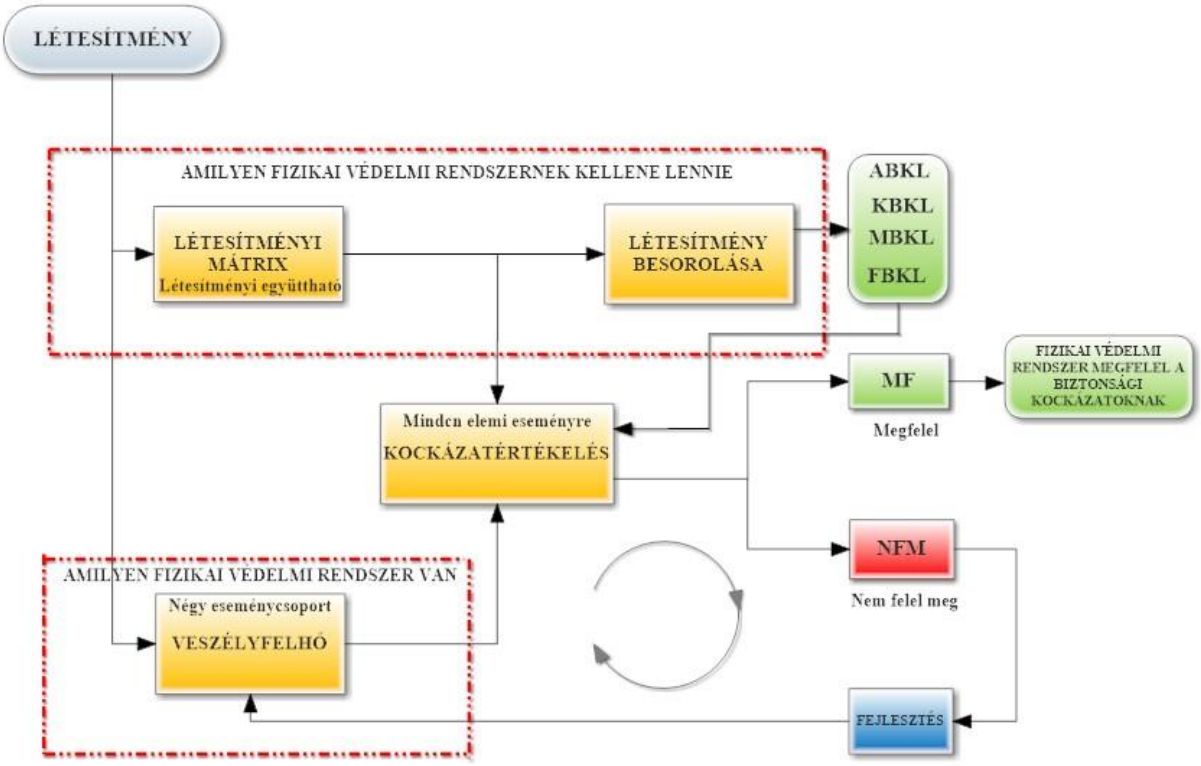
A kockázatértékelés tekintetében fontos tudni, hogy az esetenként jelentős pénzügyi erőfeszítéseket igényel, de amint John. M. White írja: „…It is safer and less costly to prevent an incident than is to act in response to one….", vagyis Biztonságosabb és olcsóbb megelőzni egy esemény bekövetkezését, mint reagálni arra. [18]

4.3. A kockázatértékelés folyamata

A kockázatértékelés logikai folyamatáról készített 7. ábrán látható, hogy valójában két, egymástól jól elkülöníthető szakasz alkotja. Egyik része az amilyen fizikai védelmi rendszernek kellene lennie az adott létesítményben, függően a létesítmény biztonsági besorolásától, másik szakasza pedig, hogy ténylegesen milyen fizikai védelmi rendszer van („Veszélyfelhő") telepítve a vizsgált létesítményben.

[33] ISO/IEC 31010:2009 – Kockázatértékelési módszerek

Amennyiben a két folyamat összevetéséből az eredmény „MF – Megfelelő”, ekkor nincs további teendő a védelmi rendszer tekintetében, hiszen az optimálisan funkcionál. Abban az esetben, ha a kockázatértékelés eredménye „NMF – Nem megfelelő”, akkor a fizikai védelmi rendszert fejleszteni szükséges a minimál követelmények teljesítéséhez.



7. ábra: A kockázatértékelés logikai folyamata

4.4. A létesítmények biztonsági kockázati besorolása és a létesítményi mátrix

Elsődlegesen meg kell határozni az önkényesen felvett négy biztonsági kockázati létesítménykategória kockázatértékelési alapjait. Első lépésben jelölni szükséges azokat a veszélyeket („Veszélyfelhő” létrehozása), amelyek relevánsak a kockázatértékelési rendszer kidolgozásához.

A veszélyek meghatározásánál a magyarországi gyakorlatot vettem figyelembe és a valószínűsíthető lehetőségekkel foglalkoztam. Meg kell azonban jegyezni, hogy ezek a veszélyek tetszés

szerint cserélhetők és bővíthetők. A szűkítés (témakörönként tíz-tíz) nem célszerű, mert ez esetben a biztonsági kockázatok nem fedik le az adott létesítmény tevékenységével kapcsolatos biztonsági kockázatokat.

A „Veszélyfelhő" valamennyi eleme a meglévő fizikai védelmi rendszerre vonatkozik, ugyanakkor nem a kockázatok teljes spektrumát tekintem (sem az üzleti folyamatok, sem az időjárási körülmények változásból adódó kockázatokkal nem foglalkozom - ezek ugyan fontosak, de egy másik kockázatértékelési rendszer részét kell, hogy képezzék). Valamennyi biztonsági kockázat (veszély) ennek megfelelően kerül a „Veszélyfelhőbe". A „Veszélyfelhőben" megjelölt veszélycsoportok is szabadon bővíthetők az adott létesítmény aktuális működési körülményei szerint. Ezek dinamikusan változtathatók és ennek megfelelően az aktuális biztonsági kockázatok változása jól követhető, így pedig a kockázatok kezeléséhez szükséges intézkedések haladéktalanul megtehetők.[34]

Az egyes létesítmények biztonsági kockázatok szerinti besorolását a „Létesítményi mátrix" eredményéből adódóan végeztem el. A „Létesítményi mátrix" lehetőséget teremt arra, hogy a vizsgált létesítmények a biztonsági kockázatok alapján összehasonlíthatók legyenek. Ennek alappillére az egyes létesítmény működéséből, annak körülményeiből adódó paraméterek. Az egyes létesítmények mindezek segítségével, a társadalmi beágyazódottságuk, illetve az általuk alkalmazott technológia védelmi igényei, valamint adatvagyonának érzékenysége alapján egy „Létesítményi együtthatóval" reprezentálhatók. Az egyes létesítmények biztonsági kategóriába történő besorolásához készítettem el azokat minimál követelményeket, amelyek megfelelnek az egyes védelmi igényeknek.

A kockázatértékelő alapmátrix kiegészítéséhez megalkottam tehát a „Létesítményi mátrixot" (5. táblázat), amely az adott létesítmény/gazdasági társaság társadalmi beágyazottságát, illetve az adott intézményben használt technológia, valamint a védendő adatokat és azok jellemzőit is bevonja a kockázatértékelés folyamatába.

[34] Példaként: az adott létesítmény beléptetési rendjét tartalmazó szabályzat módosítása, a biztonsági technikai rendszerek bővítése, átalakítása akár részleges visszabontása.

LÉTESÍTMÉNYI MÁTRIX			LÉTESÍTMÉNY HATÁSA A KÖRNYEZETÉRE (Társadalmi beágyazódottság)				
			A társaság/intézmény üzletmenet-folytonosságának sérülése esetén a tevékenység akadozik, megszűnik és maximálisan néhány száz főt érint. Nem igényel semmilyen helyi/kormányzati szintű beavatkozá	A társaság/intézmény üzletmenet-folytonosságának sérülése esetén a tevékenység akadozik, megszűnik és maximálisan néhány száz főt érint, de hatása a környező lakosság számára nehézséget jelent. A helyi hatóságok beavatkozására szükség lehet. (Pl.: helyi vízszolgáltatás)	A társaság/intézmény üzletmenet-folytonosságának sérülése esetén a tevékenység akadozik, megszűnik és maximálisan néhány ezer főt érin de hatása a környező lakosság számára nehézséget jelent. A helyi hatóságok/ kormányzati adminisztráció beavatkozására szükség lehe (Pl.: tartalék erőművek)	A társaság/intézmény üzletmenet-folytonosságának sérülése esetén a tevékenység akadozik, megszűnik és maximálisan néhány ezer főt érin de hatása a környező lakosság számára nehézséget jelent. A helyi hatóságok/ kormányzati adminisztráció beavatkozása nélkül nehezo oldható meg a probléma. (Pl.: városi vízszolgáltatás)	Régiós beágyazottság kiemelkedő, sok ezres létszámú munkavállalók kör, a tevékenység megszűnése országos, vagy nagyobb hatású. Kormányzati adminisztráció számára nehézséget okoz.
			1	2	3	4	5
VÉDENDŐ TECHNOLÓGIA/ADATOK	A védendő intézmény/vállalat önmaga számára védendőnek ítélt technológiát nem alkalmaz, védendő adatokkal (kivéve a védendő személyi, alapvetően HR adatok) nem dolgozik.	1	1	2	3	4	5
	A védendő intézmény/vállalat önmaga számára csak részben védendőnek ítélt technológiát alkalmaz, melynek sérülése önmaga számára okozhat nehézségeket, védendő adatokkal (kivéve a védendő személyi, alapvetően HR adatok) nem dolgozik.	2	2	4	6	8	10
	A védendő intézmény/vállalat önmaga számára védendőnek ítélt technológiát alkalmaz, melynek sérülése, illetve adatvagyonának nyilvánosságra kerülése lokális problémákat okozhat.	3	3	6	9	12	15
	A védendő intézmény/vállalat önmaga számára védendőnek ítélt technológiát alkalmaz, amelynek sérülése, adatvagyonának nyilvánosságra kerülése regionális problémákat okozhat.	4	4	8	12	16	20
	A védendő intézmény/vállalat védendőnek ítélt technológiát alkalmaz, amely technológia sérülése, adatvagyonának nyilvánosságra kerülése esetén kormányzati problémákat okozhat. (pl.: országos/régiós villamosenergia ellátás; nemzeti/EU/NATO minősített adatok)	5	5	10	15	20	25

5. táblázat: Létesítményi mátrix[35]

A Létesítményi mátrixban az adott létesítmény társadalmi elfogadottságának és az általa alkalmazott technológia és az adatvagyona védelmi igénye szorzatát képezem. A Létesítményi mátrix elemeinek kialakításához, mind szellemiségében, mind tartalmában igénybe vettem az Európai Unió 2008/114/EC direktíváját, amely a kritikus infrastruktúrák azonosítása, védelme tárgyában került kiadásra. Ez a direktíva az Egyesült Államok Kongresszusa által elfogadott tudományos, kutatási anyagra alapoz, amelyben a szakértők pontosan meghatározzák azokat az elveket, amelyek a kritikus infrastruktúra meghatározásában alapvetők. [19]

[35] A színek magyarázata: zöld: alacsony, citrom sárga: közepes, narancs sárga: magas, piros: fokozott kockázat.

Ez a Létesítményi mátrix tehát maga a hozzáadott érték az eddigi, már jól ismert kockázatértékelési módszerhez. Ezt azért készítettem el, hogy az intézmények, gazdasági társaságok biztonsági auditja során ne az adott létesítményt, mint egy önálló egységet elszigetelten elemezzük, hanem analizáljuk a környezetéhez, a magyar gazdasághoz, az azt működtető munkavállalókhoz, a lakókörnyezetéhez és esetleg tágabb régiójához való viszonyát is. Megfelelő mennyiségű biztonsági kockázatelemzés elkészítésével egy olyan adatbázis nyerhető, amely egy adott régió biztonsági szakterületi sérülékenységét képes reprezentálni. Ez érdemben hozzájárul egy sor magas színvonalú javítóintézkedés bevezetéséhez.

A Létesítményi mátrixban egy az adott létesítmény társadalmi elfogadottságának és az általa alkalmazott technológia és az adatvagyona védelmi igénye szorzatát képezem. Részletesen:

Társadalmi elfogadottság, mint a szorzat egyik eleme **(1. dimenzió)**

1. A védendő intézmény/vállalat önmaga számára védendőnek ítélt technológiát nem alkalmaz, védendő adatokkal (kivéve a védendő személyi, alapvetően HR adatok) nem dolgozik. (Például: csónakház, áruházak, autószerviz, stb.).

2. A védendő intézmény/vállalat önmaga számára csak részben védendőnek ítélt technológiát alkalmaz, melynek sérülése önmaga számára okozhat nehézségeket, védendő adatokkal (kivéve a védendő személyi, alapvetően HR adatok) nem dolgozik. (Például: csatornázási művek, taxi szolgáltatók, stb.).

3. A védendő intézmény/vállalat önmaga számára védendőnek ítélt technológiát alkalmaz, melynek sérülése, illetve adatvagyonának nyilvánosságra kerülése lokális problémákat okozhat. (Például: régiós villamos erőmű, tervező irodák, stb.).

4. A védendő intézmény/vállalat önmaga számára védendőnek ítélt technológiát alkalmaz, amelynek sérülése, adatvagyonának nyilvánosságra kerülése regionális problémákat okozhat. (Például: regionális ellátást biztosító villamos erőmű, mobil szolgáltatók, stb.).

5. A védendő intézmény/vállalat védendőnek ítélt technológiát alkalmaz, amely technológia sérülése, adatvagyonának nyilvánosságra kerülése esetén kormányzati problémákat okozhat. (pl.: országos/régiós villamosenergia ellátás; nemzeti/EU/NATO minősített adatok) (Például: országos hatáskörű szervezetek, titkosszolgálati adatok, atomerőmű, tartalék gázerőmű, villamos rendszerirányítás, stb.).

Alkalmazott technológia és meglévő adatvagyon, mint a szorzat másik tényezője **(2. dimenzió)**

1. A társaság/intézmény üzletmenet-folytonosságának sérülése esetén a tevékenység akadozik, megszűnik és maximálisan néhány száz főt érint. Nem igényel semmilyen helyi/kormányzati szintű beavatkozást. (Például: egy-egy élelmiszer bolt, kisméretű pékség, autószerviz, stb.).

2. A társaság/intézmény üzletmenet-folytonosságának sérülése esetén a tevékenység akadozik, megszűnik és maximálisan néhány száz főt érint, de hatása a környező lakosság számára nehézséget jelent. A helyi hatóságok beavatkozására szükség lehet. (Pl.: helyi vízszolgáltatás) (Például: bevásárló központok, lokális, kisméretű vízművek, stb.).

3. A társaság/intézmény üzletmenet-folytonosságának sérülése esetén a tevékenység akadozik, megszűnik és maximálisan néhány ezer főt érint, de hatása a környező lakosság számára nehézséget jelent. A helyi hatóságok/ kormányzati adminisztráció beavatkozására szükség lehet. (Például: lokális szemétszállítás, lokális vízművek, üzemanyag ellátás kiesése, szállítással foglalkozó társaságok, stb.).

4. A társaság/intézmény üzletmenet-folytonosságának sérülése esetén a tevékenység akadozik, megszűnik és maximálisan néhány ezer főt érint, de hatása a környező lakosság számára nehézséget jelent. A helyi hatóságok/ kormányzati adminisztráció beavatkozása nélkül nehezen oldható meg a probléma. (Pl.: városi vízszolgáltatás, szemétszállítás, logisztikai központok, stb.).

5. Régiós beágyazottság kiemelkedő, sok ezres létszámú munkavállalói kör, a tevékenység megszűnése országos, vagy nagyobb hatású. Kormányzati adminisztráció számára nehézséget okoz. (Például: tartalék villamos erőmű, villamos rendszerirányítás, regionális, vagy nagyobb távközlési szolgáltató, stb.).

Tekintettel a Létesítményi mátrixban foglalt jellemzőkre, a teljes kockázatértékelési folyamat első lépéseként az adott auditálandó intézményre, illetve gazdasági társaságra jellemző „Létesítményi mátrix" eredmény meghatározását kell elvégezni. Ezen prioritás indoka, hogy a „Veszélyfelhő" egyes elemi biztonsági kockázatai alapvetően függnek, illetve függhetnek az adott létesítményben alkalmazott technológiától, a védendő adatvagyontól, illetve az intézmény társadalmi beágyazottságától.

A Létesítményi mátrix alapján az auditálandó, a biztonsági kockázatokat megállapító, értékelő folyamatot megelőzően biztonsági kategóriába sorolást kell végezni (6. táblázat). Ennek alapját

az adott intézmény/vállalat társadalmi beágyazódottsága, az általa alkalmazott technológia védelmi igényei döntik el.[36]

MEGNEVEZÉS	RÖVIDÍTÉS	KOCKÁZATI ÉRTÉK	JELÖLÉS
Alacsony Biztonsági Kockázatú Létesítmény	ABKL	1, 2	
Közepes Biztonsági Kockázatú Létesítmény	KBKL	3, 4	
Magas Biztonsági Kockázatú Létesítmény	MBKL	5, 6, 8, 9, 10, 12, 15, 16	
Fokozott Biztonsági Kockázatú Létesítmény	FBKL	20,25	

6. táblázat: A létesítmények biztonsági kockázatú besorolása.[37] (készült az 5. táblázat alapján)

4.5. A „Veszélyfelhő" létrehozása

Meghatároztam egy viszonylag széleskörű listát annak érdekében, hogy a létesítményeket az aktuális biztonsági kockázatok szerint vizsgálni tudjuk. Az elemi események (melyek biztonsági kockázatokat jelentenek) listáját azonban valamennyi konkrét létesítmény esetén testre kell szabni. Gyakorlati szempontból ez azt jelenti, hogy egy biztonsági kockázatokat meghatározó „Veszélyfelhőt" hoztam létre, amely a későbbiekben a környezeti, intézményi/vállalati és technológiai változások szerint módosítható, az éppen hatályos szabályok szerint kiegészíthető, sőt ezt az aktualizálást ciklikusan és visszatérően el is kell végezni. Az elemi események vizsgálatakor minden esetben azt kell szemügyre venni, hogy az adott elemi esemény milyen hatással van a létező fizikai védelmi rendszerre.

A Veszélyfelhő elemei (valamennyi elem a fizikai védelmi rendszerre megfelelő működésének biztonsági kockázatait rögzíti), biztonsági veszélyei adódhatnak a létesítmény működéséből (7. táblázat), műszaki problémákból (8. táblázat), bűnügyi fertőzöttségből (9. táblázat) és emberi munkavégzésből (10. táblázat)

[36] Az általam kidolgozott biztonsági auditból kinyerhető adatok üzleti titkok, de akár nemzeti minősített adatokká is válhatnak, így az auditálandó létesítmény adataival, a kockázatkezelésre adott javaslatokkal ennek megfelelően kell eljárni. Hangsúlyozottan fontos, hogy az egyes létesítmények biztonsági kategóriákba történő besorolását gondos kiválasztás, fegyelmezett, esetenként a jogszabályoknak, belső szabályozásnak tökéletesen megfelelő munkavégzés jellemezze.

Tétel	Veszélyek megnevezése
1	**Működésből adódó biztonsági veszélyek**
1.1	Tevékenységből adódóan ügyfélfogadás van a létesítményben
1.2	Közismert a létesítményben folyó tevékenység
1.3	Közismert a létesítményen belüli környezet, felhasznált technológia
1.4	Létesítményben több intézmény/társaság tevékenykedik
1.5	Számítani lehet a végzett tevékenysége elleni akár erőszakos lakossági tiltakozásokra
1.6	A létesítmény ellen elkövetendő terrortámadás reális veszély
1.7	Nincsenek kidolgozott szabályzatok, rutinok a krízishelyzetek kezelésére (ÜFT; Pandémiás terv; stb.)
1.8	Nincsenek a létesítmény működéséhez kidolgozott és érvényben lévő biztonsági szabályzatok
1.9	Létesítménybe ellenőrzés nélkül léphetnek személyek és/vagy vihetnek be- és ki csomagokat
1.10	Meglévő porta, recepciós, őrszolgálat csomagokat átvehet, őrizhet, továbbíthat

7. táblázat: A létesítmény saját működéséből adódó lehetséges veszélyek.

Tétel	Veszélyek megnevezése
2	**Műszaki problémákból adódó biztonsági veszélyek**
2.1	Villamos energia kiesése (áramszünet)
2.2	Közvilágítással, világítással kapcsolatos üzemszünet (látási problémák)
2.3	Nincs önálló hálózat (más hálózattól fizikailag elválasztott) kiépítve a biztonságtechnikai rendszerek számára (DEPEDENCIA)
2.4	Természeti csapás (műszaki problémákat generált) miatt a létesítmény üzeme akadozik, leállt
2.5	Kiépített biztonságtechnikai rendszerek nincsenek.
2.6	Vannak kiépített elektronikus biztonságtechnikai rendszerek, de nincs rendszeres karbantartás, a szükséges javítások nem készülnek el időben.
2.7	Nincs, vagy nem megfelelő a kiépített szünetmentes berendezés, illetve hálózat a biztonságtechnikai rendszerek számára.
2.8	Létesítmény kerítéssel nem, vagy csak részben van elválasztva a környezetétől. A meglévő kerítés állapota nem megfelelő
2.9	Meglévő biztonságtechnikai rendszerek üzemideje meghaladta a 10 évet, és/vagy a gyártói támogatás megszűnt.
2.10	A létesítményben veszélyes kategóriájú technológiai, biztosnági szempontból kockázatos anyagokkal, folyamatok zajlanak.

8. táblázat: A létesítmény műszaki problémáiból adódó lehetséges veszélyek.

Tétel	Veszélyek megnevezése
3	**Bűnügyi fertőzöttségből adódó biztonsági veszélyek**
3.1	Létesítmény környezetében a tulajdon ellen elkövetett cselekmények éves száma országos átlag, vagy az feletti
3.2	Létesítményben végzett technológiai folyamatokat kurens (fekete gazdaság területén keresett és jól eladható) anyagokkal, szerszámokkal folytatnak.
3.3	Társaság által használt gépkocsikban beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs.
3.4	Társaság által a technológiai folyamathoz használt gépjárművekben beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs.
3.5	Létesítményben élőerős őrzést nem alkalmaznak, a biztonságtechnikai rendszerek üzemeltetése a munkavállalók feladata.
3.6	Létesítményben élőerős biztonsági szolgálat működik, de járőrözés nincs, vagy nem megfelelően van szervezve.
3.7	Létesítménybe történő be- és kiléptetés nem, vagy nem megfelelően szabályozott, a rezsimintézkedéseket nem, vagy nem teljes körűen hajtják végre.
3.8	Létesítmény fizikai védelmi rendszerében a mélységi védelem kaialkítása nincs, vagy nem megfelelő.
3.9	Létesítmény fizikai védelmi rendszerében biztonsági zónák, területek nincsenek, vagy nem megfelelően vannak meghatározva.
3.10	Létesítmény közvetlen környezet nem átlátható, nem gondozott, a telekhatárok, külterületi objektumok rejtve megközelíthetőek.

9. táblázat: A létesítmény környezetéből adódó lehetséges veszélyek.

Tétel	Veszélyek megnevezése
4	**Emberi munkavégzésből adódó biztonsági veszélyek**
4.1	Az IT/ICT hálózat üzemeltetői a biztonságtechnikai hálózat üzemeltetői is egyben (fizikailag azonos hálózat)
4.2	A biztonságtechnikai rendszerek felügyeletét szakmailag nem kompetens munkavállalóval látja el társaság
4.3	Szabályzatokban rögzített folyamatok betartatása nem konzekvens.
4.4	Biztonságtechnikai rendszerek karbantartását és javítását végző társaság munkavállalói munkavégzésének színvonala nem megfelelő
4.5	Társaság biztonságtudatossági szintje nem ismert, vagy igen alacsony.
4.6	A rezsimintézkedések nincsenek, vagy azok betartatása nem megfelelő részletességgel kidolgozottak.
4.7	Biztonsági őrök tevékenységének ellenőrzöttsége, a munkavégzés szinvonala nem megfelelő.
4.8	Meglévő fizikai védelmi rendszerek használtata nem napi rutin a társaság életében.
4.9	Biztonsági rendszerek esemény- és hibaüzeneteire a társaság nem időben reagál.
4.10	Biztonsági terület munkatársai képzése, továbbképzése nem megoldott.

10. táblázat: A létesítményben dolgozók munkájából adódó lehetséges veszélyek.

A kialakított – négy témakör köré csoportosított – lehetséges biztonsági kockázatok egy-egy egységes csoportot alkotnak, amelyek tehát így a „Veszélyfelhőt” képezik. Az egyes csoportokat úgy választottam meg, hogy azok valóban egy tematikus csoportosítást biztosítsanak, ugyanakkor lefedjék az egyes létesítmények tevékenységének alapvető részleteit.

Fontos szempont volt a csoportosítás megalkotása során egy olyan rendszer kialakítása, amely a kockázatértékeléseket követően számtani átlagszámítással az adott csoportba tartozó biztonsági kockázatok átlagértékét megmutassák.[38]

[38] Az egyes kockázatok értékelése az adott létesítmény fizikai védelmében a releváns veszélyek meghatározásával kezdődik, majd azok kockázatai minősítésével folytatódik.

4.6. Elemi események bekövetkezésének esélyei, annak hatása[39]

Második lépésben önkényesen felvettem egy, a bekövetkezés esélyére utaló rangsort. Ezután egy másik listát készítettem, amely megmutatja az esetlegesen bekövetkezett elemi esemény hatását a vizsgált létesítményre vonatkozóan. A biztonsági szakterületen eltöltött néhány évtizedes gyakorlatom azt mutatja, hogy egy ötös terjedelmű skála elegendő az esetlegesen bekövetkezett elemi események kockázatértékelésének figyelembevételekor. Ezen skálán kerül meghatározásra a bekövetkezés esélyei rangsor és a bekövetkezés hatásának jellemzése.[40]

Érték	Elemi esemény bekövetkezésnek esélye
1	Nagyon kevés eséllyel következik be
2	Kevés eséllyel következik be
3	Közepes eséllyel következik be
4	Nagy eséllyel bekövetkezik
5	Csaknem biztosan/Biztosan bekövetkezik

Érték	A veszély hatása
1	Alacsony, közel jelentéktelen
2	Kimutatható, de nem számottevő
3	Közepes
4	Jelentős
5	Nagyon súlyos, katasztrófális

11. táblázat: Bekövetkezési esély és hatás táblázat.

4.4.1 A veszély bekövetkezésének esélye

A veszély bekövetkezési bekövetkezés esélyének meghatározásakor az esetlegesen bekövetkező elemi események önálló értékeléséből indulok ki. Ezeket az adott létesítmény biztonsági auditálása során interjúkkal, az adott társaság működési történetének historikus adataival egészítem ki. Általánosságban kijelenthetem azonban, hogy a fizikai védelmi rendszerrel kapcsolatos biztonsági kockázatok tekintetében rendkívül ritka, sőt gyakorlatilag nincsenek historikus adatok. Ennek következtében a klasszikus matematikai valószínűség számítás ezen a szakterületen nem végezhető el. Ez a tény megnehezíti a Veszélyfelhőben meghatározott elemi események bekövetkezési valószínűségének meghatározását. Éppen ezért nem valószínűségről, hanem bekövetkezési esélyről, vagy lehetőségről célszerű beszélni. A kockázatértékelések bizonyos területén, ahol a történeti adatok – még soha nem következett be, de előfordulhat - nem

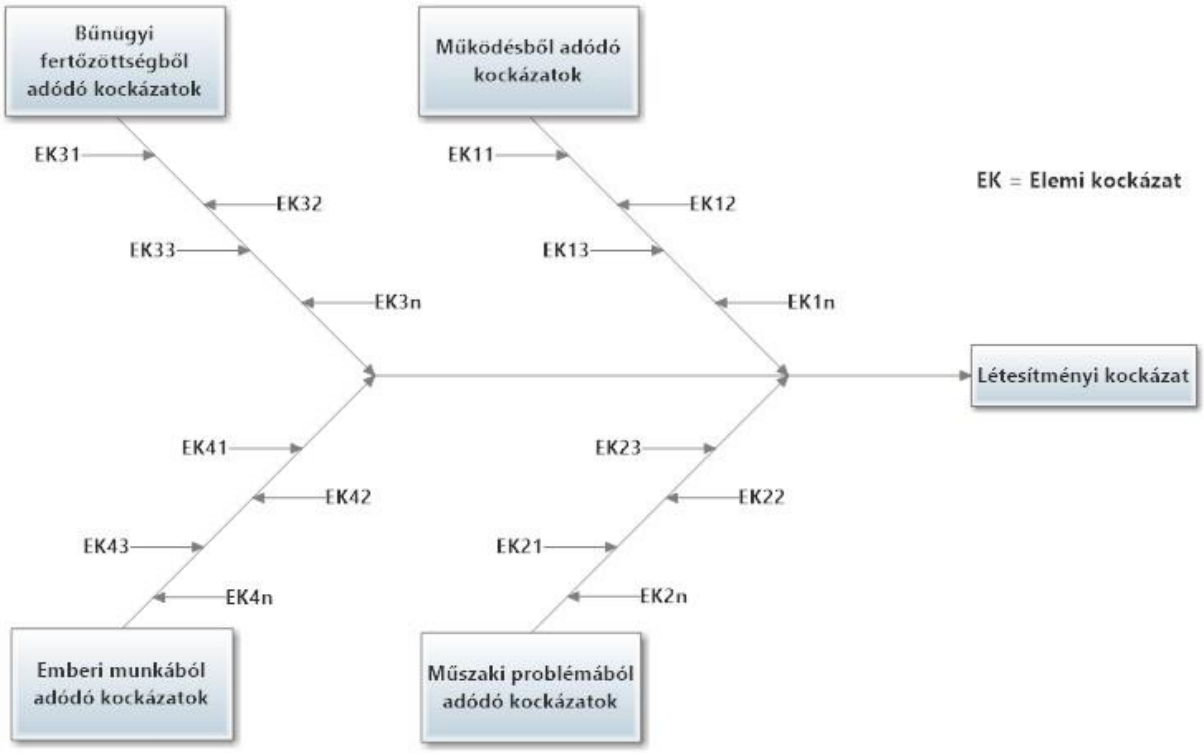
[39] Dr. Takács Szabolcs (Anima Group) saját interjú; 2016. március hónapban, több alkalommal

[40] Az adott esemény bekövetkezésnek lehetőségét meghatározó mátrix esetében a valószínűtlen (0 értékű) bekövetkezést nem jelöltem, tekintettel arra, hogy a „Veszélyfelhőt" kizárólag olyan elemi eseményekből alakítottam ki, amelyek bekövetkezésének van esélye.

állnak, vagy nem állhatnak rendelkezésre, gyakori módszer az elemi események bekövetkezésének lehetőségéről, esélyéről beszélni, mivel a klasszikus valószínűség nem számítható.

Amennyiben olyan elemi eseményeket kell figyelembe vennünk, amelyekről historikus adataink nincsenek, és a matematikában jól ismert valószínűség számítására nincs lehetőség, akkor az adott elemi események tekintetében különböző szakértőket, szakértő csoportot kell igénybe venni és közösen meg kell állapítani az adott elemi esemény bekövetkezésnek esélyét és annak a hatását, akár a fizikai védelmi rendszer tekintetében a gazdasági következményeit is. **[17]**

Áttekintve a kockázatértékelési módszereket, lehetőségeket, valamint a rendelkezésre álló biztonsági kockázatokat, elsősorban a „Veszélyfelhő" elemi eseményeinek értékeléséhez a halszálka diagram (Ishikawa[41] diagram) megfelelő módszer. Szakértői csoport támogatásával az egyes ok-hatás kapcsolatok részletekbe menő feltárásával egzakt módon meghatározható a létesítményi kockázat pontos mértéke.



8. ábra: Ok-okozati diagram a " Veszélyfelhő" feldolgozásnak folyamatában.

[41] Kaoru Ishikawa (1915 -1989) a japán University of Tokyo tanára, aki az 1960-as években publikálta az önmagáról elnevezett diagramot az ipari folyamatok minőségbiztosításának támogatására.

Az ok-okozati összefüggések vizsgálatának egyik legelterjedtebb előforduló módszere a hazánkban is alkalmazott SOL elemzés[42], amely rendkívül részletes analízist biztosít az egyes biztonsági okok és azok következményei (okozat) pontos meghatározásához. **[20]**

4.4.1 A veszély hatása

Az esetlegesen bekövetkezett elemi esemény – amelynek a bekövetkezési bekövetkezés esélyét előzőleg meghatároztam – hatását az adott létesítményre nézve is meghatározom. Ebben a biztonsági kockázatértékelési rendszerben nincs szükség tényleges értékek meghatározására, mert egyfelől nehéz lenne egy szakszerű, korrekt, gazdaságilag is kimutatható értéket meghatározni, másfelől az általam felvett öttényezős rendszerbe minden elemi esemény szakértői munkával jól besorolható. Annak érdekében, hogy a kárhatás nagyságát pénzügyi szempontból is értékelni tudjuk, az elemi kockázatok értékelésnek folyamatában a sávos skála használatát vezetem be. Tekintettel arra, hogy ez egy módszertan, ezért az adott létesítmény esetén a sávok, sávhatárok tetszőlegesen (szakértők bevonásával) módosíthatók.

4.4.2 Kockázatértékelés

A kockázatértékelés folyamatában tovább lépve meghatározzuk a kockázati események két paraméterét, a besorolni kívánt létesítmény esetében releváns veszélyeket kiválasztva a korábban rögzített – szükség esetén testreszabott és aktualizált – Veszélyfelhőből. A kockázatértékelés során az elemi esemény bekövetkezésének esélyét tekintve ún. ordinális skálát[43] alkalmazok, ugyanis nem határozhatóak meg az egyes bekövetkezési esélyek közötti különbségek. A hatást tekintve azonban sávos skálát használok, hogy a következmények pénzügyi vetületei is jelölhetőek legyenek, miközben a pontos költségek nem határozhatóak meg. [21]

Az energia szektor esetében a létesítmények fizikai védelmi rendszere ezekben a megadott sávokban mozog. Minden más esetben a bevont szakértők ismeretei, tapasztalatai alapján kell meghatározni a felhasználandó sávokat.

---

[42] SOL: Safety through Organizational Learning
[43] http://ramet.elte.hu/~kún.adam/oktatas/biometria8.pdf (letöltve: 2017. július 1.)

ÉRTÉKELŐ MÁTRIX (releváns veszély megnevezése)			KÖVETKEZMÉNY HATÁSA				
			Alacsony, közel jelentéktelen	Kimutatható, de nem számottevő	Közepes	Jelentős	Nagyon súlyos, katasztrófális
			Éves árbevétel százaléka				
			0,0-1,0	1,1-2,0	2,1-3,0	3,1-4,0	4,1-
			1	2	3	4	5
BEKÖVETKEZÉS ESÉLYE	Nagyon kevés eséllyel következik be	1	1	2	3	4	5
	Kevés eséllyel következik be	2	2	4	6	8	10
	Közepes eséllyel következik be	3	3	6	9	12	15
	Nagy eséllyel bekövetkezik	4	4	8	12	16	20
	Csaknem biztosan/Biztosan bekövetkezik	5	5	10	15	20	25

12. táblázat: Kockázatértékelő alapmátrix.

A létesítmény biztonsági kockázati alapértékét a megjelölt elemi esemény bekövetkezésének esélye és annak a létesítményre gyakorolt hatásának érték-szorzata adja, amely érték az alapmátrixban látható (12. táblázat). Ez az érték valójában egy bekövetkezési eséllyel súlyozott értékként értelmezhető.

Az egyes események bekövetkezésének esélyét, vagy a létesítmény életútja során összegyűjtött történeti adatbázisból, vagy szcenárióelemzéssel tudjuk meghatározni. Az esetlegesen bekövetkező elemi esemény hatását az adott társaságra (létesítményre) vonatkozó történeti adatokból, interjúk készítésével, illetve a kockázatértékelést végző szakértő szaktudása, tapasztalata segítségével tudjuk.

Az esetlegesen bekövetkező esemény biztonsági kockázatának következménye meghatározásához matematikai és szubjektív módszereket is használhatunk. [22]

Az értekezésem fókuszában lévő fizikai védelmi rendszereket érintő kockázatok esetében - tekintettel arra, hogy ezen a szakterületen a historikus események teljes hiánya miatt a különböző matematikai apparátusok bevezetése nem lehetséges - a szubjektív értékelési módszert van lehetőség használni.

A szubjektum által törvényszerűen velejáró helytelen értékítéletek, következtetések csökkentése érdekében szakértői csoport létrehozásával, és csoportszintű következtetések levonásával igen jó pontossággal meghatározhatóak az esetlegesen bekövetkező események hatásai. A következmények, hatások értelmezhetősége érdekében az adott vizsgált létesítmény (vállalat)

éves árbevétele (esetleg költségvetése, amennyiben az árbevétele nem értelmezhető) százalékában célszerű megadni annak érdekében, hogy értelmezhető pénzügyi kockázatokkal is számolni lehessen.

A nem matematikai úton megállapított bekövetkezési esélyek és következmények miatt a károkat sávos skálában célszerű kezelni. Tekintettel arra, hogy a következmény hatását jellemző ordinális skálában használt számjegyek értéke 1-5 között került meghatározásra, így a sávos skála felállításánál is ezt a metódust alkalmaztam annak érdekében, hogy ezen értékelő mátrix további torzításokat ne vihessen a rendszerbe.

Példaként elkészítettem az alábbi, 13. táblázatot, amelyben jól látható, hogy az éves árbevétel esetében a különböző kárhatások nem nulla értékeket jelentenek, főként akkor nem, ha az adott tagvállalat éves eredményével vethetnénk össze. Amennyiben azt feltételezzük, hogy egy gazdasági társaság éves árbevételének képes 5-10 %-t eredményként létrehozni, előállítani (ez általában nem így van, az árbevételekből létrehozható eredmények a gyakorlatban nem tudnak lineárisan növekedni, az eredmény ilyen módon nem számítható, de számunkra a kárhatás pénzügyi nagyságának becsléséhez megfelelő).

%	ÉVES ÁRBEVÉTEL (Mrd Ft)				
	0,1	1	10	100	400
0,1	0,01	0,01	0,10	10,00	4 000,00
1,1	0,11	0,11	1,10	110,00	44 000,00
2,1	0,21	0,21	2,10	210,00	84 000,00
3,1	0,31	0,31	3,10	310,00	124 000,00
4,1	0,41	0,41	4,10	410,00	164 000,00

13. táblázat: Kárhatás táblázat (példa).

A 13. táblázatban példaként megjelölt árbevételekkel számolva jól látható, hogy a fizikai védelmi rendszer biztonsági kockázatai jelentős gazdasági károkat okozhatnak, amely közvetve, vagy közvetlenül a teljes létesítmény számára nehezen kezelhető helyzetet teremthet. Könnyen belátható, hogy egy 100 m Ft árbevétellel (költségvetéssel, amennyiben nem rendelkezik a létesítményben működő intézmény közvetlen bevétellel) rendelkező társaság számára 100 e Ft kárértékkel bíró esemény nem meghatározó (főként, ha egy részét biztosítással is fedezi), de már 4,1 m Ft esetében akár a példaként említett társaság éves eredményét, költségvetési intézmény esetén akár a fejlesztési lehetőségeit is elveszítheti.

A táblázatból jól érthető, hogy egy nem megfelelően tervezett, kiépített és üzemeltetett biztonsági rendszer számottevő gazdasági károkat okozhat csupán azzal, hogy a fizikai védelmi rendszer biztonsági kockázatai közül (Veszélyfelhő) egy-egy elemi esemény bekövetkezik.

4.7. Az adott elemi esemény kockázatának kiszámítása

Egy elemi esemény bekövetkezésének esélye és a bekövetkezett elemi esemény hatásának szorzata a kockázati érték, vagy együttható. Az általam kialakított rendszerben többféle kockázati együtthatót határozunk meg annak érdekében, hogy a számításaink befejezésekor egy adekvát kockázati érték legyen az eredmény.

A vizsgált létesítményre releváns, a veszélyfelhőből kiválasztott elemi események elemi kockázati együtthatóját egy egyszerű szorzattal határozhatjuk meg az „Értékelő mátrix” segítségével.

$$k_e = P_e H_e$$

ahol
k_e: elemi esemény kockázati együtthatója;
P_e: az elemi esemény bekövetkezésének esélye;
H_e: az elemi esemény következményének hatása a létesítményre.

Az egyes elemi események kockázati együtthatója, az egyes kockázati csoportokban számtani átlaggal csoportjellemzővé, csoport kockázati együtthatóvá konvertálható. Ennek az átalakításnak a jelentősége az, hogy ugyanazon veszélycsoportok kockázati együtthatója jelzés arra, hogy az azonos csoportban lévő elemi események biztonsági kockázatának kezelése hasonló módszerekkel, egymást kiegészítő intézkedésekkel biztosítható, ezért az átlag adat meghatározása célszerű.

További indokként elmondható, hogy a kockázatértékelés végeredménye számszerűen meghatározható. Például egy alacsony biztonsági kockázatú létesítményhez szükséges kockázatértéktől eltérhet mindkét irányban (kisebb, vagy nagyobb kockázati értéket vehet fel), amely iránymutató lehet az adott létesítmény biztonsági vezetőjének, vagy tervezőjének a kockázatkezelés szempontjából.

A „Veszélyfelhő” egyes csoportjai elemeinek kockázati értékei átlagának kiszámítása

$$k_{cs} = \sum_{i=1}^{m} \frac{k_{e_i}}{n}$$

összefüggéssel adható meg, ahol

k_{cs}: az elemi események csoportjának kockázati együtthatója;

i:

m:

k_{ei}: az elemi események kockázati együtthatója;

n: az elemi események száma az adott kockázati csoportban.

A „Veszélyfelhő” elemei kockázati értékei átlagának kiszámítása a következő összefüggéssel történik, ahol

$$k = \sum_{i=1}^{m} \frac{k_{csi}}{n}$$

k: a vizsgált létesítmény kockázati együtthatója;

i:

m.

k_{CSi}: az esemény bekövetkezésének bekövetkezés esélyének csoportátlaga;

n: a kockázati csoportok száma.[44]

[44] A fentebb elkészített átlagszámítás mellett, vagy helyett bármely más (a célokat megfelelően alátámasztó) függvény is értelmezhető lehet. Például a maximális értéket meghatározó MAX-, mint legnagyobb elérhető veszélyforrás, vagy a legalább mekkora veszélyekkel kell szembenézni MIN-függvények. A disszertációmban az átlagos, mint az "általában várható veszélynagysággal" számolok annak érdekében, hogy a vizsgált környezet átlagos biztonsági kockázatait bemutassam. A felhasználható különböző matematikai függvények tág teret biztosíthatnak a szakértői csoport számára, hogy a valós biztonsági kockázatok és a vállalati célok közötti összefüggéseket, eseményeket pontosan meghatározzák. Ez a tény az általam kidolgozott módszer univerzalitását erősíti.

4.8. A létesítmények biztonsági kockázatát jellemző szám értelmezése és a kockázatértékelés folyamata

Felhasználva a kockázati mátrixokat a maximum és a minimum értéke 25, illetve 1.

A folyamat során meghatározott, az adott létesítmény aktuális biztonsági kockázatairól készített pillanatfelvételből kiszámított biztonsági kockázati értéket jelző szám mutatja meg, hogy a vizsgált létesítmény biztonsági helyzete, a létesítmény biztonsági kockázatok kezelésére való felkészültsége jelenleg milyen szintű.

Az elemi események kockázatértékelési mátrixának kialakítása során azért alkalmaztam a Létesítményi együtthatóhoz hasonló kialakítású mátrixot, mert így az adott létesítményre megadott „Veszélyfelhőben" szereplő elemi események kockázati értékének számtani átlaga a Létesítményi együtthatóval összevethető, az közvetlenül beilleszthető a Létesítményi mátrix segítségével elkészített létesítmények kockázati besorolásába, azaz a meglévő és kockázatértékelt fizikai védelmi rendszer megfelelősége, vagy meg nem felelősége megállapítható.

Példaként tekintsük a következőt: a Létesítményi mátrix alkalmazásával megállapítottuk az adott létesítmény Létesítményi együtthatóját, amely 12.

Ennek az értéknek alapján a biztonsági kockázati besorolás: MBKL (lásd: 6. táblázat!)

A „Veszélyfelhőben" rögzített elemi események bekövetkezési esélye és a kárhatás táblázat alkalmazásával elemezzük az összes elemi eseményt és meghatározzuk a teljes elemi eseménysor („Veszélyfelhő") számtani átlagát (4·10 esemény). Tekintettel arra, hogy minden elemi esemény kockázati értéke maximálisan 25-ös értéket vehet fel (a mátrix 5·5 formában került kialakításra), így az átlaguk is maximálisan 25 lehet (Létesítményi együttható meghatározásakor használt 5·5-ös mátrixhoz hasonlóan). Ennek következtében az adott létesítmény biztonsági kockázatait tartalmazó „Veszélyfelhő" számtani átlaga és a Létesítményi együtthatója összehasonlításával eldönthető, hogy az adott létesítmény fizikai védelmi rendszere a biztonsági kockázati besorolásnak megfelel, vagy nem felel meg (azaz a fizikai védelmi rendszerét fejleszteni szükséges-e).

Folytatva az előzőeket, ha a Létesítményi együttható 12, azaz Magas Biztonsági Kockázatú Létesítmény (MBKL) és ha a „Veszélyfelhő" átlaga 8, akkor a kiépített fizikai védelmi rendszer összességében megfelel a létesítmény biztonsági kockázatainak, azaz jelentősebb fejlesztésekre biztosan nincs szükség.

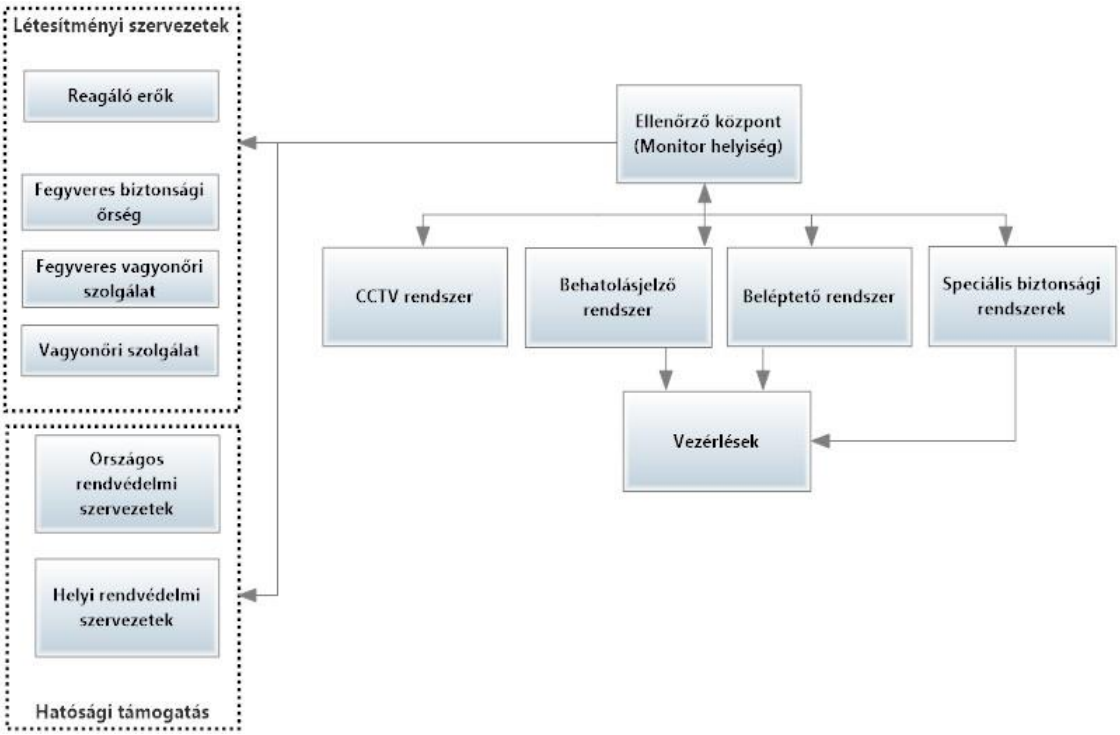
A fizikai védelmi rendszer megfelelőségének a részleteiről ad információt a négyes csoportba rendezett elemi események sorozata, ahol már a csoportátlag elképzelhető, hogy nem illeszkedik a MBKL 5-12 sávjába. Ennek megfelelően a megrendelő közvetlenül adatokat kap arra vonatkozóan, hogy fizikai védelmi rendszerének mely részét, elemeit kell magasabb védelmi szintre fejleszteni, illetve mely elemeit lehetséges esetlegesen lekapcsolni (leszerelni).

A kockázati értéknek, a kockázatok kezelésének folyamata során – amelybe beletartozik, az értekezésem témáját adó videó megfigyelő rendszer is – ennek az értéknek az egyhez, mint határértékhez kellene közelednie, amely azt jelentené ebben a szélsőértékben –, hogy az adott létesítmény/intézmény biztonsági kockázatai valamennyi biztonsági területen megfelelnek az előírásoknak (tökéletes biztonság, de ennek a megvalósítása lehetetlen).[45]

Disszertációm 2.1.2. fejezete a meghiúsítási tervezési stratégiával foglalkozik, amely hazánkban nem elterjedt tervezési elv annak ellenére, hogy a végeredményt tekintve – az esetleges elkövető nem képes a terve megvalósítására – hatékonyabb megoldás. Erre a következtetésre több irányból el lehet jutni. Az egyik ilyen teória, hogy a meglepetés (a reagáló erő képessége, pillanatnyi elhelyezkedése, taktikai lehetőségei, stb., 9. ábra) rendkívül nehezen felmérhető, így arra az esetleges elkövető nem lesz képes megfelelően felkészülni.

Természetesen a folyamatos magas költségszint miatt ez a tervezési stratégia csak a megfelelő, a legmagasabb biztonsági kockázatok esetén reális alternatíva.

[45] A maximális 25-ös érték - hasonlóan a kockázatértékelés minimumához - a valóságban értelmezhetetlen, mert ebben az esetben a létesítmény/intézmény úgy került megépítésre, hogy a biztonsági által jelzett elemi események bekövetkezte biztos és hatása a létesítményre nézve magas (katasztrofális). Ez nem azt jelenti, hogy biztonsági szempontból semmilyen védelem nincs (sem zár, sem kerítés, sem beépített biztonságtechnika, sem őrzés, így a biztonsági kockázatok kezelése alapszinten sem megoldott), hanem azt, hogy egy esetlegesen bekövetkező kiemelkedő veszélyű esemény hatása drámai lehet, amely ellen a védelmet ki kell alakítani.



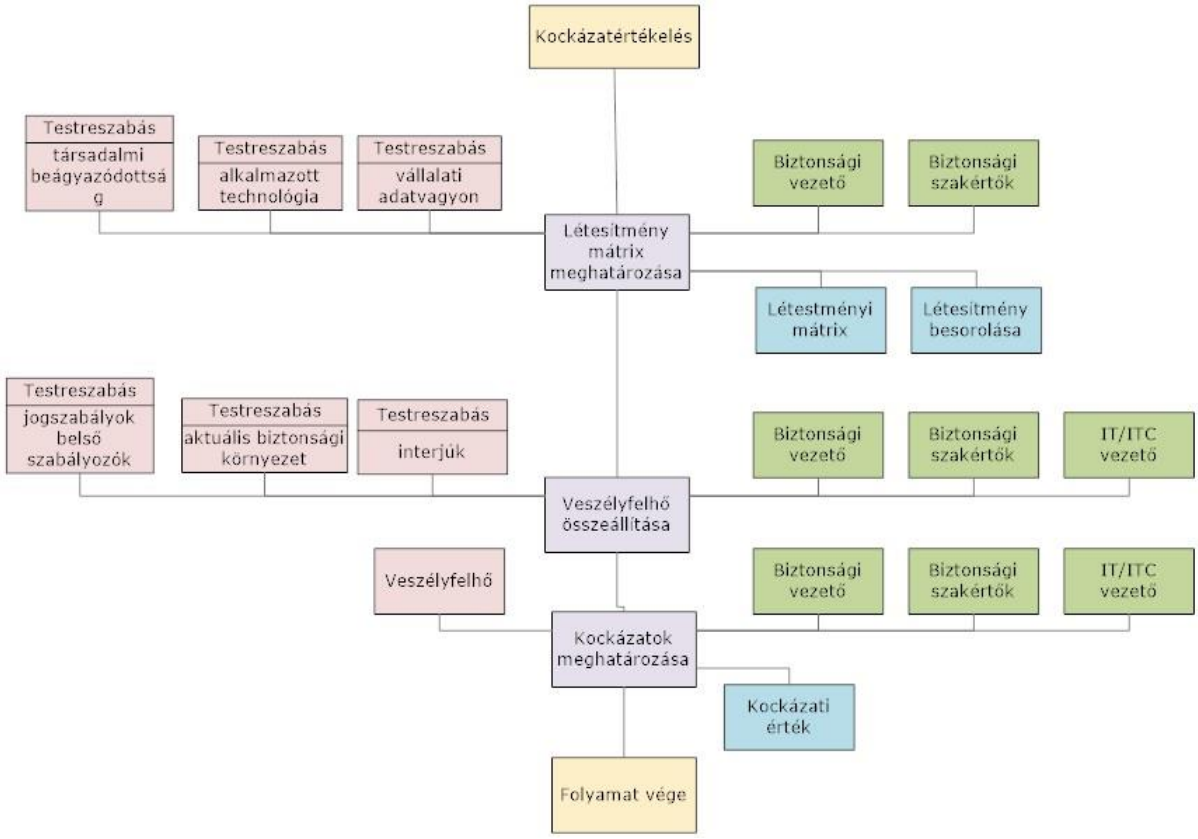
9. ábra: A meghiúsítás tervezési stratégia megvalósítása esetén az élőerő alkalmazásának szükségessége.

A Létesítményi mátrix felhasználásával elvégzett biztonsági osztályba sorolást követően láthatóvá válnak azok a biztonsági kockázatok, melyek kezelése, a kockázatok csökkentése céljából elengedhetetlenek.

Egy gazdasági társaság, vagy egy intézmény életében döntő szerepe lehet a tevékenységét, illetve magát a létét befolyásoló kockázatok teljes körű, komplex értékelésének (10. ábra). Ennek köszönhetően a kockázatkezelés (risk management) a hétköznapokban önálló területként jelenik meg egy társaság életében, amely tevékenység interdiszciplináris feladatnak tekinthető. Önálló, e szakterületet felügyelő pozíció is kialakult („risk manager")[46], aki támogatja a gazdasági társaságok felső vezetőinek munkáját.

A biztonsági kockázatok tekintetében némileg bonyolultabb a helyzet. A kockázatok többségében ugyanis olyan eseményeket kell értékelni, amelyekre nincsenek az adott létesítményben archivált adatok, a biztonsági kockázatokat befolyásoló környezet rendkívül dinamikusan változhat, ráadásul a szakterületen belül önállóan is érvényes a multidiszciplinaritás.

[46] A Risk manager olyan, speciálisan a kockázatkezelés területén kiemelkedő ismeretekkel rendelkező szakértő, aki egy vállalat, intézmény kockázatkezelését szervezi, koordinálja, elemzéseivel, javaslataival támogatja a felső vezetés munkáját.



10. ábra: Kockázatértékelési részletes folyamatábra.

Az értekezésem mellékletében megtalálható táblázatokban, - amelyekben kizárólag a biztonsági kockázatokkal foglalkozom -, az egyes létesítményekkel kapcsolatos számítások is ellenőrizhetők.

Ezzel az általam kidolgozott módszerrel teljesen analóg módon létrehozható egy, a kereskedelmi létesítményeknél is alkalmazható ún. Létesítményi mátrix. Ennek segítségével meghatározott környezetben - jogszabályi előírások, létszám-, és területi adatok – lehet a kockázati mátrixot felállítani annak érdekében, hogy az ilyen típusú létesítményekkel kapcsolatos biztonsági kockázatok – egy aktuálisan összeállított „Veszélyfelhő” mellett – kiszámíthatók, értékelhetők legyenek.

Természetesen minden kockázatértékelés célja a kockázatok csökkentése, a fennmaradó kockázatok kezeléséhez szükséges intézkedések kidolgozása és végrehajtása. Jelen disszertációm középpontjában a biztonsági kockázatértékelésekből adódó veszélyek fizikai védelmi rendszerekkel történő kezelése áll.

4.9. A fejezet összegzése – következtetések

Egy létesítmény biztonsági kockázatainak kezelése egy sok szabadságfokú függvényként is értelmezhető, melyet jellemez a létesítmény társadalmi beágyazottsága (milyen mélyen, sokrétűen vesz részt környezete gazdasági életében). Sajátossága továbbá a létesítményben alkalmazott technológia, az adatvagyon szenzitivitása és az a „Veszélyfelhő", amelyben az adott létesítmény a tevékenyégét folytatja. Minden egyes kérdésre önálló választ kell adni, de a biztonsági kockázatok kezelését biztosító rendszerbe illeszthetőnek kell lennie.

A disszertációmban foglalkoznom kell az ún. létfontosságú létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. CLXVI. törvénnyel (Ltv.), hiszen az, a fizikai védelmi környezetet alapvetően meghatározó Üzemeltetési Biztonsági Terv feltételrendszerének összeállítására is előírásokat fogalmaz meg. Az általam vizsgált létesítmények jelenleg ugyan nem tartoznak e jogszabály hatálya alá, de az ott leírt feltételek alkalmazása egyáltalán nem mond ellent az általam kidolgozott rendszerkövetelményeknek, ráadásul más létesítmények esetén is lehetnek létfontosságúnak minősített infrastruktúrák, rendszerelemek.

A létfontosságú rendszerekkel kapcsolatos feladatok tekintetében az Országos Katasztrófavédelmi Főigazgatóság (OKF) kiemelkedő szerepet játszik. A katasztrófavédelem szervei az uniós és a nemzeti azonosítási, kijelölési eljárás során szakhatóságként, nyilvántartó és javaslattevő hatóságként, felügyeleti, ellenőrzési, koordinációs, valamint nemzeti kapcsolattartó és hálózatbiztonsági elemző-értékelő feladatokat látnak el.

A „Veszélyfelhő" összeállítása minden esetben a biztonsági kockázatokat elemző, értékelő szakértők feladata. Az általam megadott kockázati csoportokba történő besorolás e döntést nagyban segíti. Az egyes létesítmények/intézmények biztonsági kockázati besorolását adó kockázati értékek, amely kiszámítása a „Veszélyfelhőben" meghatározott négy csoportba sorolt kockázatok értékeléséből számítható, releváns irányt mutathatnak az adott létesítmény/intézmény védelmi rendszereinek fejlesztéséhez.

A kockázatértékelés tekintetében meg kell jegyezni, hogy ez a feladat, folyamat nem csak egyszer elvégzendő munka. Ez egy folytonos frissítést kívánó dokumentum, amellyel követni szükséges az adott létesítményben működő társaság tevékenységi körében beállt változásokat.

5. A SZÁMÍTÁSOKBÓL ADÓDÓ KÖVETKEZTETÉSEK

Ebben a fejezetben példákkal mutatom be az általam létrehozott rendszer használhatóságát oly módon, hogy az egyes biztonsági kockázati kategóriába sorolt létesítmények esetében részletesen taglalom a védelmi igényeket, a számítások eredményeit és az azokból levonható következtetéseket.

5.1. Litér Gázturbinás Tartalék Erőmű (L=12; MBKL[47]) és Sajószöged Tartalék Gázturbinás Erőmű (L=12; MBKL)

1. diagram: Litér Gázturbinás Tartalék Erőmű főbb biztonsági kockázatai.

[47] Létesítményi együttható L=12; MBKL: Magas Biztonsági Kockázatú Létesítmény

2. diagram: Sajószöged Gázturbinás Tartalék Erőmű főbb biztonsági kockázatai.

A Litér Gázturbinás Tartalék Erőmű és Sajószöged Gázturbinás Tartalék Erőmű főbb biztonsági kockázatainak értékeléséből – melyet valós adatok alapján állítottam össze – készített grafikonok világosan mutatják azokat a kockázatokat, amelyek kezelése jelenleg a legfontosabb. A környezet bűnügyi fertőzöttsége – mely átlagosnak tekinthető a magyar viszonyok között is – számottevő veszélyeket generál, amelyek kezelése elsődleges a tulajdonos, illetve a biztonsági szervezet számára. Az erőművek elemi biztonsági kockázati értékei és az azokból számított átlag csaknem azonos (1. és 2. diagramok). Ez nem véletlen, hiszen az erőmű kialakítása nagyon hasonló, a létrehozás időszaka is egyező, a létesítmény környezete is közel megegyező – annak ellenére, hogy Litér a Dunántúlon (Veszprém közelében), míg Sajószöged Észak-Kelet Magyarországon található.

A műszaki problémából adódó biztonsági kockázatokat (1. és 2. SZ. MELLÉKLETEK) elsősorban a villamos energia kiesése, valamint az ebből adódó világítási problémák okozhatják.

További magas kockázati értékű veszélyek között – a műszaki problémából adódó biztonsági kockázati csoportban – az alábbiakra érdemes figyelni:

- természeti csapásokból adódó akadozó üzemmenet,
- a biztonságtechnikai rendszerek kora meghaladta a 10 évet,
- a létesítményekben veszélyes kategóriájú technológia üzemel.

A létesítmények környezetének bűnügyi fertőzöttségből adódó biztonsági kockázati csoport magas kockázati értékét az alábbiak határozzák meg:

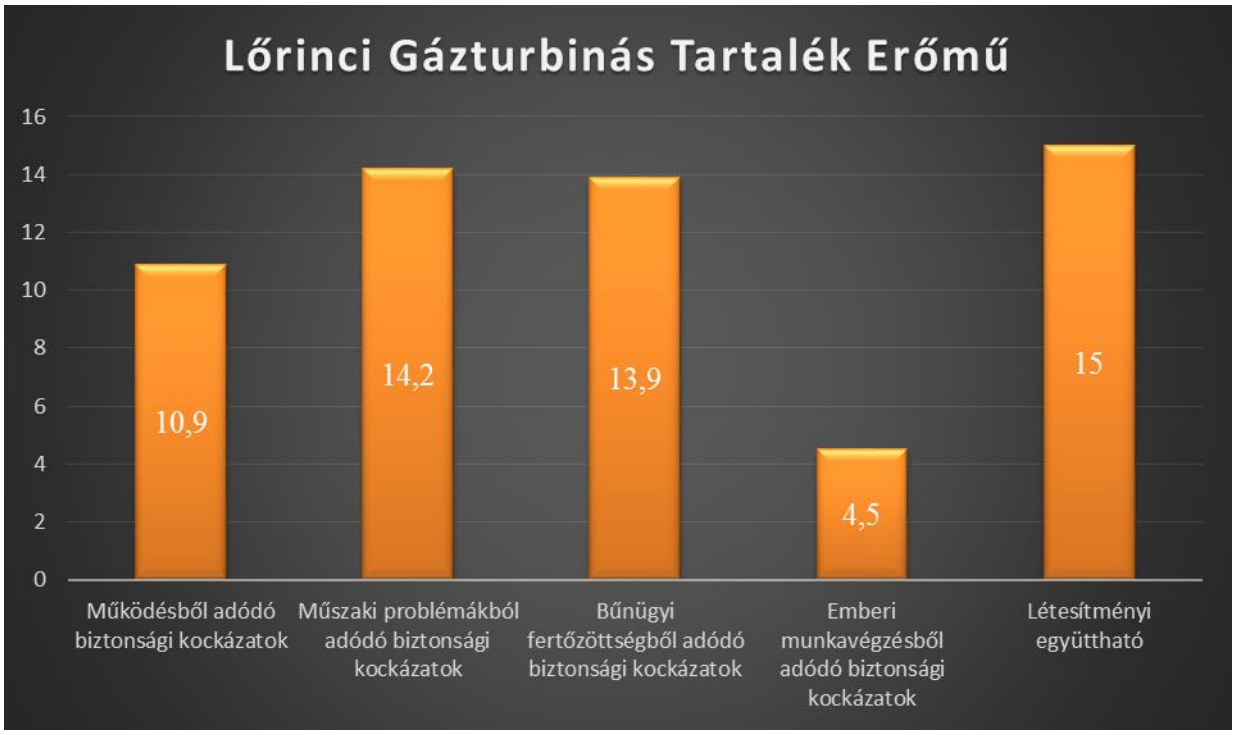
- nincs élőerős őrzés,
- a létesítményekben nincs kialakított mélységi védelem,
- biztonsági zónák nincsenek, vagy helytelenül meghatározottak,
- a létesítmények közvetlen környezete nem átlátható, stb.

Az erőművekben az emberi munkavégzésből származó kockázatok igen alacsony szinten vannak, ami azt jelenti, hogy szakszerű a munkavégzés, a munkavállalók biztonságtudatossága megfelelő (de természetesen még tovább is javítható szinten van).

5.2. Lőrinci Gázturbinás Tartalék Erőmű (L=15; FBKL)

A Lőrinci Gázturbinás Tartalék Erőmű biztonsági kockázatait tekintve (3. SZ. MELLÉKLET): a létesítmény különlegessége a „Black Start Erőmű”[48]jelenlétén alapul, amely egy különösen védendő létesítmény. További különbség az előző két tartalék erőműhöz képest, hogy a Lőrinci erőmű környezete teljesen más. Egy korábban szénalapú erőműnek otthont adó létesítmény egyik épületében került telepítésre. Ennek megfelelően igen nagy a védendő terület. A hűtőtó megléte – amely természetesen a tartalék erőmű működtetéséhez is szükséges, bár megfelelő technológiai megoldással kiváltható lenne – a korábbi erőműnek egyéb létesítményei (szivatytyútelep, távol az alaperőműtől) is vagyonvédelmi szempontból értéket és egyben kockázatot jelent.

[48] A Black Start erőmű egy olyan speciálisan kialakított erőmű egység, amely a környezetétől teljes egészében elzártan is elindítható – az égéshez felhasználandó tüzelőanyag mellett, az égéshez szükséges oxigén is egy zárt konténerben található, amely konténer a teljes „Black Start” erőműnek otthont ad. Az erőmű feladata egy teljes magyarországi villamos hálózati leállást követően a magyar villamos energiatermelő hálózat újraindítása.

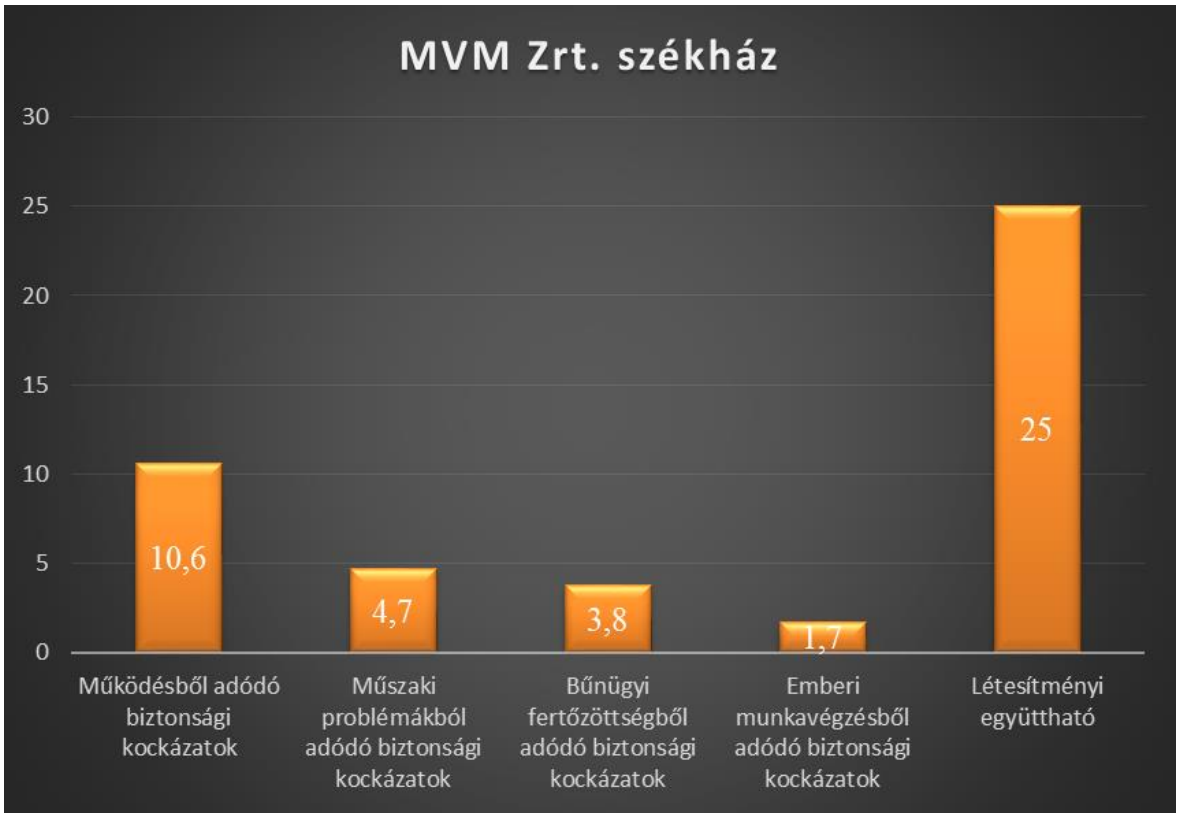


3. diagram: Lőrinci tartalék erőmű főbb biztonsági kockázatai.

Az emberi munkavégzésből adódó biztonsági kockázatok értéke azért lett magasabb az előző két erőműhöz viszonyítva, mert a létesítmény maga is magasabb biztonsági kockázatú kategóriába került besorolásra - éppen a „Black Start" erőmű fokozott biztonsági kockázata miatt (3. diagram).

Fontos megjegyezni, hogy mindhárom erőmű azonos társaság irányítása alatt működik, így az emberi munkavégzésből adódó biztonsági kockázatok érthető módon azonosak, miközben egyéb veszélyek, azok kezelése is igen szervezett, koherens módon történik. Az alapvető problémát mindhárom erőmű esetében a biztonsági rendszerek műszaki elavulása okozza, amelyet természetesen nem képes kompenzálni a gondos üzemeltetés, a gyakori javítás, a szabályzatok pontos betartása sem.

5.3. Az MVM Zrt. központi irodaháza (L=25; FBKL)

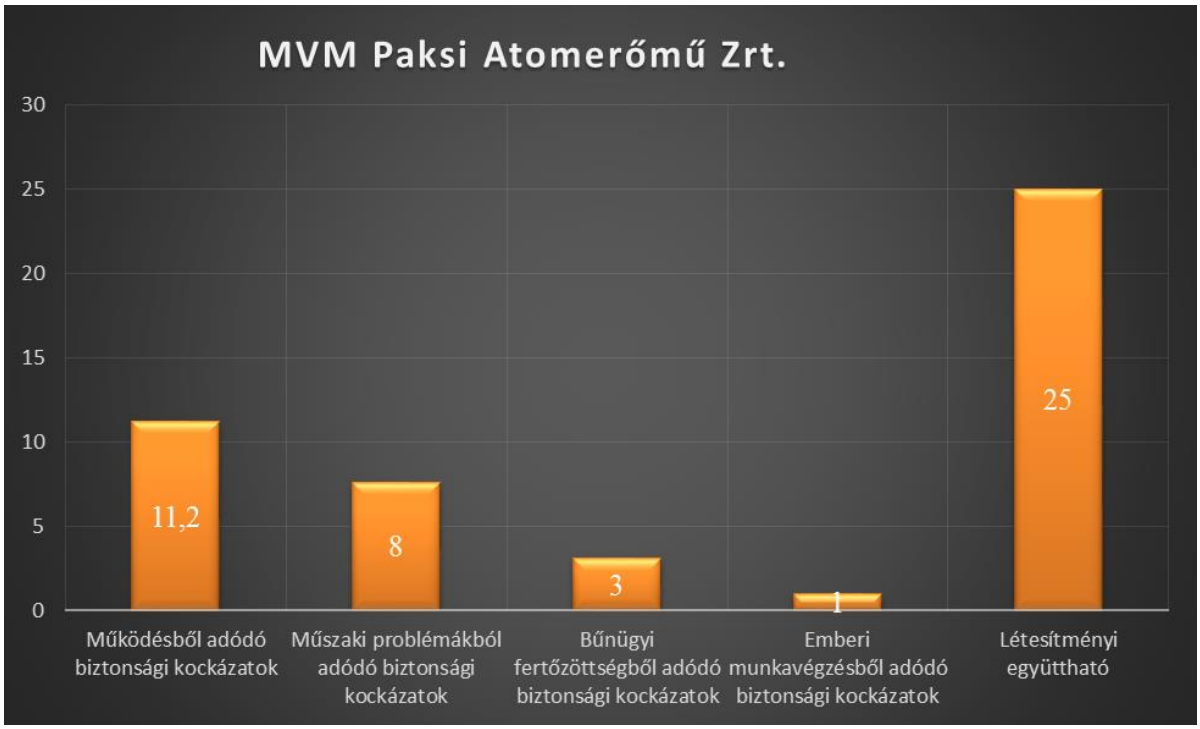


4. diagram: Az MVM Zrt. székházának főbb biztonsági kockázatai.

Az MVM Zrt. székházának biztonsági kockázatait elemezve (4. diagram) szembetűnő, hogy a működésből adódó biztonsági kockázati csoport átlagértéke kiemelkedően magas. Ez annak köszönhető, hogy az MVM Csoport központja, a MAVIR Zrt. is a székházban található, amely Magyarország energiaellátásának biztonsága szempontjából meghatározó. Ezen háttér mellett a létesítményben ügyfélfogadás is működik, a székházban folyó tevékenység közismert a lakosság számára.

Szót érdemel továbbá az a tény is, hogy - a további biztonsági kockázati csoportokat tekintve- a kockázati érték alacsony, miközben a létesítmény a Fokozott Biztonsági Kockázatú Létesítmény besorolást kapta – a Lőrinci tartalék gázturbinás erőműhöz hasonlóan – a létesítményi mátrix számításai alapján. A mellékletben (4. SZ. MELLÉKLET) található részletes számításokból következik, hogy a székház fizikai védelmi rendszerei képesek a biztonsági kockázatok – az MVM Zrt. Biztonsági Igazgatósága által meghatározott – szintű kezelésére, minthogy azok műszaki állapota kifogástalan.

5.4. MVM Paksi Atomerőmű Zrt. (L=25; FBKL)



5. diagram: Atomerőmű biztonsági kockázatai.

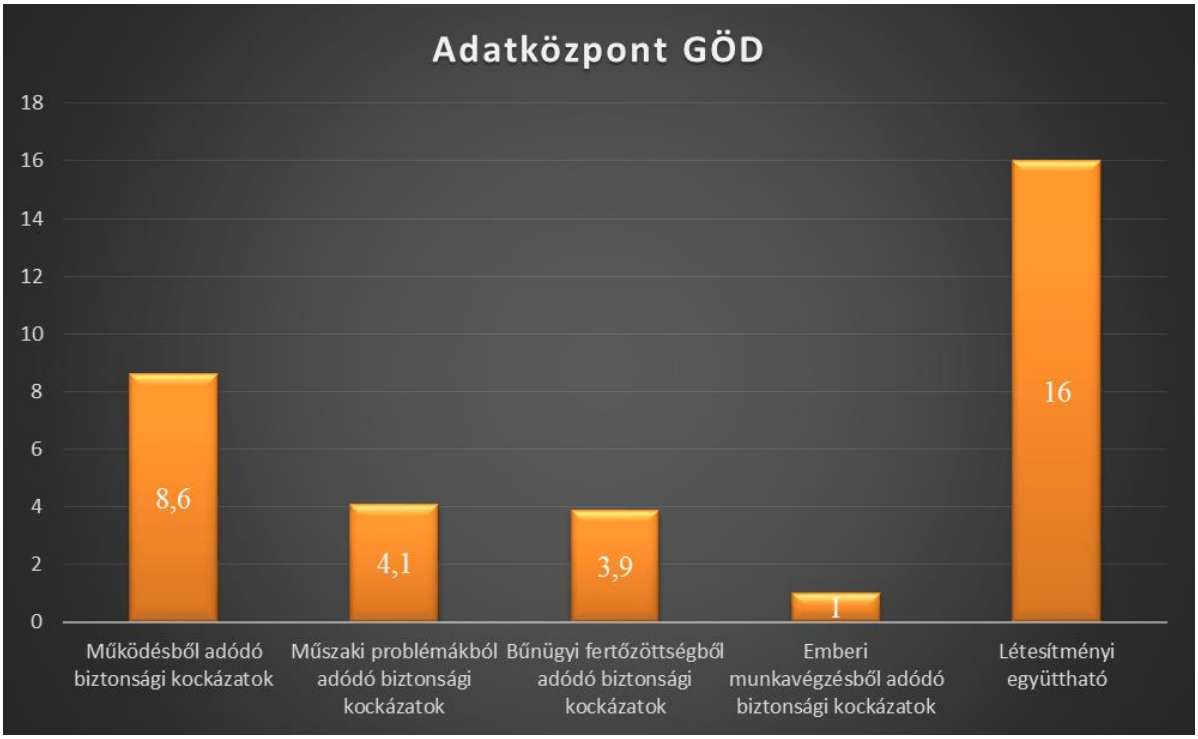
Az MVM Paksi Atomerőmű Zrt. fizikai védelmi rendszerének biztonsági kockázatait értékelve (5. diagram) az eredmény nagyon meggyőző, köszönhetően a létesítmény üzemeltetésében résztvevő munkatársaknak, valamint a vállalat elkötelezett menedzsmentjének a biztonsági kérdések megoldása iránt. A mellékletben (5. SZ. MELLÉKLET) megtalálható részletes értékelési táblázatból látható, hogy a kezelendő biztonsági kockázatokat maga a létesítmény működése adja. A biztonsági szakterület tevékenysége megfelelően kezeli a kihívásokat és a biztonsági kockázatokat. A telepített fizikai védelmi rendszer műszaki állapota példás, annak üzemeltetése kifogástalan.

Az adatgyűjtés során sok éve működő biztonsági kultúra programot ismerhettem meg, mely program eredményének is köszönhető az emberi munkavégzésből adódó biztonsági kockázatok alacsony szintje.

Az MVM Paksi Atomerőmű Zrt. tekintetében fontos kiemelni, hogy a disszertációm által vizsgált fizikai védelmi rendszer valamennyi jellemzője nemzeti minősített adat, azaz a hozzáférés ún. Személyi Biztonsági Tanúsítvány megléte nélkül nem lehetséges, közkeletű elnevezéssel

államtitoknak minősül. Ezen ok miatt, az elemzésem, illetve a disszertációban leírt adatok nem lehetnek elegendően széleskörűek és pontosak.

5.5. Adatközpont Göd – épülő létesítmény (L=16; FBKL)



6. diagram: Az épülő adatközpont biztonsági kockázatai.

A zöldmezős beruházásként kialakításra kerülő adatközpont biztonsági kockázatainak (6. diagram) egy jelentős részét – hasonlatosan az Atomerőműhöz – maga a létesítmény megléte adja. A tervezési folyamatnál a mellékletben (6. SZ. MELLÉKLET) található részletes adatokat érdemes felhasználni, amelyek figyelembe vételével a biztonsági kockázatok kezelhetővé válnak.

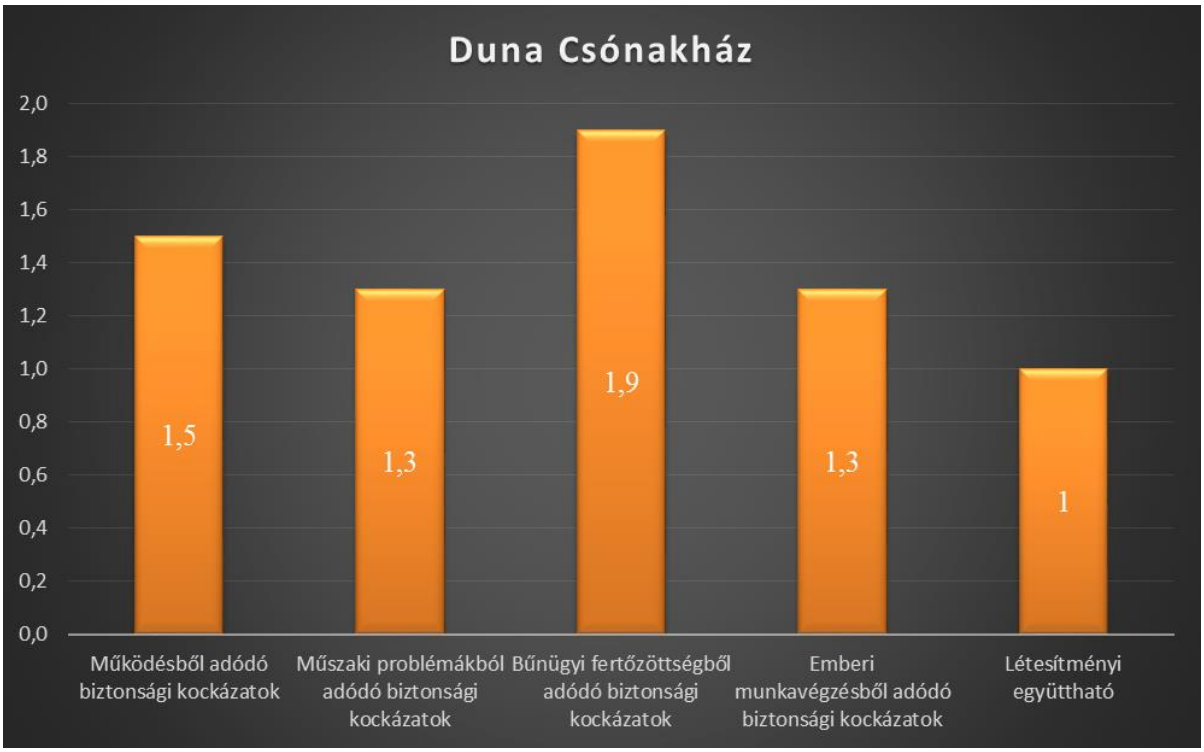
5.6. Szálloda (L=4; KBKL)

7. diagram: Hotel Panoráma biztonsági kockázatai.

A kockázatértékelésben szereplő szálloda az MVM Zrt. tulajdonában lévő balatongyöröki Hotel Panoráma. A szálloda biztonsági kockázatait tekintve az adatok nagyon meggyőzőek (7. diagram), jól jellemzik az általam kialakított kockázatértékelési módszer alkalmazhatóságát olyan körülmények között is, amikor a környezet fizikai védelmet érintő biztonsági kockázatai elenyészőek. A létesítményi mátrix által adott létesítményi együttható 2, mivel az adott szálloda társadalmi szempontból mérhető beágyazódottsága alacsony, miközben a szálloda védendő technológiát nem alkalmaz, védendő adatvagyona a személyi adatokban kimerül. A létesítmény gazdasági adatai nyilvánosak.

Fizikai védelmi rendszere nincs, mert a technológia védelméről nem kell gondoskodni, az alkalmazott rendszer teljesen nyilvános és közismert. A védelmi eszközök a vagyonvédelmet biztosítják, amely kamerákból, valamint a szükséges mennyiségű - a behatolásjelző központjához kapcsolt - érzékelőkből áll, mindezek csatlakoztatva egy távfelügyeleti szolgáltatáshoz.

5.7. Duna Csónakház (L=2; ABKL)



8. diagram: A Duna Csónakház kockázatai.

A MVM Zrt. tulajdonában lévő Duna Csónakház alapvetően oktatási és pihenési feladatokra felkészített épület, vagyonvédelmi szempontból ennek megfelelően kialakított védelmi rendszerrel. Az épületben folyamatos jelenlét nincs, így a biztonságtechnikai rendszer biztosítja a terület védelmét. A 8. diagramból jól látható, hogy a biztonsági kockázati szint alacsony, azonban a biztonsági kockázatok kezelése nem mindenben felel meg a kidolgozott minimális biztonsági követelményeknek (ABKL), a kockázati értékek meghaladják a létesítmény besorolási értékét. A vagyonvédelmi rendszer fejlesztése nem elkerülhető.

5.8. A fejezet összegzése – következtetések

A fejezetben a hat létesítményre elvégzett kockázatértékelésből és annak eredményeiből, illetőleg az itt tárgyalt számításokat összegezve bizonyítom, hogy a biztonsági kockázatok az általam kidolgozott és részletezett módon, világosan és jól érthetően levezethetők. Az értekezésem címében olvasható objektumorientált megfigyelő és ellenőrző rendszerek – tágabban biztonsági rendszerek – a biztonsági kockázatok rendszerében valóban értelmezhetők, és a tervezési, létesítési körülmények jól meghatározhatók.

Saját rendszer-szemléletű számításaim alapján egyértelművé válik, hogy a különböző biztonsági kockázati besorolású létesítményekben milyen elvek alapján szükséges a biztonságtechnikai rendszereket kialakítani.

MEGNEVEZÉS	LITÉR	LŐRINCI	SAJÓSZÖGED	ATOMERŐMŰ	ADATKÖZPONT	SZÁLLODA	SZÉKHÁZ	CSÓNAKHÁZ
Működésből adódó biztonsági kockázatok (átlag)	5	11	12	11	9	1	11	2
Műszaki problémákból adódó biztonsági kockázatok (átlag)	11	14	13	8	4	2	5	1
Bűnügyi fertőzöttségből adódó biztonsági kockázatok (átlag)	14	14	16	3	4	4	4	2
Emberi munkavégzésből adódó biztonsági kockázatok (átlag)	5	5	5	1	1	1	2	1
LÉTESÍTMÉNY KOCKÁZATI ÁTLAG (számított)	9	11	11	6	4	2	5	2
	MBKL	FBKL	MBKL	FBKL	FBKL	KBKL	FBKL	ABKL
LÉTESÍTMÉNYI EGYÜTTHATÓ	12	15	12	25	16	4	25	1
A JELENLEGI FIZIKAI VÉDELMI RENDSZER	MF	MF	MF	MF	MF	MF	MF	NFM

14. táblázat: Kockázatok összehasonlítása.

A 14. táblázat adatait értékelve megállapítható, hogy az egyes létesítmények közül csak a Duna Csónakház vagyonvédelmi rendszerének fejlesztése szükséges, mert a Létesítményi együttható és a kockázatértékelés eredményének összehasonlításából a „Nem Felel Meg – NFM" végeredményre jutunk.

Érdemes megjegyezni továbbá, hogy az egyes létesítmények esetében az egyes kockázati csoportok átlaga is hordoz értékelhető információkat. Az adott létesítmény Létesítményi együtthatójánál magasabb, vagy ahhoz nagyon közeli érték felhívja a megbízó, illetve a tervező figyelmét, hogy az adott biztonsági kockázati eseményekkel kapcsolatosan kiemelt jelentőséget tanúsítson. Az általam kidolgozott módszer ezen tulajdonsága további értéket hordoz, amely jól használható és kihasználható a tervezési és implementálási folyamat során.

Az ebben a fejezetben látható diagramok, az azokat megalapozó számítások jól mutatják, hogy az adott létesítmény védelmi rendszerének milyen specifikus területére kell fokozottan koncentrálni, illetve hol kell a fejlesztéseket elvégezni.

Bizonyos adatok még ebben a körben sem lehetnek publikusak, ugyanis egy atomerőmű fizikai védelmi rendszerére vonatkozó információ-csomag valamennyi eleme nemzeti minősített adat,

így azokról csak általánosságban, konkrétumok nélkül beszélhetünk. A disszertációmban szereplő adatokat, biztonsági kockázatokat a magyar és nemzetközi gyakorlat és szabályozás alapján kutattam és hasznosítottam.

Az elemzett példákban szereplő, az MVM Csoporthoz tartozó létesítmények esetén jól látható annak a többéves erőfeszítésnek az eredménye, amely a biztonsági szakterület következetes tevékenységét mutatja: az emberi tevékenységből adódó kockázatok minden, a példákban szereplő létesítmény esetén alacsonyak. Ezeket az alacsony kockázati értékeket az évek óta tartó biztonságtudatossági program alapozza meg, amely a tudatos biztonsági kultúra program része. Ez a mutató, vagyis a biztonsági kockázati érték alacsony szinten tartása, illetve további csökkentése meghatározó lesz a következő évek munkájában is. Ennek oka az, hogy nemcsak a szűk értelemben vett fizikai védelmi kockázatok és intézkedések rendszerében értelmezhető ez az adat, hanem az információbiztonsági kockázatok környezetében is, amely napjainkban kiemelt jelentőséget és figyelmet kap.

6. A FIZIKAI VÉDELMI KONCEPCIÓK A GYAKORLATBAN

Ebben a fejezetben bemutatom, hogy az általam kidolgozott létesítmény besorolási és a minimális követelményrendszer milyen módon, milyen feltételek mellett kerül felhasználásra

- adatközpont-,
- villamos erőmű-,
- nagyvállalat központi irodaháza-,
- nukleáris erőmű fizikai védelmére.

6.1. Adatközpont

Egy jelenleg tervezési fázisban lévő adatközpont kialakításának fizikai védelmi elveit és feladatait részletezve szemléltetem az objektumorientált, biztonsági rendszerszemléletű folyamatot. Ez a biztonsági fokozatú létesítmény (saját besorolásom szerint Fokozott Biztonsági Kockázatú Létesítmény – FBKL) adatbiztonsági szempontból (TIERIII) is az első lesz Magyarországon.

Az adatközpontokkal szemben támasztott követelmények szerinti TIER besorolást (Uptime Institute – 2012)[49] [23] a 15. táblázaton lehet tanulmányozni.

Tevékenység	TIER I	TIER II	TIER III	TIER IV
Aktív kiszolgálóegységek az ICT eszközök ellátására	**N**	**N+1**	**N+1**	bármely elem hibáját követően is "**N**"
Ellátási útvonal	1	1	1 aktív, 1 tartalék	2 egyidejűleg aktív
Szolgáltatás-kiesés nélkül karbantartható	Nem	Nem	Igen	Igen
Hibatűrő	Nem	Nem	Nem	Igen
Független ellátási útvonalak	Nem	Nem	Nem	Igen
Folyamatos hűtés	Terhelésfüggő	Terhelésfüggő	Terhelésfüggő	Igen
Rendelkezésre állás	99,67%	99,75%	99,98%	99,99%
Éves tervezett leállás és kiesett idő	28,8 óra	22 óra	1,6 óra	0,8 óra

15. táblázat: TIER besorolás. [23]

[49] https://uptimeinstitute.com/tiers

6.1.1 A fizikai védelmi rendszer (FVR[50]) kialakításának alapelvei

Tekintettel arra, hogy az adatközpont átmenetileg tervezési fázisban van, ezért fontosnak tartom, hogy az építészeti kialakításhoz is adjak megbízható támpontot az építésztervező munkatársak számára. Ez a kidolgozott koncepció mintaként szolgálhat más, hasonló létesítmények, azok fizikai védelmi terveinek megalkotásához.

Az adatközpontok fizikai védelmi rendszereinek kialakításához magyar szabványok, előírások ugyan nincsenek, de a „legjobb gyakorlatok" (*Best practices*), a megfelelő kialakítási módok és javaslatok nagy számban megtalálhatók a nemzetközi szakirodalomban[51]. Áttekintve a rendelkezésre álló helyszínrajzot, alaprajzi elrendezéseket, valamint az építészeti metszetek terveit, a kialakítandó adatközpont biztonsági kockázatait, mindezeket a fizikai védelmi koncepció kidolgozásakor figyelembe vettem az esetlegesen elhelyezésre kerülő ICT eszközök védelmi igényei tekintetében. [24]

Építészeti kialakítással kapcsolatos megjegyzések

Minthogy a létesítmény biztonsági kockázatait alapvetően veszélyeztetheti, ezért a létesítményen sehol, semmilyen, a létesítményben folyó munkára, feladatokra utaló felirat, „logo[52]", piktogram nem kerülhet elhelyezésre.

A szerver termekre olyan ablak beépítése nem célszerű, amely közvetlenül az irodákra és a közösségi terekre néz. Amennyiben ez nem elkerülhető, az üvegfelületek alapanyagaként biztonsági, lehetőleg lövedékálló üvegek kerüljenek beépítésre.

A gépkocsi parkolók elhelyezése lehetőleg az épülethomlokzatoktól, vagy magától az épülettől legalább 18 m-re kerüljön. Műszaki adottságnak tekintve a jelenlegi állapotot, a parkoló gépkocsik és az épülethomlokzat közé olyan építészetileg elfogadható akadályok elhelyezése szükséges, amelyek megakadályozzák a homlokzatnak ütközést. A kerítésen kívül ellenőrzött gépkocsik részére (azok visszafordítására is alkalmas) ideiglenes megállóhelyet kell kialakítani (ezzel biztosítva azt, hogy az esetlegesen ellenőrzésre szoruló gépkocsik a létesítmény tervezett és mindennapi üzemét ne tarthassák fel, és az őrszolgálat az ellenőrzési feladatait zavartalanul, kifogástalanul végezhesse).

---

[50] FVR: Fizikai Védelmi Rendszer
[51] https://www.sans.org/reading-room/whitepapers/awareness/data-center-physical-security-checklist-416 (SANS Institute InfoSec Reading Room, Data Center Physical Security Checklist)
[52] A társaság logója, amellyel az adott létesítmény/intézmény azonosítja magát.

Napjainkban további biztonsági kihívást jelent az építészeti tervezés folyamatában, hogy a fal- és tetőszerkezet stabilitását egy esetleges „drón-támadás” ellen is védeni kell.

A létesítményüzemeltetés során a teljes - őrzött és ellenőrzött - területen a növényzet rendszeres ápolását, nyírását el kell végezni annak érdekében, hogy illetéktelen behatolók rejtőzködésére, tevékenységük eltakarására ne tudják azokat felhasználni.

A létesítmény külső határán építendő kerítés külső és belső oldalán legalább 3-3 m szabad, jól áttekinthető sávot kell biztosítani a technikai eszközök megfelelő üzemeltetéséhez, valamint a járőrszolgálat útvonalának biztosításához.

A létesítmény külső határvonalára kerülő kerítésnek legalább 2,5 m magasnak kell lennie az ún. NATO pengés drót telepítésével.

Közvetlenül a létesítmény bejárata mellé őrszolgálati helyiség tervezése szükséges, amely 3 fő részére 7/24 órás tartózkodásra alkalmas és megfelel az előírásoknak (klíma, fűtés stb.).

A tervezett gépjármű útvonalakon biztosítani kell a közeledő gépkocsik garantált sebességcsökkentését (bármely közeledő gépjármű maximálisan 40 km/h sebességgel érkezhet a kerítéskapuhoz). Amennyiben a létesítményhez vezető úton a sebességcsökkentést biztosító nyomvonal nem megvalósítható, akkor a tervezett kerítés előtt 5-10 m távolságban mindkét forgalmi sávban egy-egy speciális, az áthajtást akadályozó távműködésű útakadályt („*Road Blocker*”-t) kell beépíteni.

A fizikai védelmi rendszerek üzemeltetése érdekében az épület bejárata melletti recepciós helyiségben át kell alakítani a monitorszobát, amely így a létesítmény fizikai védelmi rendszerének központjaként képes működni.

Az élőerős őrzés (fegyveres biztonsági őrség) működtetéséhez szükséges öltöző és fegyverszoba kialakítása is. A töltő-ürítő helyet az épületen kívül kell kialakítani.[53]. Elképzelhető az őrszemélyzet részére az esetleges személyátvizsgáláshoz önálló helyiség biztosítása is.

A recepciós térben el kell helyezni egy korpuszban kialakított 4-6 db zárható szekrényt, amelyben a létesítménybe be nem vihető tárgyakat (átvizsgálást követően) az oda érkezők elhelyezhetik.

[53] A töltő-ürítő hely kialakítására lehetőség van épületen, akár gépkocsin belül is – a korszerű lövedékcsapdák ezt lehetővé teszik -, de fegyverszobában tiltott a kiépítés.

A munkatársak részére a helyszínen kell elkészíteni a belépőkártyákat, a biometrikus adatok regisztrációját. Ennek megfelelően egy regisztrációs helyiséget is biztosítani kell a már védett területen belül.

6.1.2 Biztonsági koncepció – a védelem kialakítása

A teljes adatközpontnak otthont adó létesítmény fizikai védelmi rendszerét a mélységi védelmi elvek alapján kell tervezni. A létesítmény területén 4 őrzött védelmi-, míg az adatközpont kerítéssel lehatárolt területén kívül egy ellenőrzött zónát kell létrehozni.

Ellenőrzött *védelmi zóna*:

1. Kerítésen kívüli területek (0. Zóna)

Őrzött védelmi zónák:

1. *Kültéri védelmi* zóna (1. Zóna)
2. Épületvédelmi zóna (2. Zóna)
3. Számítógépterem (-ek) védelmi zóna (3. Zóna)
4. Rack szekrények védelmi zóna (4. Zóna)

Olyan rendszert célszerű tervezni, amely meg tudja akadályozni a bejáratokon keresztül történő erőszakos behatolást, ehhez a biztonságtechnikai eszközök, eszközrendszerek széleskörű felhasználása javasolt [*bollard* (járműblokkoló oszlop), sorompó, stb.].

Az ellenőrzött beléptetés rendjét, mind a technikai, mind a humán erőforrások tekintetében szabályzatban szükséges rögzíteni, ahol részletezni kell a személyek, a gépjárművek és a csomagok be-, és kiszállításának formai és gyakorlati követelményeit.

A létesítménybe, illetve a kialakított őrzött zónákba történő ellenőrzött beléptetést olyan műszaki megoldásokkal érdemes kialakítani, amellyel ellenőrizetlen személyek behatolása, belépése kizárható (anti-passback, tailgating, zsilip, *forgókereszt*, stb.).

A védett létesítmény területén a vendégek kizárólag szakmai, szükség esetén biztonsági őri kísérettel tartózkodhatnak.

A javasolt beléptető rendszer széleskörűen konfigurálható, így a védelmi és üzemeltetési igények messzemenően támogathatók (jogosultsági rendszer, irányfigyelés, kísérőkártyás üzemmód, többes ellenőrzés, stb.).

A létesítmény teljes területén a mozgások kitakarás mentes megfigyelése és archiválása CCTV rendszer segítségével szakszerűen megoldható. A létesítmény területére belépett (és bárhol tartózkodó) személyek felismerését és azonosítását videotechnikai eszközökkel is biztosítani kell.

A videó megfigyelő rendszert úgy kell kialakítani, hogy rendelkezzen az őrszolgálat munkáját támogató videó analitikai lehetőségekkel, ugyanakkor biztosítsa a megfigyelést minden időjárási körülmények között (hőkamerák, megvilágított kerítés, stb.).

A létesítmény valamennyi nyílászárójának állapotáról az őrszolgálatnak tudomása kell, hogy legyen.

6.1.3 Telepítésre tervezett fizikai védelmi rendszerek

Ellenőrzött zóna („0. Zóna")

A létesítmény kerítésén kívül, közvetlenül a kerítés mellett 3 m szélességben egy jól belátható, kitakarásoktól mentes (folyamatos karbantartással rendben tartott), szabad nyomsávot, ellenőrzött zónát kell létre hozni. Ezzel lehet biztosítani a tervezett kerítésvédelmi rendszer (virtuális kerítés: hőkamerákkal és videó analitikával kialakított rendszer) megfelelő működését (a kerítés megközelítése esetén már jelzést küld az őrszolgálat részére), valamint a járőrszolgálat számára annak útvonalát is garantálhatja.

A gépkocsi bejáratoknál videó kaputelefon biztosítja a zárt úszókapuk, illetve a személybejáró felől érkező személyek számára az őrszolgálattal történő kapcsolatfelvételt.

Őrzött zónák

Kültéri védelmi zóna („1. Zóna")

a) Kerítésvédelmi rendszer (hőkamerák, virtuális kerítés videó analitikával) kialakítása.
b) A virtuális kerítés üzemeltetésének kiegészítéséhez ún. kivizsgáló kamerákat (nagy optikai zoom átfogású, látható fénytartományban működő ún. Speed *Dome*[54] kamerákat) telepítünk.
c) Az esetlegesen a létesítmény légterét megközelítő, ott tevékenykedő pilóta nélküli repülőeszközök mozgásának figyelemmel kíséréséhez forgózsámolyos kamerákkal

[54] Speed Dome kamerának hívjuk azokat a távvezérelhető kamerákat, amelyek kifejezetten gyors mozgással képesek a vezérlésekre reagálni. A gyors mozgás leggyakrabban 1 sec alatti körbefordulást jelent.

szükséges felszerelni a CCTV rendszert és a hatóságok közreműködésével kidolgozni az ellenük való védekezés lehetőségét.

d) A létesítmény kerítésén belül, közvetlenül a kerítés mellett 3 m szélességben egy jól belátható, kitakarásoktól mentes, őrzött területet kell létrehozni - ezzel felügyelve a tervezett kerítésvédelmi rendszer (virtuális kerítés: hőkamerákkal és videó analitikával kialakított rendszer) megfelelő működését, valamint a járőrszolgálat számára biztosítva a járőrözési útvonalat.
e) A 3 m széles szabad belső nyomsávban *infrasugaras sorompó*kból kialakított fedővédelmet szükséges kialakítani.
f) A bejáratoknál többsugaras infra-sorompókkal kell biztosítani az elektronikus fedővédelmet.
g) A gépkocsibejárókon át történő erőszakos behatolás megakadályozása érdekében a beléptető rendszerbe integrálva „*bollard*-okat" kell telepíteni. A létesítmény megközelítési útvonalait úgy kell kialakítani, hogy a rossz szándékú behatolók járműveinek sebessége ne léphesse túl a 40-50 km/h-t, illetve a telepítendő mozgó járműblokkoló határsebességét.
h) A gépkocsik teljes körű ellenőrzésére mindkét gépkocsi bejáratnál (teherforgalom számára, illetve a személygépkocsik számára kialakított bejáratok) egy-egy alvázszkennert kell elhelyezni.
i) A gépkocsi bejáratoknál (személy és tehergépkocsi) rendszámfelismerő rendszereket szükséges telepíteni.
j) Az őrszolgálat részére biztosítani kell, hogy hordozható robbanóanyag detektorral - indokolt esetben - ellenőrzéseket tudjanak végezni a belépésre jelentkező gépkocsik, illetve személyek környezetében.

Épületvédelmi zóna („2. Zóna")

a) Az érkezést követően a jogosultsággal rendelkező személyek a recepciós előtérből két forgókereszt segítségével léphetnek az épületbe.
b) A recepciós térben valamennyi üvegfelületet lövedékálló (karabély lőszer ellen védettséget biztosító) anyagból kell készíteni, csakúgy, mint a recepciós iroda falszerkezetét. A recepcióban dolgozó munkatársak védelme és kommunikációs lehetőségének megteremtése érdekében a lövedékálló üvegfalon mozgatható átadófiók és átbeszélő beépítése is szükséges.

c) Az épület irodarészeinek egyes folyosószakaszaira történő belépéshez (igény szerint tovább szegmentálva) motoros forgóvillás és motoros áruszállító kaput kell telepíteni az irodaépületben történő ellenőrzött mozgás biztosítása érdekében (kártyás és PIN kódos beléptetés).
d) Szükség esetén az egyes irodaterületekre történő bejutást kártyás jogosultság-ellenőrzéssel biztosítani kell.
e) A belépési pontokon történő eseményeket egy-egy nagyfelbontású (2 MP) IP kamerával rögzíteni, és a jogszabályban engedélyezett időtartamra archiválni szükséges.
f) A recepciós térben a vendégek vendégkártyát kapnak, amellyel a forgó kereszten keresztül – kísérőkártyás összerendelést követően – tudnak az irodaépületbe bejutni (kísérő munkatárs nélkül – tekintettel a szegmentált, több zónás beléptető rendszerre – a vendégek az irodaépületben nem tudnak mozogni).
g) Minden személynek, aki belépni szándékozik az irodaépületbe (2. Zónába) egy fémkereső kapun keresztül kell mennie. A bevinni szándékozott táskák, csomagok ellenőrzésére egy csomagröntgent is telepíteni kell.

Számítógépterem (termek) védelmi zóna („3. Zóna”)

a) A számítógéptermekbe történő belépési jogosultságot a *belépőkártya* mellett egy biometrikus azonosítóval („érhálózatszkenner”, vagy „kézgeometria azonosító”) ellenőrizni kell. Alapesetben az egyes számítógéptermekbe történő belépést kártyával és PIN kódos tasztatúra segítségével (birtoklás és tudás alapú ellenőrzés) szükséges biztosítani. A biometrikus azonosító terminált a fizikai védelmi rendszer rack szekrényeinek helyet adó teremben kell kiépíteni (más termekhez csak az infrastruktúra kialakítása szükséges).
b) A belépési pontokon történt eseményeket egy-egy nagyfelbontású, személyazonosításra is alkalmas (2 MP) IP kamera rögzítse, a felvételek archiválása a jogszabályban biztosított ideig történjen.
c) A beléptető rendszer a jogosulatlan belépési kísérletekről, az ajtók nem időben történő visszazárásáról az őrszolgálatot automatikusan értesítse.

Rack szekrények védelmi zóna („4. Zóna”)

a) A telepítendő beléptető rendszerbe integrálható, off-line üzemű rack-szekrény zárszerkezeteket kell telepíteni (működését tekintve az egyes belépőkártyákon rögzített

jogosultság felhasználható az adott rack-szekrény nyitásához, amely a beléptető rendszerben teljes körűen kezelésre, archiválásra és „logolásra”[55] kerül).

b) A rack-szekrények illetéktelen nyitását megakadályozandó, biztosítani kell a szekrények kulcsainak biztonságos, logolt tárolását.

6.1.4 Élőerős őrzés

A teljes létesítmény élőerős őrzése Fegyveres Biztonsági Őrökkel (FBŐ) lehetséges. Az FBŐ fenntartásához szükséges valamennyi feltételt önálló jogszabály[56] rögzíti. Az egyes létesítményekben alkalmazandó FBŐ tekintetében a védendő objektumra vonatkozóan az Országos Rendőr-főkapitányság kockázatértékelése és határozata az irányadó.

A teljes létesítmény élőerős őrzésének támogatására egy digitális kommunikációs (kézi rádió adó-vevő) rendszer kiépítése szükséges, amely képes a csoportokban, egymástól teljesen független kommunikációs csoportokat kezelni. Így az őrszolgálaton kívül az objektum menedzsmentje, a karbantartók és egyéb közreműködők is használhatják a kézi adó-vevő hálózatot. A kialakításra tervezett berendezés egy diszpécser központon keresztül a kommunikáció archiválására is képes, miközben az egyes készülékek GPS koordinátákat tudnak továbbítani az őrszolgálat részére. Lényeges az a tulajdonsága is, hogy a 45^{o} –nál nagyobb dőlés esetén riasztásjelzést ad az őrszolgálatnak[57].

A létesítmény területén történő járőrözés ellenőrzése és szakszerű végrehajtása érdekében őrjárat-ellenőrző rendszert szükséges telepíteni, amely szabadtéren képes a járőrök mozgását elektronikusan (GPS koordinátákkal térképen megjelölve) követni.

6.2. Villamos erőmű

Egy villamos erőmű fizikai védelmi rendszere alapjaiban nem tér el egy, a szakemberek számára már közismert biztonsági rendszer kialakításától. A biztonsági kockázatok csökkentése és kezelése érdekében telepített megfigyelő és ellenőrző rendszer és az alkalmazott technológia ellenőrzést biztosító CCTV rendszer aránya jól követi a fizikai védelmi rendszerekkel szemben támasztott követelmények stratégiáját.

---

[55] Logolásnak hívjuk azt a tevékenységet, amelyet informatikai környezetben egy-egy számítógép végez a saját, illetve a vele valamilyen kapcsolatban lévő kijelölt eszközök tevékenységének, működésének rögzítésére.
[56] 1997. évi CLIX. törvény A fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról
[57] ’Man down’ – „Elesett ember” üzemmód/funkció.

A disszertációmhoz készült kutatásaim során elemeztem néhány villamos erőmű (Litér, Lőrinci és Sajószöged Tartalék Gázerőmű) fizikai védelmi rendszerének kialakítását, amelyek még a tervezés időszakában a biztonsági kockázatok figyelembe vételével készültek.

A teljes fizikai védelmi rendszer már nem felel meg napjaink biztonsági kihívásainak, de a tervezés időpontjában (2008) a kialakított rendszerrel szemben támasztott követelményeknek még eleget tettek. Magyarország villamosenergia ellátásának biztonságát közvetlenül sem a terrorizmus, sem az informatikai alapú támadások nem veszélyeztették - a védelmi rendszerek ezen elveknek megfelelően kerültek kialakításra.

Az egyik legnagyobb biztonsági kockázatot a környezet bűnügyi fertőzöttsége jelenti, amely kockázat ma sem elhanyagolható, sőt még növekedés is érzékelhető. A biztonságtechnikai rendszer alapját egy klasszikus értelemben vett, de korlátozott képességekkel, műszaki jellemzőkkel bíró informatikai hálózat képezi, amelyre csatlakoznak a CCTV rendszer kamerái, és a kártyás beléptetés rendszerelemei.

A behatolásjelző rendszer önállóan sziget-üzemben került kiépítésre, de a rendszerek kezelését egy integrált felügyeleti program (G4View[58]) végzi, amely a tervezés és kivitelezés időszakában kiemelkedően korszerűnek számított.

A program kezelését az erőmű vezérlőjében dolgozó (biztonságszakmai szempontból nem minden esetben képzett munkatárs) végzi. Élőerős őrség nincs a létesítményben, az ellenőrzött riasztás-jelzést követően a távfelügyeleti szolgáltató által helyszínre küldött járőr biztosítja a szakszerű intézkedést. Annak érdekében, hogy a munkatársak és a berendezések biztonsága minden időben a biztonsági kockázatoknak megfelelően garantálható legyen, a létesítmény megerősített mechanikai védelemmel rendelkezik. A kerítés, illetve az épületek falai biztosíthatják a járőr kiérkezésig szükséges késleltetést.

A létesítményben, elsősorban a kiemelt biztonsági kockázatú helyiségek és az épület védelmére birtoklás és tudás alapú beléptető rendszert (proximity kártya és *PIN kód tasztatúra*) alkalmaznak. Valamennyi ajtóvezérlőn történő átlépést egy-egy videokamera felügyeli.

Azokat a helyiségeket, amelyekben folyamatosan nincs munkavégzés, a turbina-épület és a kerítéseket behatolásjelző rendszerrel védik. A folyamatos munkarendben dolgozó munkatársak a munkavégzéshez szükséges jogosultságokkal rendelkeznek.

---

[58] G4Wiev integrált felügyeleti program a G4S Zrt. által fejlesztett program, amely lehetőséget teremt különböző biztonságtechnikai rendszerek egységes felületen történő kezelésére.

Az egyik legnagyobb biztonsági kihívás és természetesen kockázat is egyben az egyes leállások esetén végzett karbantartások és javítások időszakában megjelenő, és az erőmű területén munkát végző szakemberek létszáma és ellenőrizhetősége. Ezen többlet biztonsági feladatokat az erőművet üzemeltető társaság biztonsági szervezete, az anyavállalat szakmai támogatása mellett, speciális felkészüléssel, indokolt esetben időszakos élőerős őrzés megszervezésével oldja meg.

6.2.1 A mélységi védelem kialakítása

Az erőmű védelmi rendszerének kidolgozásakor az alábbi mélységi védelem struktúrát kell tervezni és kivitelezni:

Ellenőrzött zóna („0. Zóna")

a) A létesítmény jogi határán futó kerítésen kívüli terület.

Létesítmény osztott területen („1. Zóna")

a) Mechanikai szempontból szilárd, 2,5 m magas kerítés.
b) Behatolásjelző rendszer (*kerítésvédelem*; nyitásérzékelők; infra-sorompók).
c) Kártyás beléptető rendszer (kültéri kártya*olvasó*k).
d) CCTV rendszer (kültéri fix kamerák; *PTZ kamera*).

Központi épület („2. Zóna")

a) Behatolásjelző rendszer (nyitás érzékelők; mozgásérzékelők).
b) Kártyás beléptető rendszer (kültéri kártyaolvasók; PIN kód tasztatúrák).
c) CCTV rendszer (beltéri fix kamerák).

Vezénylő, turbina csarnok („3. Zóna")

a) Behatolásjelző rendszer (nyitás érzékelők; mozgásérzékelők).
b) Kártyás beléptető rendszer (kültéri kártyaolvasók; PIN kód tasztatúrák).
c) CCTV rendszer (beltéri fix kamerák).

6.3. Nagyvállalat központi irodaháza

Egy nagyvállalat központi irodaházának fizikai védelmi rendszere alapjaiban nem tér el egy, a szakemberek számára már közismert biztonsági rendszer kialakításától. A biztonsági kockázatok csökkentése és kezelése érdekében telepített megfigyelő és ellenőrző-, és az alkalmazott technológia ellenőrzését biztosító CCTV rendszer aránya jól követi a fizikai védelmi rendszerekkel szemben támasztott követelmények stratégiáját.[59]

Egy nagyvállalat központi irodaházának fizikai védelmi rendszerének kialakítása minden esetben megfelel azoknak a tervezési elveknek, amelyek a magas (MBKL), vagy fokozott biztonsági kockázatú létesítményekben (FBKL) alkalmazandók.

Tekintettel arra, hogy napjainkban a magyar villamosenergia ellátás biztonságát közvetlenül a terrorizmus, az erőműi informatikai alapú támadások még nem veszélyeztetik, de ezeknek a veszélyeknek a biztonsági kockázatai folyamatosan növekednek, a védelmi rendszereket ezen elveknek megfelelően kell kialakítani.

A biztonsági kockázatok közül eddig nem beszéltem azokról a veszélyekről, amelyek az adott nagyvállalat (például az MVM Zrt.) alaptevékenységében, a piaci riválisok aktív tevékenysége okozhat, azaz a gazdasági hírszerzésről.[60] Ez minden létesítmény esetében szóba jöhet. Valódi biztonsági kockázatot azonban csak olyan társaságok esetén jelent, amelyek legalább országos szinten meghatározóak, tevékenységükkel a versenytársak piaci részesedését veszélyeztethetik.

Egy nagyvállalat központi irodaházának fizikai védelmi rendszerének kialakításnál már előtérbe kerülhetnek speciális szempontok, amelyek magát a létesítményt magas biztonsági kockázatú kategóriába sorolják.

6.3.1 A mélységi védelem kialakítása

Az irodaház védelmi rendszerének kidolgozásakor az alábbi mélységi védelem struktúrát célszerű tervezni és kialakítani:

---

[59] Az irodaház fizikai védelmi rendszerének kiépítésénél nem foglalkozom ebben az értekezésben a tűzvédelmi berendezésekkel (a létesítési engedély része, így annak üzemeltetése is szorosan kapcsolódik a többszintes irodaházi funkcióhoz). Az egyes jelző-, és oltóberendezések adatainak feldolgozását, karbantartását és távfelügyeletét a biztonságtechnikát felügyelő szervezet is végezheti.

[60] A Nemzetbiztonsági Hivatal szerint „az ipari kémkedés olyan tevékenység, amely törvénytelen, a versenytárs végzi a konkurenciával szemben, hogy kifürkéssze annak piaci pozícióját, továbbá erősítse a saját pénzügyi helyzetét, és jelentős költségmegtakarítást végezzen a megszerzett információik alapján.”[25]

Ellenőrzött zóna („0. Zóna”)

a) A létesítmény jogi határán futó kerítésen kívüli terület.

Létesítményi épületen kívüli terület („1. Zóna”)

a) Mechanikai szempontból szilárd, 2,5 m magas kerítés.
b) Behatolásjelző rendszer (nyitásérzékelők; infra-sorompók; kültéri kombinált mozgásérzékelők).
c) Kártyás beléptető rendszer (kültéri kártyaolvasók; rendszámfelismerő rendszer).
d) CCTV rendszer (kültéri fix kamerák; PTZ kamera).

Irodaépület („2. Zóna”)

a) Behatolásjelző rendszer (nyitás érzékelők; kombinált mozgásérzékelők; nedvességérzékelők).
b) Kártyás beléptető rendszer (kártyaolvasók; kártyaolvasók és PIN kód tasztatúrák a rendszerhatárokon).
c) CCTV rendszer (beltéri fix kamerák).

Kiemelten védett területek: szerver termek; irattárak; pénztárak; tárgyalók; irodák („3. Zóna”)

a) Behatolásjelző rendszer (nyitás érzékelők; kombinált mozgásérzékelők).
b) Kártyás beléptető rendszer (kártyaolvasók; PIN kód tasztatúrák).
c) CCTV rendszer (beltéri fix kamerák).
d) Speciális védelem (hangszigetelés; rendszeres RF[61] ellenőrzés).

A fizikai védelmi rendszerek nem önállóan, hanem integráltan egy országos hálózat részeként kerültek kiépítésre, amelyeket egy Központi Diszpécser Szolgálat[62] (KDSZ) 7/24 munkarendben felügyel.

[61] RF – rádiófrekvenciás ellenőrzés: olyan helyiség ellenőrzés, amikor a nem szabványos, ismeretlen kisugárzást adó rádiótechnikai elemeket kutatják fel (az ilyen típusú eszközök beszerzéséhez hatósági engedély is szükséges lehet).

[62] Központi Diszpécser Szolgálat az MVM Csoport biztonsági szolgáltatója (MVM BSZK Zrt.) által kiépített és üzemeltetett szolgálat, ahol 7/24 órás munkarendben szakképzett operátorok végzik az MVM Csoport fizikai védelmi rendszereinek felügyeletét a Paksi Atomerőmű Zrt. kivételével ez a tagvállalat más jogszabályi környezetben működik).

A KDSZ operátori helyiségében dolgozó, biztonságszakmai szempontból kompetens munkatársak végzik az MVM Csoport tagvállalatai és a központi irodaház biztonsági felügyeletét annak ellenére, hogy az irodaház a magas biztonsági kockázatok miatt saját operátorokkal és élőerős őrzéssel is rendelkezik.

Annak érdekében, hogy a munkatársak és a berendezések biztonsága minden időben a biztonsági kockázatoknak megfelelően garantálható legyen, a létesítmény megerősített mechanikai védelemmel rendelkezik. A kerítés, illetve az épületek falai biztosítják az őrszolgálat beavatkozásához szükséges késleltetési időtartamot, miközben a kivonuló őrszolgálat értesítése is megtörténik.

A létesítmény fizikai védelmében birtoklás és tudás alapú beléptető rendszert (proximity kártya és PIN kód tasztatúra) alkalmaznak. Valamennyi ajtóvezérlőn történő átlépést videokamerák felügyelik. Az épület folyosóinak, lift előtereinek videokamerával történő megfigyelése biztosítja, hogy az egyes belépők által bejárt útvonal biztonsági szempontból követhető legyen.

Azokat a helyiségeket, épületeket (pénztár, irattárak), amelyekben folyamatosan nincs munkavégzés, behatolásjelző és beléptető rendszerrel külön védik. A folyamatos munkarendben dolgozó munkatársak a munkavégzéshez szükséges jogosultságokkal rendelkeznek.

Az egyik legnagyobb biztonsági kihívás és természetesen kockázat is egyben az, hogy a létesítmény irodaépülete a közforgalom részére megnyitott, azaz idegen személyek vendégként, meghívottként történő megjelenésére - elsősorban fő munkaidőben - számítani kell. A belépni szándékozó személyek irányítása, kísérése szintén az őrszolgálat feladata. Ennek szakszerű végrehajtásához biztosít adminisztratív és informatikai támogatást az MVM Csoport biztonsági szolgáltatója, az MVM Biztonsági Szolgáltató Központ Zrt.

6.4. Nukleáris erőmű

Egy nukleáris erőmű fizikai védelmi rendszere, annak pontos megismerése és elemzése nem lehet ennek az értekezésnek a része, ugyanis valamennyi információ egy már meglévő atomerőmű fizikai védelmi rendszeréről nemzeti minősített adat (államtitok). Ezt a tényt szem előtt tartva, csupán általános elgondolásokról, megfontolásokról és kialakítási elvekről lehet beszélni, amelyeket Magyarországon és az Amerikai Egyesült Államokban tanulmányoztam [15] és tapasztaltam.

Tekintettel arra, hogy egy nukleáris erőműbe telepített technológia megoldásokra vonatkozó nem védett információk (az interneten oldalak ezrei olvashatók e témában), ráadásul a Nemzetközi Atomenergia Ügynökség (NAÜ) honlapján bármikor elérhetőek a kötelezően implementálandó szabályok [2], a disszertációmban az atomerőmű biztonsági besorolását az adatvagyon (nemzeti minősített adatok) és a társadalmi beágyazódottsága adják, amelyek alapján így a Fokozott Biztonsági Kockázatú Létesítmény (FBKL) kategóriába sorolandó.

Egy nukleáris erőmű fizikai védelmi rendszerének tervezése szakhatóság által elrendelt, az adott létesítmény Tervezési Alapfenyegetettség (DBT – Design Basic Threat) meghatározásával kezdődik. E dokumentumot a kidolgozást követően azonnal minősíti az illetékes hatóság (Országos Atomenergia Hivatal - OAH), majd az „nemzeti minősített adat" kategóriába kerül, így ezt kizárólag azon személyek ismerhetik meg, akiknek erre a jogosultságuk megvan.

A gyakorlatban az ilyen környezetben tevékenykedni akaró társaságoknak Telephely Biztonsági Tanúsítványért kell folyamodniuk a Nemzeti Biztonsági Felügyelethez, amely a jogszabályok által előírt körülmények megléte esetén – például iparbiztonsági helyiség a megfelelő biztonságtechnikai kialakításban – ezt az engedélyt megadhatja. Ez az engedély az egyik, de elégséges feltétele annak, hogy minősített adatokat a társaság szakemberei megismerjék.

A tervezési alapfenyegetettség ismeretének birtokában kezdődik el aztán a fizikai védelmi rendszer tervezése, amely a Nemzetközi Atomenergia Ügynökség által kiadott ajánlásnak [2] megfelelően történik.

A fizikai védelmi rendszer tervezésének a „meghiúsítási stratégiát" kell követnie (megfelelő detektálási és késleltetési elveknek kell megvalósulni) annak érdekében, hogy a behatoló semlegesítése valóban sikeres legyen.

A detektálásnak, mint első lépésnek - a behatoló cselekményének felderítésére -, kiemelkedő szerep jut. Ezért annak hatásfokát is meghatározza a hatóság, amelynek legalább a 0,85 és 0,90 közötti sávba kell esnie. Ez a magas érték – azaz a behatolásjelző rendszer gyakorlatilag biztosan érzékeli a behatolót – úgy érhető el, hogy több, más-más technológiát alkalmazó biztonságtechnikai berendezést kell telepíteni, valamint többszintű fedővédelmet kialakítani.

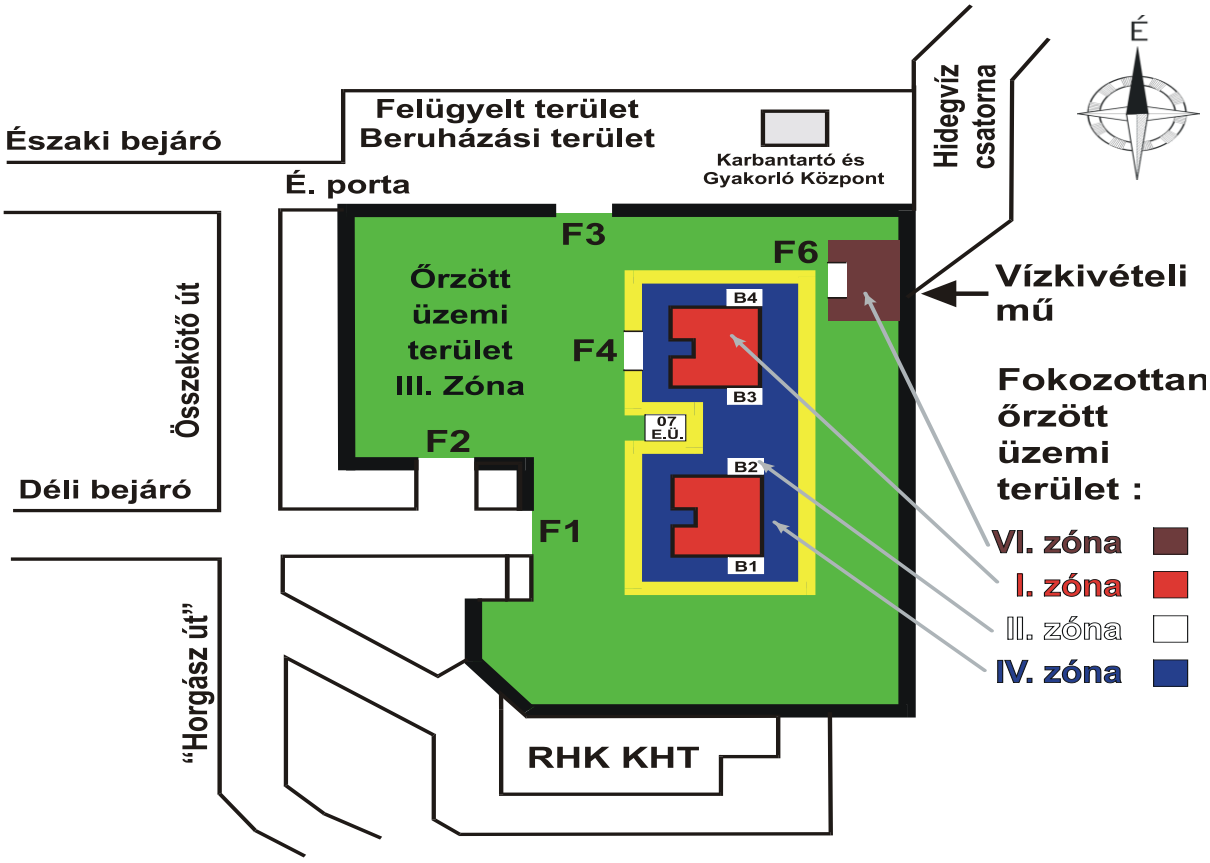
Tekintettel arra, hogy az MVM Paksi Atomerőmű Zrt. fizikai védelmi rendszerére vonatkozó valamennyi információ nemzeti minősített adat kategóriába sorolt, ezért a disszertációmban példaként a magyar atomerőműhöz hasonló, azonos elvek alapján tervezett és kiépített, de az Amerikai Egyesült Államokban lévő atomreaktor biztonságtechnikai berendezéseit tárgyalom.

A fizikai védelmi rendszer első elemként közvetlenül a létesítmény jogi határán húzódó 3 m magas, mindkét oldalon pengés NATO dróttal ellátott kerítésen kívül:

1. Külső kerítés a létesítményi terület határán (3 m magas, hegesztett 40x60-as zártszelvényekből álló kerítés, mindkét oldalon pengés NATO dróttal).
2. Belső kerítés a külső kerítéstől 6-10 m-re (így egy 6-10 m széles semleges, vagy izolációs zónát kialakítva; 3 m magas, hegesztett 40x60 zártszelvényekből álló kerítés, mindkét oldalon pengés NATO dróttal), ahol a kiegészítő biztonságtechnikai védelem elemei kerülnek telepítésre.
3. A semleges, vagy izolációs zónában átfedéssel telepített infra-sugaras sorompó rendszer.
4. A semleges, vagy izolációs zónában átfedéssel telepített *mikrohullámú sorompó* rendszer.
5. A semleges, vagy izolációs zónában, a belső kerítés mellett 25 m-ként egy-egy világítási oszlop, a semleges, vagy izolációs zónát teljes egészében és a külső kerítés melletti területet – nem atomerőműi területet – mintegy 3-6 méteren megvilágítva.
6. A semleges, vagy izolációs zónában lévő világítási oszlopokon a kamerák egymást is képkivágásban tartó, az egyes képmezőket átfedő, fix telepítésű kamerák.
7. A semleges, vagy izolációs zóna világítási oszlopain (minden második oszlopon) 1-1 *távvezérelhető* kamera.
8. A belső kerítésen 1 m magasan végigfutó, 40 mm átmérőjű fonott drótkötél, 25 méterenként átfedésben történő rögzítéssel.
9. A személybejáratnál kártyaolvasóval telepített forgókapu, amely zárt folyosón keresztül egy beléptető helyiségbe (zsilipeléssel történő továbbjutás, biztonsági őri felügyelet mellett) vezet.
10. Gépkocsi bejáratnál két sorban 8-8 automata „*bollard*-dal" biztosított, megerősített, érzékelőkkel ellátott motoros kapu.

Ebben a környezetben (három különböző technológiájú érzékelő rendszer) egy esetleges behatoló 0,9 bekövetkezés-valószínűséggel detektálható. (9. SZ. MELLÉKLET). A beépített késleltetést biztosító rendszerelemek adják a szükséges időtartamot a készenléti erők helyszínre érkezéséig, hogy a behatoló semlegesítése megtörténhessen. Nukleáris létesítmény fizikai védelmi rendszerének kialakítása során a mélységi védelem megszervezése és kiépítése alapvető fontosságú.

A 11. ábrán látható, hogy a mélységi védelemmel szembeni fokozott biztonsági elvárások és annak üzemeltethetősége érdekében 6 biztonsági zóna, különböző biztonsági kockázatokkal (I, II, III, IV, V, VI) került kialakításra (jelenleg az V. Zóna már nem létezik, egy átalakítás során megszüntetésre került). A felügyelt, őrzött és fokozottan őrzött üzemi terület elnevezéseket az atomerőművek fizikai védelmével kapcsolatos 190/2011 (IX.19.) Korm. rendelet [26] szabályozza.



11. ábra: Atomerőmű fizikai védelmi zónáinak egy lehetséges kialakítása.

A mélységi védelem kialakítása során a belépési jogosultsági szintek, az azok ellenőrzéséhez szükséges azonosítási módszerek természetes módon bővülnek, illetve erősödnek. Ezért, míg a létesítménybe történő beléptetés birtoklás és tudás alapú környezetben történik (nagy biztonságú proximity kártya és PIN kód használat), addig a magasabb védettségű zónák esetén már hosszabb PIN kódok, illetve a biometrikus azonosítás is szerepet kap. Az elektronikus védelem mellett mechanikai védelemmel is növelt a biztonsági szint (teljes magasságú, acél forgókapuk).

Az élőerős őrzés tekintetében egy atomerőműnek magas létszámú, az őrszolgálatok valamennyi szegmensét felvonultató szervezettel kell rendelkeznie. Ennek megfelelően az alábbi élőerős őrzést biztosító szolgálatok léteznek:

1. Fegyver nélküli vagyonőrök.
2. Fegyveres vagyonőrök.
3. Fegyveres Biztonsági Őrök.
4. Közvetlen hatósági kapcsolat (Terrorelhárítási Központ - TEK).

Természetesen a kommunikációs eszközök (kidolgozott alternatív megoldásokkal), fegyverek és monitorközpontok mind a fizikai védelem megfelelő szintjét biztosítják.

6.5. A fejezet összegzése – következtetések

Az egyes létesítményfajták biztonsági kockázatainak megfelelő fizikai védelmi rendszereket áttekintve megállapítható, hogy az általam kidolgozott kockázatértékelés és biztonsági kockázati rendszerbe történő besorolás jól alkalmazható a gyakorlati életben.

Az egyes létesítményeknél minden esetben megjelenik a mélységi védelem, a testreszabhatóság, azaz az objektumorientáltság igénye, amelyek értekezésem lényegi elemei.

Az általam kidolgozott módszer koherens módon képes kezelni a különböző biztonsági kockátokkal szembe néző különböző létesítményeket, amelyekben gazdasági társaságok, vagy akár állami intézmények tevékenykednek.

Az összeállított kockázatértékelési metódus különösen fontos előnyének gondolom, hogy az egyes, a fizikai védelmi rendszer megfelelő működését érő biztonsági kockázatok részleteit is képes kezelni, ami egyfajta garancia a kiegyenlített és objektumorientált védelemnek.

A rendszer rugalmassága lehetővé teszi az adott létesítmény esetében az optimális, jövőálló fizikai védelmi rendszer kialakítását, amely már gazdasági kérdés is.

A példaként felhozott valós létesítmények - követve az általam kidolgozott kockázatértékelési módszert - megfelelnek a biztonsági szakterületük által megszabott feltételeknek.

7. A KUTATÓMUNKA ÖSSZEGZÉSE

A különböző biztonsági kockázatú létesítményekben telepítendő, illetve telepített biztonságtechnikai berendezések alkalmazhatóságának értékelése a mostani szakmai gyakorlat szerint nem egységes abban, hogy a rendszerek megfelelnek-e a szakmai-megbízói elvárásoknak, vagy, hogy mindezek egyáltalán képesek-e a létesítmények biztonsági kockázatainak kezelésére. A - főként biztonságtechnikai szempontból esetlegesen elvégzett - biztonsági auditok, ellenőrzések, felülvizsgálatok nem azonos alapról indulnak ki, emiatt a szakmai kompetenciák sem értékelhetők egységesen. Mindezek eredményeképp az alul-, vagy szükségtelenül felültervezett biztonságtechnikai rendszerek gyakori problémát okoznak a mindennapi gyakorlatban.

E probléma megoldása érdekében dolgoztam ki az általános érvényű objektum-specifikus tervezési és kivitelezési alapelveket.

Felállítottam egy egységes elvrendszert, amely meghatározó támogatást tud biztosítani mind a megbízói, mind a tervezői oldal számára. Ennek segítségével már az elvárások szintjén is konkrét és célorientált tervezés válik lehetővé az egyértelmű eszköz-, és struktúraszükséglet előrevetítésével. Mindez ugyanakkor jelentős segítség a megbízói oldal üzemeltetői számára, mivel iránymutatással szolgál a biztonsági kockázatok aktualizálásából adódó esetleges módosítások, biztonságtechnikai fejlesztések, azok irányai és részletei meghatározásában is.

Kidolgoztam egy minimális követelményrendszert a biztonságtechnikai rendszerek tekintetében. Ennek alapja a biztonsági kockázatokkal arányos, kétszegmensű kockázati mátrixot figyelembe vevő szempontrendszer. Ebben egyértelműen megfogalmaztam azokat a biztonsági kockázatkezelési igényeket, amelyekkel egy meghatározott létesítmény üzemeltetése során foglalkozni szükséges. Ezen elemekből hoztam létre a „Veszélyfelhő”-t, amely a kockázatértékelési rendszer kidolgozásához a releváns adatokat tartalmazza.

A „Veszélyfelhő”-ben megjelölt veszélycsoportok dinamikusan változtathatók, mégpedig az adott létesítmény aktuális működési körülményei szerint. Ennek megfelelően az aktuális biztonsági kockázatok változása jól követhető, így pedig a kockázatok kezeléséhez szükséges intézkedések haladéktalanul megtehetők.

Elvégeztem az egyes létesítmények biztonsági kockázatok szerinti besorolását. Ehhez a „Létesítményi mátrix” eredményét használtam. A „Létesítményi mátrix” segítségével válnak a vizsgált létesítmények a biztonsági kockázatok alapján összehasonlíthatókká. Ennek megalkotásá-

hoz több adatot használtam fel, amelyek az egyes létesítmények működéséből, annak körülményeiből adódó paraméterek. A vizsgált létesítményeket ezek alapján egy „Létesítményi együtthatóval" jellemeztem. Ennek alapját a társadalmi beágyazódottságuk, illetve az általuk alkalmazott technológia védelmi igényei, valamint az adott létesítmény adatvagyonának érzékenysége adja. Az egyes létesítmények biztonsági kategóriába történő besorolásához készítettem el azokat a minimál követelményeket, amelyek megfelelnek az egyes védelmi igényeknek.

Ezt követően meghatároztam az adott létesítményre aktuálisan kiszámított biztonsági kockázati értéket jelző számot. Ez mutatja meg, hogy a vizsgált létesítmény biztonsági helyzete, a létesítmény biztonsági kockázatok kezelésére való felkészültsége jelenleg milyen szintű.

Az elemi események kockázatértékelési mátrixának kialakítása során a Létesítményi együtthatóhoz hasonló kialakítású mátrix-ot alkalmaztam, mert így az adott létesítményre kialakított „Veszélyfelhő"-ben szereplő elemi események kockázati értékének számtani átlaga a Létesítményi együtthatóval összevethető. Így az közvetlenül beilleszthető a Létesítményi mátrix segítségével elkészített létesítmények kockázati besorolásába, azaz a meglévő és kockázatértékelt fizikai védelmi rendszer megfelelősége, vagy meg nem felelése egyenesen megállapítható - ugyancsak lehetőséget teremtve a folyamatos és visszatérő rendszerellenőrzésre, a biztonsági környezet, és az azt követő védelmi technikák rendszerszemléletű aktualizálására.

Alapvetően négy biztonsági kockázatú létesítményi kategóriát határoztam meg. Ezt követően a hozzátartozó biztonságtechnikai rendszerkialakítási és értékelési elveket dolgoztam ki. E négy biztonsági kockázatú létesítményi kategória tökéletesen illeszkedik és megfeleltethető az elektronikus információbiztonsággal kapcsolatos fizikai védelmi rendelkezések számára is. Ebbe a kockázati rendszerbe ez a szakterület is jól beilleszthető. Ezeknek a biztonsági kockázati szinteknek a meghatározásához egy jól érthető és követhető kockázatértékelési módszert dolgoztam ki annak érdekében, hogy az objektivitási elvek messzemenően transzparensek legyenek.

Módszeremmel egyértelmű és célorientált, az adott létesítmény biztonsági kockázatait értékelő dokumentáció készíthető, amely már a tervezéskor szükséges. Ennek segítségével nemcsak az elkészítés időpontjában aktuális terveket produkálhatunk, hanem megteremtjük az „up-to-date" állapotot, vagyis a szinten tartás követelményének is megfelelő metodikát. Mivel az általam elkészített tervek, iránymutatások igen rugalmasak, azonnali reagálást tesznek lehetővé a mindennapi gyakorlat követéséhez, a változó biztonságtechnikai igények maximális kiszolgálásához.

Meghatároztam a „normál” üzemi működés mellett a „minősített időszakban” történő fizikai védelmi rendszerek üzemeltetési körülményeit is a biztonsági kockázatok változásának függvényében.

Összességében munkám eredményeként tehát kidolgoztam egy jól követhető és használható kockázatértékelési módszert és ahhoz közvetlenül kapcsolódó biztonságtechnikai rendszerkialakítási elvet. Ezek eredményeként pedig az általam szolgáltatott rendszer és értékelési javaslat kellő rugalmassággal le tudja követni a piaci igényeket, elvárásokat is. Megalkottam tehát egy objektumorientált tervezési és kivitelezési elvrendszert, amely jól követhető alkalmazási normákat jelent a felhasználók teljes köre számára.

7.1. Következtetések, tézisek, folytatás

A magyarországi és külföldi gyakorlat a fizikai védelmi rendszerek tervezése és kialakítása tekintetében nem áll nagyon távol egymástól. Azonban az a szemléletmód, amely elsősorban a hatékonyságot és objektumorientáltságot helyezi előtérbe, még nem teljes mértékben honosodott meg itthon. Ami minden szempontból figyelemre méltó és a kutatómunkám során bebizonyosodott: egy a biztonsági kockázatoknak megfelelő, jól testreszabott fizikai védelmi rendszer mind a költségvetés, mind a biztonságtechnikai rendszer telepítésének tekintetében szükségszerű. Mindez pedig a biztonsági szakterület szabályozásának, mind a megvalósításban résztvevő szakembernek alapvető szakmai segítség.

7.1.1. Új tudományos eredmények (tézisek)

7.1.1.1. Elsőként létrehoztam egy biztonsági kockázatokat értékelő módszert, amely biztonságtechnikai rendszerek tervezéséhez ad támogatást. [16]

7.1.1.2. Bebizonyítottam, hogy az egyes létesítményeket elegendő négy biztonsági kockázati kategóriába sorolni. [16]

7.1.1.3. Igazoltam, hogy az általam kidolgozott módszerrel objektumorientált módon van lehetőség - az egyes biztonsági kockázatoknak megfelelő besorolás mellett - az adott létesítmények fizikai védelmi rendszerének tervezésére, kialakítására.

7.1.2. **Javaslat a kutatómunka további folytatására**

Értekezésem kidolgozása során jól láthatóan körvonalazódott az a védelmi probléma, amely szerint a fizikai védelmi rendszerek működtetése minősített időszakban milyen módon változik.

Fontos lenne kidolgozni annak módszerét, hogy a normál (közhasználati kifejezéssel élve „békeidőben") időszakban meglévő biztonsági kockázatok kezelését milyen módon kellene módosítani, ha minősített időszakot jelent be a kormányzat, vagy akár a társaság biztonsági szervezetének vezetője, illetve ezen időszakban az adott létesítmény milyen biztonsági kockázatokkal szembesül és ez a változás milyen módon kezelhető az általam kidolgozott rendszerben.

Egy másik, napjainkban egyre akutabb biztonsági problémát okozó ún. drónok[63], az azok elleni védekezés fontos tanulmányozási terület lehet. Az elmúlt néhány év robbanásszerű technológiai fejlődése rendkívüli biztonsági kihívásokat állít a létesítmények fizikai védelmét üzemeltető, tervező és kivitelező társaságok elé. Nem kell sokat vizsgálódni az Internet végeláthatatlan hálóján, hogy a rengeteg nagyszerű felhasználási példa mellett néhány a robbanóanyagok, vagy kisméretű géppisztolyok szállítására és alkalmazására is megfelelő mintát találjunk. Ezek olyan eszközök, amelyek már kiemelkedő biztonsági kockázatot jelentenek. E veszélyek feldolgozása, az erre alapozott kockázatkezelési módok rendszerbe illesztése további kutatási célokat ad.

Végeredményben: a közeli jövő újabb lehetőséget teremthet egy még komplexebb, valamennyi körülményt figyelembe vevő kockázatkezelési és fizikai védelmi rendszer kidolgozásához, amelyhez ez az értekezés megfelelő alapot szolgáltat.

[63] „Drone" angol elnevezésből átvett szóhasználat, amely valójában egy pilóta nélküli repülőszerkezet – UAV: Unmanned Aerial Vehicle -, amely felhasználása szerint a hobbitól az ipari, hadiipari területekig megtalálható.

BEFEJEZÉS (KÖSZÖNETNYILVÁNÍTÁS)

A doktori disszertációm elkészítéséhez a szakirodalom tanulmányozásán kívül sok szakmai interjúra, műszaki megbeszélésre volt szükség, amely a közvetlen munkatársaim és az MVM Csoport tagvállalatainál dolgozó szakemberek támogatása és közreműködése nélkül nem lett volna lehetséges.

Kiemelt köszönet illeti az MVM Csoport biztonsági szakterületének vezetőjét, az MVM Zrt. Biztonsági Igazgatóját (Dr. Tamási Gábor) és helyettesét (Dr. Fogarasi Attila) azokért a lehetőségekért, személyes konzultációkért, szakmai vitákért, amelyek nélkül ez az értekezés nem készülhetett volna el. Külön köszönöm azt a lehetőséget, amelyet a Nemzetközi Atomenergia Ügynökség által szervezett szakmai tanfolyam elvégzéséhez kaptam.

Kiemelt köszönetet szeretnék mondani Prof. Dr. Kovács Tibor tanszékvezető úrnak, témavezetőmnek, aki a kutató munkám során mindenben támogatott, lehetőséget biztosított disszertációm összeállítására, rendszeres konzultációkkal segítette a munkámat.

A köszönetnyilvánítások között nem feledkezhetem meg Tóth Levente kollégámról, barátomról, akinek szakmai támogatása fontos támpontokat biztosított részemre.

Külön köszönet a családomnak, akik elviselték az egyébként is kevés szabadidő további csökkentését és mindenben támogatták az értekezésem megírását.

FELHASZNÁLT IRODALOM

1. GARCIA, M. L. (Sandia National Laboratories): Vulnerability and assessment of physical protection systems, ISBN13 978-0-7506-7788-2 (2001) **[1]**

2. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No.13 (INFCIRC/225/Rev.5)
http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf
letöltve: 2015. február 18. **[2]**

3. GARCIA, M. L.: Design and Evaluation of Physical Protection System (PPS), ISBN-13: 978-0-08-055428-0 (Kindle Location 230), Elsevier Science, Kindle Edition **[3]**

4. Interagency Security Committee Guide 2015 December
https://www.dhs.gov/.../isc-planning-managing-physical-security-reso...
letöltve: 2016. február 20. **[4]**

5. The history of Home security
https://www.livewatch.com/history-of-home-security
letöltve: 2017. június 30. **[5]**

6. The history of the alarm system
https://www.abus.com/eng/Guide/Break-in-protection/Alarm-systems/History-of-the-alarm-system
letöltve: 2017. június 2. **[6]**

7. KISS S.: A biztonságtechnika kialakulásának történetéről; Hadmérnök, X. évfolyam, 4. szám, 2015. december, 24-29. oldalak, ISSN 1788-1919 **[7]**

8. SANS Institute InfoSec Reading Room: The history and evaluation of Intrusion detection, SANS Institute 2001
https://www.sans.org/reading-room/whitepapers/detection/history-evolution-intrusion-detection-344
letöltve: 2017. április 15. **[8]**

9. PAPP P.: IP a biztonságtechnika világában
http://www.detektor.siteset.hu/fajl.php?id=8267
letöltve: 2017. július 1. **[9]**

10. UTASSY S., BÁRKÁNYI P.: IP alapú kommunikáció az elektronikus vagyonvédelmi rendszerekben;
http://uni-nke.hu/downloads/bsz/bszemle2006/2/06%20Utassy-Barkanyi.pdf
letöltve: 2016. október 12. **[10]**

11. The evolution of access control systems
http://securecomminc.com/2014/06/19/the-evolution-of-access-control-systems/
letöltve: 2017. augusztus 1. **[11]**

12. The evolution of access control
https://www.isonas.com/news-education/the-evolution-of-access-control/
letöltve: 2017. augusztus 2. **[12]**

13. HORVÁTH T., KOVÁCS T.: Kockázatértékelési módszerek és lehetőségeik a fizikai védelem területén
http://www.securinfo.hu/termekek/biztonsagi-szolgalat-az-eloero-eszkozei/978-kockazatertekelesi-modszerek-es-lehetosegeik-a-fizikai-vedelem-teruleten.html
letöltve: 2017. július 1. **[13]**

14. MABISZ Betöréses lopás- és rablásbiztosítás technikai feltételei (Ajánlás)
Telephelyek és létesítmények, helyiségek őrzésének, vagyontárgyak tárolásának, szállításának szabályai: 2015. április 24.- módosítás
http://www.pluto.hu/_A/A2.html
letöltve: 2016. február 15. **[14]**

15. IAEA International Training Course on the Physical Protection of Nuclear Material and Nuclear Facilities (2016. november 11.-22.), Albuquerque, NM, USA **[15]**

16. HORVÁTH T., KOVÁCS T.: Kockázatértékelési módszerek, azok alkalmazási lehetőségei a fizikai védelem területén; Tavaszi Biztonságtechnikai Szimpózium 2013., Budapest, Magyarország, 2013. április 10., Óbudai Egyetem, 10. oldal (ISBN: 978-615-5018-53-4) **[16]**

17. Mark-Recapture Maximum Likelihood Estimators adapted from Seber et al. 1982 (page 200) and Burnham et al. 1987 (page 114) for CJS models
studylib.net/.../calculation-of-detection-probabilities-adapted-from-bu..
letöltve: 2017. július 3. **[17]**

18. WHITH, J. M.: Security Risk Assessment, Managing Physical and Operational Security, ISBN: 978-0-12-800221-6; 206. oldal **[18]**

19. MOTEFF, J., PARFORMAK, P.: Critical Infrasturcture and Key Assets: Definition and Identification; October 1, 2004
file:///C:/Users/B5596/Downloads/ADA454016.pdf
letöltve: 2016. szeptember 30. **[19]**

20. IZSÓ L.: SOL. Safetyafety through Organizational. Learningearning. Tengelic, november pszichológia előadás 2.
http://docplayer.hu/33819749-Sol-safetyafety-through-organizational-learningearning-tengelic-november-pszichologi-az-eload-2.html
letöltve: 2016. október 15. **[20]**

21. Skálatípusok.
http://ramet.elte.hu/~kún.adam/oktatas/biometria8.pdf
letöltve: 2017. március 1. **[21]**

22. TATAY T., PATAKI L.: Kockázatelemzés, Kockázatértékelés, cselekvési tervek; 2008. december, Raabe Kiadó
www.spek.hu/letoltes.php?fajl=anyagok/Tatay-Pataki-kockazatelemzes.pdf

letöltve: 2016. szeptember 4. **[22]**

23. Uptime Institute LLC. Datacenter Site Infrastructure Tier Standard: Topology
LLC UPTIMEINSTITUTE – 2012
pdfs.semanticscholar.org
letöltve: 2016. február 10. **[23]**

24. Az IEC/ISO 31010:2009 Risk management. Risk assessment techniques magyar nyelvű változata, MSZ EN 31010 (2010), Kockázatkezelés. Kockázat felmérési eljárások. **[24]**

25. HARMADOS Gy.: Gazdasági hírszerzés és ipari kémkedés, Detektor Plusz 2006/8-9.
www.detektor.siteset.hu/fajl.php?id=8277
letöltve: 2017. február 20. **[25]**

26. 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1100190.kor
letöltve: 2017. február 20. **[26]**

27. ISO/IEC Guide 73:2009 – Kockázat menedzsment (elérhetőség: https://www.iso.org /standard/44651.html)

28. BARKER, D.: A Guide to Physical Security for Data Centers; 2012
http://www.datacenterjournal.com/a-guide-to-physical-security-for-data-centers/)
letöltve: 2017. február 6.

29. TAKÁCS Sz.: Érzékenységvizsgálatok a statisztikai eljárásokban; Alkalmazott matematikai lapok 29 (2012), 67-100. oldalak
aml.math.bme.hu/wp-content/uploads/2012/06/29-Takács.pdf
letöltve: 2016. augusztus 1.

30. JÓSZAI J.: A határőrség objektumainak őrizete és védelme (doktori értekezés), Zrínyi Miklós Nemzetvédelmi Egyetem, 2002
uni-nke.hu/downloads/konyvtar/digitgy/phd/2002/joszai_janos.pdf
letöltve: 2016. február 20.

31. SOL elemzés: BME Ergonómiai és Pszichológiai Tanszék; PARt. eseményelemzési továbbképzés, Tengelic; 2005. november 15-17.;
http://erg.bme.hu/sol/SOL_bevezeto_prez.pdf
letöltve: 2016. október 15.

32. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from =EN
letöltve: 2016. augusztus 23.

33. FENNELLY, L. J.: Effective Physical Security, Fifth Edition; ISBN: 978-0-12-804462-9

34. PATTERSON, D. G. CPP PSP: Implementing Physical Protection Systems: A Practical Guide (Kindle Locations 87-88), ASIS International, Kindle Edition

35. Home Safety: The history of home security
http://www.alarm.org/homesafety/evolutionofhomesecurity.aspx
letöltve: 2016. június 30.

36. Iparági egységes fogalomtár (IVSZ Adatközpont munkacsoport) Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége
www.isafe.hu/data/pdf/ivsz_adatkozpont_fogalomtar_v10.pdf
letöltve: 2016. február 10.

37. Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide, 2015 December
https://www.dhs.gov/.../isc-planning-managing-physical-security-reso...
letöltve: 2016. február 20.

38. Nemzeti Szabványügyi Testület Állásfoglalása a műszaki előírások nemzeti bevezetése és jogállása tárgyában
www.mszt.hu/web/guest/tevhitek-es-tenyek
letöltve: 2017. február 28.

39. MÓRÉ A.: Biztonságtechnikai Szabványok 2016. július 14.
servinternkft.hu/sites/...hu/.../2016/biztonsagtechnikai_szabvanyok_-_2016-07.pdf
letöltve: 2017. február 28.

40. Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (HL L 281., 1995.11.23., 31. oldal)
eur-lex.europa.eu/legal-content/HU/TXT/?uri=celex%3A31995L0046
letöltve: 2017. március 7.

41. 1997. évi CLIX. törvény a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99700159.tv
letöltve: 2017. március 9.

42. Fejezetek a kritikus infrastruktúra védelméről (tanulmánykötet), Magyar Hadtudományi Társaság 2013., ISBN 978-963-08-6926-3
mhtt.eu/hadtudomany/KIV_tanulmanykotet.pdf
letöltve: 2017. január 9.

43. 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról
https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1300065.kor
letöltve: 2017. január 9.

44. BEREK T., HORVÁTH T.: Fizikai védelmi rendszerek dinamikusan változó környezetben, Hadmérnök IX:(2), 2014, 16-24. oldalak, ISSN 1788-1919

45. HORVÁTH T., KOVÁCS T.: Possible application of thermal cameras with regard to security engineering; Hírvillám = Signal Badge 4: pp. 17-31., 2014, ISSN 2061-9499

46. HORVÁTH T., KOVÁCS T.: Létfontosságú rendszerek és létesítmények védelme, üzemeltetői biztonsági terv a gyakorlatban; Biztonságtechnikai Szimpózium a Magyar Tudomány Ünnepe 2013 keretében: Bánki közlemények, Konferencia helye, ideje: Budapest, Magyarország, 2013. november 12-19., Óbudai Egyetem, 1-10. oldalak, ISBN: 978-615-5018-89-3

47. HORVÁTH T., KOVÁCS T.: A hőkamerák alkalmazási területei, kiemelten a biztonságtechnikai felhasználásokban; International Engineering Symposium at Bánki – Bánki Kari Tudományos Konferencia; Konferencia helye, ideje: Budapest, Magyarország, 2011. november 15-16., Óbudai Egyetem, 13. oldal, ISBN: 978-615-5018-15-2

48. HORVÁTH T., KOVÁCS T.: Zsetonok és IP kamerák – a játéktermek biztonságtechnikájának egyes kérdései, Konferencia helye, ideje: Budapest, Magyarország, 2010. november 10-11., Óbudai Egyetem, 11 oldal, Nemzetközi Gépész, Mechatronikai és Biztonságtechnikai Szimpózium, ISBN: 978-615-5018-10-7

49. HORVÁTH T.: Kábelek, hálózatok, CCTV rendszerek; Hadmérnök VI: (3), 5-13. oldalak, 2011, ISSN 1788-1919

50. HORVÁTH T.: Korszerű kerítésvédelem; Hadmérnök VI: (3), 14-21. oldalak, 2011, ISSN 1788-1919

51. MESSAUD, B.: Access Control Systems: Security, Identity Management and Trust Models; IBM Corp. Austin, ISBN-10: 0-387-00445-9; springeronline.com; 2006

52. TAKÁCS Sz.: Érzékenységvizsgálatok a statisztikai eljárásokban; Alkalmazott Matematikai Lapok 29 (2012), 67-100. oldalak, ISSN 0133-3399

53. BERÉNYI M.: A kockázatelemzés buktatói, kockázatbecslés szabványos módszerekkel, előadás anyag
www.wil-zone.hu/szakmaianyagok/EOQ_risk01.pdf
letöltve: 2017. május 21.

54. BEDZSULA B.: Minőségmenedzsment módszerek
file:///C:/Users/B5596/Downloads/minmenmod_4_2017.pdf
letöltve: 2017. augusztus 2.

55. KISS S.: Atomerőmű, vagy alternatív energia, a biomassza
http://uni-nke.hu/downloads/bsz/bszemle2012/2/03.pdf
letöltve: 2016. május 18.

56. TÓTH A.: A magánbiztonsági ágazat minősítési rendszere; Hadmérnök online; XI. Évfolyam, 4. szám, 2016. december, ISSN 1788-1919
www.matarka.hu/cikk_list.php?fusz=149368
letöltve: 2017. február 2.

57. HORVÁTH K., KÁTAI-URBÁN L., SEBESTYÉN Zs.: A nukleáris biztonság és védettség hazai kutatási-fejlesztési eredményei; Hadmérnök online; XI. Évfolyam, 4. szám, 2016. december, ISSN 1788-1919
www.matarka.hu/cikk_list.php?fusz=149368
letöltve: 2017. február 2.

58. SZŰCS E.: Az ősember „biztonságtechnikai" eszközei; Hadmérnök online; XI. Évfolyam, 4. szám, 2016. december, ISSN 1788-1919
www.matarka.hu/cikk_list.php?fusz=149368
letöltve: 2017. február 2.

59. TAKÁCS Z.: Vagyonvédelmi eszközök és módszerek az ipari nagyberuházások területén; Hadmérnök online; IX. Évfolyam, 4. szám, 2014. december, ISSN 1788-1919
hadmernok.hu/144_05_takacsz_2.pdf
letöltve: 2017. augusztus 2.

60. BENANTAR, M.: Access Control Systems Security, Identity Management and Trust Models; IBM Corp, Austin, TX, USA
www.springer.com/us/book/9780387004457
letöltve: 2017. április 14.

61. SCHMIEDL, E., SPINDEL, M.: Strengths and Weaknesses of Access Control System; előadás;
https://archive.org/.../HOPE-7-Strengths_and_Weaknesses_of_Physic...
letöltve: 2017. január 22.

62. ANDERSON, R.: Security Engineering Second Edition;
http://www.cl.cam.ac.uk/~rja14/book.html;
letöltve: 2017. július 31.

63. KHAIRALLAH, M.: Physical Security Systems Handbook The design and Implementation of Electric Security Systems; 2017, Elsevier; ISBN 13: 978-0-7506-7850-6
https://www.elsevier.com/.../physical-security-systems-handbook/khai...
letöltve: 2017. augusztus 2.

64. NORMAN, T. L.: Electric Access Control; 2012, Elsevier; ISBN: 978-0-12-3820297
https://www.elsevier.com/...access-control/norman/978-0-12-382028-...
letöltve: 2016. november 25.

1. SZ. MELLÉKLET

LITÉR GÁZTURBINÁS TARTALÉK ERŐMŰ FIZIKAI VÉDELMI RENDSZERE BIZTONSÁGI KOCKÁZATAIT KIÉRTÉKELŐ TÁBLÁZATOK

Veszélyek megnevezése	LITÉR		Kockázati érték	Létesítmény együttható	ÁTLAG
Működésből adódó biztonsági kockázatok	ESÉLY	HATÁS		20	
Tevékenységből adódóan ügyfélfogadás van a létesítményben	0	0	0		
Közismert a létesítményben folyó tevékenység	5	3	15		
Közismert a létesítményen belüli környezet, alkalmazott technológia	3	3	9		
Létesítményben több intézmény/társaság tevékenykedik	0	0	0		
Lehetséges lakossági tiltakozás, akár erőszakos formában is, a létesítményben végzett tevékenysége elleni	1	5	5		5
A létesítmény ellen elkövetendő terrortámadás reális veszély	2	5	10		
Nincsenek kidolgozott szabályzatok, rutinok a krízishelyzetek kezelésére (ÜFT; Pandémiás terv; stb.)	1	5	5		
Nincsenek a létesítmény működéséhez kidolgozott és hatályba helyezett biztonsági szabályzatok	1	5	5		
Létesítménybe ellenőrzés nélkül léphetnek személyek és/vagy vihetnek be- és ki csomagokat	1	5	5		
Meglévő porta, recepciós, őrszolgálat csomagokat átvehet, őrizhet, továbbíthat.	0	0	0		

Veszélyek megnevezése	LITÉR		Kockázati érték	Létesítmény együttható	ÁTLAG
Műszaki problémákból adódó biztonsági kockázatok	ESÉLY	HATÁS		20	
Közvilágítással, világítással kapcsolatos üzemszünet (látási problémák)	3	5	15		
Nincs önálló hálózat (más hálózattól fizikailag elválasztott) kiépítve a biztonságtechnikai rendszerek számára (DEPEDENCIA)	1	5	5		
Természeti csapás (műszaki problémákat generált) miatt a létesítmény üzeme akadozhat, akár le is állhat	3	5	15		
Kiépített biztonságtechnikai rendszerek nincsenek.	1	5	5		
Vannak kiépített elektronikus biztonságtechnikai rendszerek, de nincs rendszeres karbantartás, a szükséges javítások nem készülnek el időben.	1	2	2		11
Nincs, vagy nem megfelelő a kiépített szünetmentes berendezés, illetve hálózat a biztonságtechnikai rendszerek számára	1	5	5		
Létesítmény kerítéssel nem, vagy csak részben van elválasztva a környezetétől. A meglévő kerítés állapota nem megfelelő	1	2	2		
Meglévő biztonságtechnikai rendszerek üzemideje meghaladta a 10 évet, és/vagy a gyártói támogatás megszűnt.	5	5	25		
A létesítményben veszélyes kategóriájú technológiai, biztonsági szempontból kockázatos anyagokkal, folyamatok zajlanak.	5	5	25		

Veszélyek megnevezése	LITÉR		Kockázati érték	Létesítmény együttható	ÁTLAG
Bűnügyi fertőzöttségből adódó biztonsági kockázatok	ESÉLY	HATÁS		20	
Létesítmény környezetében a tulajdon ellen elkövetett cselekmények éves száma országos átlag, vagy az feletti	4	3	12		
Létesítményben végzett technológiai folyamatokat kurens (fekete gazdaság területén keresett és jól eladható) anyagokkal, szerszámokkal, gépekkel folytatnak.	4	3	12		
Társaság által használt gépkocsikban beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs	1	5	5		
Társaság által a technológiai folyamathoz használt gépjárművekben, gépekben beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs.	1	5	5		
Létesítményben élőerős őrzést nem alkalmaznak, a biztonságtechnikai rendszerek üzemeltetése a munkavállalók feladata.	5	5	25		14
Létesítményben élőerős biztonsági szolgálat működik, de járőrözés nincs, vagy nem megfelelően van szervezve.	0	0	20		
Létesítménybe történő be- és kiléptetés nem, vagy nem megfelelően szabályozott, illetve az nem a szabályok szerint történik	1	5	5		
Létesítmény fizikai védelmi rendszerében a mélységi védelem kaialkítása nincs, vagy nem megfelelő.	3	5	15		
Létesítmény fizikai védelmi rendszerében biztonsági zónák, területek nincsenek, vagy nem megfelelően vannak meghatározva.	3	5	15		
Létesítmény közvetlen környezet nem átlátható, nem gondozott, a telekhatárok, külterületi objektumok rejtve megközelíthetőek.	5	5	25		

Veszélyek megnevezése	LITÉR		Kockázati érték	Létesítmény együttható	ÁTLAG
Emberi munkavégzésből adódó biztonsági kockázatok	ESÉLY	HATÁS		12	
Az IT/ICT hálózat üzemeltetői a biztonságtechnikai hálózat üzemeltetői is egyben	1	5	5		
A biztonságtechnikai rendszerek felügyeletét szakmailag nem kompetens munkavállalóval látja el társaság	1	5	5		
Szabályzatokban rögzített folyamatok betartatása nem konzekvens.	1	5	5		
Biztonságtechnikai rendszerek karbantartását és javítását végző társaság munkavállalói munkavégzésének színvonala nem megfelelő	1	5	5		
Társaság biztonságtudatossági szintje nem ismert, vagy igen alacsony.	1	5	5		5
A be- és kiléptetésre, áruszállításokra vonatkozó szabályzatok nincsenek, vagy azok betartatása nem megfelelő részletességgel kidolgozottak.	1	5	5		
Biztonsági őrök tevékenységének ellenőrzöttsége, a munkavégzés szinvonala nem megfelelő.	0	0	0		
Meglévő fizikai védelmi rendszerek használtata nem napi rutin a társaság életében.	1	5	5		
Biztonsági rendszerek esemény- és hibaüzeneteire a társaság nem időben reagál.	1	5	5		
Biztonsági terület munkatársai képzése, továbbképzése nem megoldott.	1	5	5		
Kockázati együttható átlaga					**9**

2. SZ. MELLÉKLET

SAJÓSZÖGED GÁZTURBINÁS TARTALÉK ERŐMŰ FIZIKAI VÉDELMI RENDSZERE BIZTONSÁGI KOCKÁZATAIT KIÉRTÉKELŐ TÁBLÁZATOK

Veszélyek megnevezése	SAJÓSZÖGED		Kockázati érték	Létesítmény együttható	ÁTLAG
Működésből adódó biztonsági kockázatok	ESÉLY	HATÁS		12	
Tevékenységből adódóan ügyfélfogadás van a létesítményben	0	0	0		
Közismert a létesítményben folyó tevékenység	5	3	15		
Közismert a létesítményen belüli környezet, alkalmazott technológia	3	3	9		
Létesítményben több intézmény/társaság tevékenykedik	0	0	0		
Lehetséges lakossági tiltakozás, akár erőszakos formában is, a létesítményben végzett tevékenysége elleni	1	5	5		12
A létesítmény ellen elkövetendő terrortámadás reális veszély	2	5	10		
Nincsenek kidolgozott szabályzatok, rutinok a krízishelyzetek kezelésére (ÜFT; Pandémiás terv; stb.)	1	5	5		
Nincsenek a létesítmény működéséhez kidolgozott és hatályba helyezett biztonsági szabályzatok	1	5	5		
Létesítménybe ellenőrzés nélkül léphetnek személyek és/vagy vihetnek be- és ki csomagokat	1	5	5		
Meglévő porta, recepciós, őrszolgálat csomagokat átvehet, őrizhet, továbbíthat.	0	0	0		

Veszélyek megnevezése	SAJÓSZÖGED		Kockázati érték	Létesítmény együttható	ÁTLAG
Műszaki problémákból adódó biztonsági kockázatok	ESÉLY	HATÁS		12	
Villamos energia kiesése (áramszünet)	3	5	15		
Közvilágítással, világítással kapcsolatos üzemszünet (látási problémák)	3	5	15		
Nincs önálló hálózat (más hálózattól fizikailag elválasztott) kiépítve a biztonságtechnikai rendszerek számára (DEPEDENCIA)	1	5	5		
Természeti csapás (műszaki problémákat generált) miatt a létesítmény üzeme akadozhat, akár le is állhat	3	5	15		
Kiépített biztonságtechnikai rendszerek nincsenek.	1	5	5		12,7
Vannak kiépített elektronikus biztonságtechnikai rendszerek, de nincs rendszeres karbantartás, a szükséges javítások nem készülnek el időben.	1	2	2		
Nincs, vagy nem megfelelő a kiépített szünetmentes berendezés, illetve hálózat a biztonságtechnikai rendszerek számára	1	5	5		
Létesítmény kerítéssel nem, vagy csak részben van elválasztva a környezetétől. A meglévő kerítés állapota nem megfelelő	3	5	15		
Meglévő biztonságtechnikai rendszerek üzemideje meghaladta a 10 évet, és/vagy a gyártói támogatás megszűnt.	5	5	25		
A létesítményben veszélyes kategóriájú technológiai, biztonsági szempontból kockázatos anyagokkal, folyamatok zajlanak.	5	5	25		

Veszélyek megnevezése	SAJÓSZÖGED		Kockázati érték	Létesítmény együttható	ÁTLAG
Bűnügyi fertőzöttségből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**12**	
Létesítmény környezetében a tulajdon ellen elkövetett cselekmények éves száma országos átlag, vagy az feletti	4	3	12		
Létesítményben végzett technológiai folyamatokat kurens (fekete gazdaság területén keresett és jól eladható) anyagokkal, szerszámokkal, gépekkel folytatnak.	4	3	12		
Társaság által használt gépkocsikban beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs	1	5	5		
Társaság által a technológiai folyamathoz használt gépjárművekben, gépekben beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs.	1	5	5		
Létesítményben előerős őrzést nem alkalmaznak, a biztonságtechnikai rendszerek üzemeltetése a munkavállalók feladata.	5	5	25		**16,4**
Létesítményben előerős biztonsági szolgálat működik, de járőrözés nincs, vagy nem megfelelően van szervezve.	5	5	25		
Létesítménybe történő be- és kiléptetés nem, vagy nem megfelelően szabályozott, illetve az nem a szabályok szerint történik	1	5	5		
Létesítmény fizikai védelmi rendszerében a mélységi védelem kaialkítása nincs, vagy nem megfelelő.	5	5	25		
Létesítmény fizikai védelmi rendszerében biztonsági zónák, területek nincsenek, vagy nem megfelelően vannak meghatározva.	5	5	25		
Létesítmény közvetlen környezet nem átlátható, nem gondozott, a telekhatárok, külterületi objektumok rejtve megközelíthetőek.	5	5	25		

Veszélyek megnevezése	SAJÓSZÖGED		Kockázati érték	Létesítmény együttható	ÁTLAG
Emberi munkavégzésből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**12**	
Az IT/ICT hálózat üzemeltetői a biztonságtechnikai hálózat üzemeltetői is egyben	1	5	5		
A biztonságtechnikai rendszerek felügyeletét szakmailag nem kompetens munkavállalóval látja el társaság	1	5	5		
Szabályzatokban rögzített folyamatok betartatása nem konzekvens.	1	5	5		
Biztonságtechnikai rendszerek karbantartását és javítását végző társaság munkavállalói munkavégzésének színvonala nem megfelelő	1	5	5		
Társaság biztonságtudatossági szintje nem ismert, vagy igen alacsony.	1	5	5		**4,5**
A be- és kiléptetésre, áruszállításokra vonatkozó szabályzatok nincsenek, vagy azok betartatása nem megfelelő részletességgel kidolgozottak.	1	5	5		
Biztonsági őrök tevékenységének ellenőrzöttsége, a munkavégzés szinvonala nem megfelelő.	0	0	0		
Meglévő fizikai védelmi rendszerek használtata nem napi rutin a társaság életében.	1	5	5		
Biztonsági rendszerek esemény- és hibaüzeneteire a társaság nem időben reagál.	1	5	5		
Biztonsági terület munkatársai képzése, továbbképzése nem megoldott.	1	5	5		
Kockázati együttható átlaga					**11,4**

3. SZ. MELLÉKLET

LŐRINCI GÁZTURBINÁS TARTALÉK ERŐMŰ FIZIKAI VÉDELMI RENDSZERE BIZTONSÁGI KOCKÁZATAIT KIÉRTÉKELŐ TÁBLÁZATOK

Veszélyek megnevezése	LŐRINCI		Kockázati érték	Létesítmény együttható	ÁTLAG
Működésből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**15**	
Black Start erőmű van a létesítményben	3	5	15		
Közismert a létesítményben folyó tevékenység	5	3	15		
Közismert a létesítményen belüli környezet, alkalmazott technológia	3	3	9		
Létesítményben több intézmény/társaság tevékenykedik	0	0	0		
Lehetséges lakossági tiltakozás, akár erőszakos formában is, a létesítményben végzett tevékenysége elleni	1	5	5		**10,9**
A létesítmény ellen elkövetendő terrortámadás reális veszély	3	5	15		
Nincsenek kidolgozott szabályzatok, rutinok a krízishelyzetek kezelésére (ÜFT; Pandémiás terv; stb.)	1	5	5		
Nincsenek a létesítmény működéséhez kidolgozott és hatályba helyezett biztonsági szabályzatok	1	5	5		
Létesítménybe ellenőrzés nélkül léphetnek személyek és/vagy vihetnek be- és ki csomagokat	4	5	20		
Meglévő porta, recepciós, őrszolgálat csomagokat átvehet, őrizhet, továbbíthat.	4	5	20		

Veszélyek megnevezése	LŐRINCI		Kockázati érték	Létesítmény együttható	ÁTLAG
Műszaki problémákból adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**15**	
Villamos energia kiesése (áramszünet)	3	5	15		
Közvilágítással, világítással kapcsolatos üzemszünet (látási problémák)	3	5	15		
Nincs önálló hálózat (más hálózattól fizikailag elválasztott) kiépítve a biztonságtechnikai rendszerek számára (DEPEDENCIA)	1	5	5		
Természeti csapás (műszaki problémákat generált) miatt a létesítmény üzeme akadozhat, akár le is állhat	3	5	15		
Kiépített biztonságtechnikai rendszerek nincsenek.	3	5	15		**14,2**
Vannak kiépített elektronikus biztonságtechnikai rendszerek, de nincs rendszeres karbantartás, a szükséges javítások nem készülnek el időben.	1	2	2		
Nincs, vagy nem megfelelő a kiépített szünetmentes berendezés, illetve hálózat a biztonságtechnikai rendszerek számára	1	5	5		
Létesítmény kerítéssel nem, vagy csak részben van elválasztva a környezetétől. A meglévő kerítés állapota nem megfelelő	5	4	20		
Meglévő biztonságtechnikai rendszerek üzemideje meghaladta a 10 évet, és/vagy a gyártói támogatás megszűnt.	5	5	25		
A létesítményben veszélyes kategóriájú technológiai, biztonsági szempontból kockázatos anyagokkal, folyamatok zajlanak.	5	5	25		

Veszélyek megnevezése	LŐRINCI		Kockázati érték	Létesítmény együttható	ÁTLAG
Bűnügyi fertőzöttségből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**15**	
Létesítmény környezetében a tulajdon ellen elkövetett cselekmények éves száma országos átlag, vagy az feletti	4	3	12		
Létesítményben végzett technológiai folyamatokat kurens (fekete gazdaság területén keresett és jól eladható) anyagokkal, szerszámokkal, gépekkel folytatnak.	4	3	12		
Társaság által használt gépkocsikban beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs	1	5	5		
Társaság által a technológiai folyamathoz használt gépjárművekben, gépekben beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs.	1	5	5		
Létesítményben élőerős őrzést nem alkalmaznak, a biztonságtechnikai rendszerek üzemeltetése a munkavállalók feladata.	0	0	0		**13,9**
Létesítményben élőerős biztonsági szolgálat működik, de járőrözés nincs, vagy nem megfelelően van szervezve.	5	5	25		
Létesítménybe történő be- és kiléptetés nem, vagy nem megfelelően szabályozott, illetve az nem a szabályok szerint történik	1	5	5		
Létesítmény fizikai védelmi rendszerében a mélységi védelem kaialkítása nincs, vagy nem megfelelő.	5	5	25		
Létesítmény fizikai védelmi rendszerében biztonsági zónák, területek nincsenek, vagy nem megfelelően vannak meghatározva.	5	5	25		
Létesítmény közvetlen környezet nem átlátható, nem gondozott, a telekhatárok, külterületi objektumok rejtve megközelíthetőek.	5	5	25		

Veszélyek megnevezése	LŐRINCI		Kockázati érték	Létesítmény együttható	ÁTLAG
Emberi munkavégzésből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**15**	
Az IT/ICT hálózat üzemeltetői a biztonságtechnikai hálózat üzemeltetői is egyben	1	5	5		
A biztonságtechnikai rendszerek felügyeletét szakmailag nem kompetens munkavállalóval látja el társaság	1	5	5		
Szabályzatokban rögzített folyamatok betartatása nem konzekvens.	1	5	5		
Biztonságtechnikai rendszerek karbantartását és javítását végző társaság munkavállalói munkavégzésének színvonala nem megfelelő	1	5	5		
Társaság biztonságtudatossági szintje nem ismert, vagy igen alacsony.	1	5	5		**4,5**
A be- és kiléptetésre, áruszállításokra vonatkozó szabályzatok nincsenek, vagy azok betartatása nem megfelelő részletességgel kidolgozottak.	1	5	5		
Biztonsági őrök tevékenységének ellenőrzöttsége, a munkavégzés szinvonala nem megfelelő.	0	0	0		
Meglévő fizikai védelmi rendszerek használtata nem napi rutin a társaság életében.	1	5	5		
Biztonsági rendszerek esemény- és hibaüzeneteire a társaság nem időben reagál.	1	5	5		
Biztonsági terület munkatársai képzése, továbbképzése nem megoldott.	1	5	5		
Kockázati együttható átlaga					**10,88**

4. SZ. MELLÉKLET

MVM ZRT. SZÉKHÁZA FIZIKAI VÉDELMI RENDSZERE BIZTONSÁGI KOCKÁZATAIT KIÉRTÉKELŐ TÁBLÁZATOK

Veszélyek megnevezése	MVM Zrt SZÉKHÁZ		Kockázati érték	Létesítmény együttható	ÁTLAG
Működésből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**25**	
Tevékenységből adódóan ügyfélfogadás van a létesítményben	5	3	15		
Közismert a létesítményben folyó tevékenység	4	5	20		
Közismert a létesítményen belüli környezet, alkalmazott technológia	5	5	25		
Létesítményben több intézmény/társaság tevékenykedik	5	3	15		
Lehetséges lakossági tiltakozás, akár erőszakos formában is, a létesítményben végzett tevékenysége elleni	4	3	12		**10,6**
A létesítmény ellen elkövetendő terrortámadás reális veszély	3	5	15		
Nincsenek kidolgozott szabályzatok, rutinok a krízishelyzetek kezelésére (ÜFT; Pandémiás terv; stb.)	1	1	1		
Nincsenek a létesítmény működéséhez kidolgozott és hatályba helyezett biztonsági szabályzatok	1	1	1		
Létesítménybe ellenőrzés nélkül léphetnek személyek és/vagy vihetnek be- és ki csomagokat	1	1	1		
Meglévő porta, recepciós, őrszolgálat csomagokat átvehet, őrizhet, továbbíthat.	1	1	1		

Veszélyek megnevezése	MVM Zrt SZÉKHÁZ		Kockázati érték	Létesítmény együttható	ÁTLAG
Műszaki problémákból adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**25**	
Villamos energia kiesése (áramszünet)	1	1	1		
Közvilágítással, világítással kapcsolatos üzemszünet (látási problémák)	1	1	1		
Nincs önálló hálózat (más hálózattól fizikailag elválasztott) kiépítve a biztonságtechnikai rendszerek számára (DEPEDENCIA)	1	1	1		
Természeti csapás (műszaki problémákat generált) miatt a létesítmény üzeme akadozhat, akár le is állhat	3	5	15		
Kiépített biztonságtechnikai rendszerek nincsenek.	0	0	0		**4,7**
Vannak kiépített elektronikus biztonságtechnikai rendszerek, de nincs rendszeres karbantartás, a szükséges javítások nem készülnek el időben.	1	1	1		
Nincs, vagy nem megfelelő a kiépített szünetmentes berendezés, illetve hálózat a biztonságtechnikai rendszerek számára	1	1	1		
Létesítmény kerítéssel nem, vagy csak részben van elválasztva a környezetétől. A meglévő kerítés állapota nem megfelelő	1	1	1		
Meglévő biztonságtechnikai rendszerek üzemideje meghaladta a 10 évet, és/vagy a gyártói támogatás megszűnt.	1	1	1		
A létesítményben veszélyes kategóriájú technológiai, biztonsági szempontból kockázatos anyagokkal, folyamatok zajlanak.	5	5	25		

Veszélyek megnevezése	MVM Zrt SZÉKHÁZ		Kockázati érték	Létesítmény együttható	ÁTLAG
Bűnügyi fertőzöttségből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**25**	
Létesítmény környezetében a tulajdon ellen elkövetett cselekmények éves száma országos átlag, vagy az feletti	3	3	9		
Létesítményben végzett technológiai folyamatokat kurens (fekete gazdaság területén keresett és jól eladható) anyagokkal, szerszámokkal, gépekkel folytatnak.	3	3	9		
Társaság által használt gépkocsikban beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs	1	5	5		
Társaság által a technológiai folyamathoz használt gépjárművekben, gépekben beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs.	1	5	5		
Létesítményben élőerős őrzést nem alkalmaznak, a biztonságtechnikai rendszerek üzemeltetése a munkavállalók feladata.	1	2	2		**3,8**
Létesítményben élőerős biztonsági szolgálat működik, de járőrözés nincs, vagy nem megfelelően van szervezve.	1	2	2		
Létesítménybe történő be- és kiléptetés nem, vagy nem megfelelően szabályozott, illetve az nem a szabályok szerint történik	1	1	1		
Létesítmény fizikai védelmi rendszerében a mélységi védelem kaialkítása nincs, vagy nem megfelelő.	1	2	2		
Létesítmény fizikai védelmi rendszerében biztonsági zónák, területek nincsenek, vagy nem megfelelően vannak meghatározva.	1	2	2		
Létesítmény közvetlen környezet nem átlátható, nem gondozott, a telekhatárok, külterületi objektumok rejtve megközelíthetőek.	1	1	1		

Veszélyek megnevezése	MVM Zrt SZÉKHÁZ		Kockázati érték	Létesítmény együttható	ÁTLAG
Emberi munkavégzésből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**25**	
Az IT/ICT hálózat üzemeltetői a biztonságtechnikai hálózat üzemeltetői is egyben	1	1	1		
A biztonságtechnikai rendszerek felügyeletét szakmailag nem kompetens munkavállalóval látja el társaság	1	1	1		
Szabályzatokban rögzített folyamatok betartatása nem konzekvens.	1	1	1		
Biztonságtechnikai rendszerek karbantartását és javítását végző társaság munkavállalói munkavégzésének színvonala nem megfelelő	1	1	1		
Társaság biztonságtudatossági szintje nem ismert, vagy igen alacsony.	2	3	6		**1,7**
A be- és kiléptetésre, áruszállításokra vonatkozó szabályzatok nincsenek, vagy azok betartatása nem megfelelő részletességgel kidolgozottak.	1	1	1		
Biztonsági őrök tevékenységének ellenőrzöttsége, a munkavégzés szinvonala nem megfelelő.	1	3	3		
Meglévő fizikai védelmi rendszerek használtata nem napi rutin a társaság életében.	1	1	1		
Biztonsági rendszerek esemény- és hibaüzeneteire a társaság nem időben reagál.	1	1	1		
Biztonsági terület munkatársai képzése, továbbképzése nem megoldott.	1	1	1		
Kockázati együttható átlaga					**5,2**

5. SZ. MELLÉKLET

PAKSI ATOMERŐMŰ FIZIKAI VÉDELMI RENDSZERE BIZTONSÁGI KOCKÁZATAIT KIÉRTÉKELŐ TÁBLÁZATOK

Veszélyek megnevezése	ATOMERŐMŰ		Kockázati érték	Létesítmény együttható	ÁTLAG
Működésből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**25**	
Tevékenységből adódóan vendégek fogadása (látogatók) van a létesítményben	5	3	15		
Közismert a létesítményben folyó tevékenység	5	5	25		
Közismert a létesítményen belüli környezet, alkalmazott technológia	5	5	25		
Létesítményben több intézmény/társaság tevékenykedik	0	0	0		
Lehetséges lakossági tiltakozás, akár erőszakos formában is, a létesítményben végzett tevékenysége elleni	3	4	12		11,2
A létesítmény ellen elkövetendő terrortámadás reális veszély	3	5	15		
Nincsenek kidolgozott szabályzatok, rutinok a krízishelyzetek kezelésére (ÜFT; Pandémiás terv; stb.)	1	5	5		
Nincsenek a létesítmény működéséhez kidolgozott és hatályba helyezett biztonsági szabályzatok	1	5	5		
Létesítménybe ellenőrzés nélkül léphetnek személyek és/vagy vihetnek be- és ki csomagokat	1	5	5		
Meglévő porta, recepciós, őrszolgálat csomagokat átvehet, őrizhet, továbbíthat.	1	5	5		

Veszélyek megnevezése	ATOMERŐMŰ		Kockázati érték	Létesítmény együttható	ÁTLAG
Műszaki problémákból adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**25**	
Villamos energia kiesése (áramszünet)	3	5	15		
Közvilágítással, világítással kapcsolatos üzemszünet (látási problémák)	3	5	15		
Nincs önálló hálózat (más hálózattól fizikailag elválasztott) kiépítve a biztonságtechnikai rendszerek számára (DEPEDENCIA)	1	1	1		
Természeti csapás (műszaki problémákat generált) miatt a létesítmény üzeme akadozhat, akár le is állhat	3	5	15		
Kiépített biztonságtechnikai rendszerek nincsenek.	1	1	1		8
Vannak kiépített elektronikus biztonságtechnikai rendszerek, de nincs rendszeres karbantartás, a szükséges javítások nem készülnek el időben.	1	1	1		
Nincs, vagy nem megfelelő a kiépített szünetmentes berendezés, illetve hálózat a biztonságtechnikai rendszerek számára	1	1	1		
Létesítmény kerítéssel nem, vagy csak részben van elválasztva a környezetétől. A meglévő kerítés állapota nem megfelelő	1	1	1		
Meglévő biztonságtechnikai rendszerek üzemideje meghaladta a 10 évet, és/vagy a gyártói támogatás megszűnt.	1	1	1		
A létesítményben veszélyes kategóriájú technológiai, biztonsági szempontból kockázatos anyagokkal, folyamatok zajlanak.	5	5	25		

Veszélyek megnevezése	ATOMERŐMŰ		Kockázati érték	Létesítmény együttható	ÁTLAG
Bűnügyi fertőzöttségből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**25**	
Létesítmény környezetében a tulajdon ellen elkövetett cselekmények éves száma országos átlag, vagy az feletti	1	3	3		
Létesítményben végzett technológiai folyamatokat kurens (fekete gazdaság területén keresett és jól eladható) anyagokkal, szerszámokkal, gépekkel folytatnak.	5	3	15		
Társaság által használt gépkocsikban beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs	1	3	3		
Társaság által a technológiai folyamathoz használt gépjárművekben, gépekben beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs.	1	3	3		
Létesítményben élőerős őrzést nem alkalmaznak, a biztonságtechnikai rendszerek üzemeltetése a munkavállalók feladata.	0	0	0		3
Létesítményben élőerős biztonsági szolgálat működik, de járőrözés nincs, vagy nem megfelelően van szervezve.	1	1	1		
Létesítménybe történő be- és kiléptetés nem, vagy nem megfelelően szabályozott, illetve az nem a szabályok szerint történik	1	1	1		
Létesítmény fizikai védelmi rendszerében a mélységi védelem kialakítása nincs, vagy nem megfelelő.	1	1	1		
Létesítmény fizikai védelmi rendszerében biztonsági zónák, területek nincsenek, vagy nem megfelelően vannak meghatározva.	1	1	1		
Létesítmény közvetlen környezet nem átlátható, nem gondozott, a telekhatárok, külterületi objektumok rejtve megközelíthetőek.	1	3	3		

Veszélyek megnevezése	ATOMERŐMŰ		Kockázati érték	Létesítmény együttható	ÁTLAG
Emberi munkavégzésből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**25**	
Az IT/ICT hálózat üzemeltetői a biztonságtechnikai hálózat üzemeltetői is egyben	1	1	1		
A biztonságtechnikai rendszerek felügyeletét szakmailag nem kompetens munkavállalóval látja el társaság	1	1	1		
Szabályzatokban rögzített folyamatok betartatása nem konzekvens.	1	1	1		
Biztonságtechnikai rendszerek karbantartását és javítását végző társaság munkavállalói munkavégzésének színvonala nem megfelelő	1	1	1		
Társaság biztonságtudatossági szintje nem ismert, vagy igen alacsony.	1	1	1		1
A be- és kiléptetésre, áruszállításokra vonatkozó szabályzatok nincsenek, vagy azok betartatása nem megfelelő részletességgel kidolgozottak.	1	1	1		
Biztonsági őrök tevékenységének ellenőrzöttsége, a munkavégzés szinvonala nem megfelelő.	1	1	1		
Meglévő fizikai védelmi rendszerek használtata nem napi rutin a társaság életében.	1	1	1		
Biztonsági rendszerek esemény- és hibaüzeneteire a társaság nem időben reagál.	1	1	1		
Biztonsági terület munkatársai képzése, továbbképzése nem megoldott.	1	1	1		
Kockázati együttható átlaga					**6**

6. SZ. MELLÉKLET

GÖDI ADATKÖZPONT TERVEZETT FIZIKAI VÉDELMI RENDSZERE BIZTONSÁGI KOCKÁZATAIT KIÉRTÉKELŐ TÁBLÁZATOK

Veszélyek megnevezése	ADATKÖZPONT		Kockázati érték	Létesítmény együttható	ÁTLAG
Működésből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**16**	
Tevékenységből adódóan vendégek fogadása (látogatók) van a létesítményben	5	3	15		
Közismert a létesítményben folyó tevékenység	5	5	25		
Közismert a létesítményen belüli környezet, alkalmazott technológia	5	5	25		
Létesítményben több intézmény/társaság tevékenykedik	0	0	0		
Lehetséges lakossági tiltakozás, akár erőszakos formában is, a létesítményben végzett tevékenysége elleni	1	2	2		8,6
A létesítmény ellen elkövetendő terrortámadás reális veszély	3	5	15		
Nincsenek kidolgozott szabályzatok, rutinok a krízishelyzetek kezelésére (ÜFT; Pandémiás terv; stb.)	1	1	1		
Nincsenek a létesítmény működéséhez kidolgozott és hatályba helyezett biztonsági szabályzatok	1	1	1		
Létesítménybe ellenőrzés nélkül léphetnek személyek és/vagy vihetnek be- és ki csomagokat	1	1	1		
Meglévő porta, recepciós, őrszolgálat csomagokat átvehet, őrizhet, továbbíthat.	1	1	1		

Veszélyek megnevezése	ADATKÖZPONT		Kockázati érték	Létesítmény együttható	ÁTLAG
Műszaki problémákból adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**16**	
Villamos energia kiesése (áramszünet)	2	5	10		
Közvilágítással, világítással kapcsolatos üzemszünet (látási problémák)	2	5	10		
Nincs önálló hálózat (más hálózattól fizikailag elválasztott) kiépítve a biztonságtechnikai rendszerek számára (DEPEDENCIA)	1	1	1		
Természeti csapás (műszaki problémákat generált) miatt a létesítmény üzeme akadozhat, akár le is állhat	3	5	15		
Kiépített biztonságtechnikai rendszerek nincsenek.	0	0	0		4,1
Vannak kiépített elektronikus biztonságtechnikai rendszerek, de nincs rendszeres karbantartás, a szükséges javítások nem készülnek el	1	1	1		
Nincs, vagy nem megfelelő a kiépített szünetmentes berendezés, illetve hálózat a biztonságtechnikai rendszerek számára	1	1	1		
Létesítmény kerítéssel nem, vagy csak részben van elválasztva a környezetétől. A meglévő kerítés állapota nem megfelelő	1	1	1		
Meglévő biztonságtechnikai rendszerek üzemideje meghaladta a 10 évet, és/vagy a gyártói támogatás megszűnt.	1	1	1		
A létesítményben veszélyes kategóriájú technológiai, biztonsági szempontból kockázatos anyagokkal, folyamatok zajlanak.	1	1	1		

Veszélyek megnevezése	ADATKÖZPONT		Kockázati érték	Létesítmény együttható	ÁTLAG
Bűnügyi fertőzöttségből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**16**	
Létesítmény környezetében a tulajdon ellen elkövetett cselekmények éves száma országos átlag, vagy az feletti	1	3	3		
Létesítményben végzett technológiai folyamatokat kurens (fekete gazdaság területén keresett és jól eladható) anyagokkal, szerszámokkal, gépekkel folytatnak.	5	5	25		
Társaság által használt gépkocsikban beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs	1	3	3		
Társaság által a technológiai folyamathoz használt gépjárművekben, gépekben beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs.	1	3	3		
Létesítményben élőerős őrzést nem alkalmaznak, a biztonságtechnikai rendszerek üzemeltetése a munkavállalók feladata.	0	0	0		**3,9**
Létesítményben élőerős biztonsági szolgálat működik, de járőrözés nincs, vagy nem megfelelően van szervezve.	1	1	1		
Létesítménybe történő be- és kiléptetés nem, vagy nem megfelelően szabályozott, illetve az nem a szabályok szerint történik	1	1	1		
Létesítmény fizikai védelmi rendszerében a mélységi védelem kaialkítása nincs, vagy nem megfelelő.	1	1	1		
Létesítmény fizikai védelmi rendszerében biztonsági zónák, területek nincsenek, vagy nem megfelelően vannak meghatározva.	1	1	1		
Létesítmény közvetlen környezet nem átlátható, nem gondozott, a telekhatárok, külterületi objektumok rejtve megközelíthetőek.	1	1	1		

Veszélyek megnevezése	ADATKÖZPONT		Kockázati érték	Létesítmény együttható	ÁTLAG
Emberi munkavégzésből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**16**	
Az IT/ICT hálózat üzemeltetői a biztonságtechnikai hálózat üzemeltetői is egyben	1	1	1		
A biztonságtechnikai rendszerek felügyeletét szakmailag nem kompetens munkavállalóval látja el társaság	1	1	1		
Szabályzatokban rögzített folyamatok betartatása nem konzekvens.	1	1	1		
Biztonságtechnikai rendszerek karbantartását és javítását végző társaság munkavállalói munkavégzésének színvonala nem megfelelő	1	1	1		
Társaság biztonságtudatossági szintje nem ismert, vagy igen alacsony.	1	1	1		**1**
A be- és kiléptetésre, áruszállításokra vonatkozó szabályzatok nincsenek, vagy azok betartatása nem megfelelő részletességgel	1	1	1		
Biztonsági őrök tevékenységének ellenőrzöttsége, a munkavégzés szinvonala nem megfelelő.	1	1	1		
Meglévő fizikai védelmi rendszerek használtata nem napi rutin a társaság életében.	1	1	1		
Biztonsági rendszerek esemény- és hibaüzeneteire a társaság nem időben reagál.	1	1	1		
Biztonsági terület munkatársai képzése, továbbképzése nem megoldott.	1	1	1		
Kockázati együttható átlaga					**4,4**

7. SZ. MELLÉKLET

HOTEL PANORÁMA VAGYONVÉDELMI RENDSZERE BIZTONSÁGI KOCKÁZATAIT KIÉRTÉKELŐ TÁBLÁZATOK

Veszélyek megnevezése	HOTEL PANORÁMA		Kockázati érték	Létesítmény együttható	ÁTLAG
Működésből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**4**	
Tevékenységből adódóan vendégek fogadása (látogatók) van a létesítményben	1	1	**1**		
Közismert a létesítményben folyó tevékenység	3	1	3		
Közismert a létesítményen belüli környezet, alkalmazott technológia	3	1	3		
Létesítményben több intézmény/társaság tevékenykedik	0	0	0		
Lehetséges lakossági tiltakozás, akár erőszakos formában is, a létesítményben végzett tevékenysége elleni	0	0	0		**1**
A létesítmény ellen elkövetendő terrortámadás reális veszély	0	0	0		
Nincsenek kidolgozott szabályzatok, rutinok a krízishelyzetek kezelésére (ÜFT; Pandémiás terv; stb.)	1	3	3		
Nincsenek a létesítmény működéséhez kidolgozott és hatályba helyezett biztonsági szabályzatok	1	1	**1**		
Létesítménybe ellenőrzés nélkül léphetnek személyek és/vagy vihetnek be- és ki csomagokat	1	1	**1**		
Meglévő porta, recepciós, őrszolgálat csomagokat átvehet, őrizhet, továbbíthat.	1	1	**1**		

Veszélyek megnevezése	HOTEL PANORÁMA		Kockázati érték	Létesítmény együttható	ÁTLAG
Műszaki problémákból adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**4**	
Villamos energia kiesése (áramszünet)	1	1	**1**		
Közvilágítással, világítással kapcsolatos üzemszünet (látási problémák)	2	1	**2**		
Nincs önálló hálózat (más hálózattól fizikailag elválasztott) kiépítve a biztonságtechnikai rendszerek számára (DEPEDENCIA)	1	1	**1**		
Természeti csapás (műszaki problémákat generált) miatt a létesítmény üzeme akadozhat, akár le is állhat	2	1	**2**		
Kiépített biztonságtechnikai rendszerek nincsenek.	1	2	**2**		**2**
Vannak kiépített elektronikus biztonságtechnikai rendszerek, de nincs rendszeres karbantartás, a szükséges javítások nem készülnek el időben.	1	3	3		
Nincs, vagy nem megfelelő a kiépített szünetmentes berendezés, illetve hálózat a biztonságtechnikai rendszerek számára	1	3	3		
Létesítmény kerítéssel nem, vagy csak részben van elválasztva a környezetétől. A meglévő kerítés állapota nem megfelelő	1	1	**1**		
Meglévő biztonságtechnikai rendszerek üzemideje meghaladta a 10 évet, és/vagy a gyártói támogatás megszűnt.	3	1	3		
A létesítményben veszélyes kategóriájú technológiai, biztonsági szempontból kockázatos anyagokkal, folyamatok zajlanak.	1	1	**1**		

Veszélyek megnevezése	HOTEL PANORÁMA		Kockázati érték	Létesítmény együttható	ÁTLAG
Bűnügyi fertőzöttségből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**4**	
Létesítmény környezetében a tulajdon ellen elkövetett cselekmények éves száma országos átlag, vagy az feletti	1	3	3		
Létesítményben végzett technológiai folyamatokat kurens (fekete gazdaság területén keresett és jól eladható) anyagokkal, szerszámokkal, gépekkel folytatnak.	1	1	**1**		
Társaság által használt gépkocsikban beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs	3	2	6		
Társaság által a technológiai folyamathoz használt gépjárművekben, gépekben beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs.	3	2	6		
Létesítményben élőerős őrzést nem alkalmaznak, a biztonságtechnikai rendszerek üzemeltetése a munkavállalók feladata.	5	2	10		**4,1**
Létesítményben élőerős biztonsági szolgálat működik, de járőrözés nincs, vagy nem megfelelően van szervezve.	1	1	**1**		
Létesítménybe történő be- és kiléptetés nem, vagy nem megfelelően szabályozott, illetve az nem a szabályok szerint történik	1	1	**1**		
Létesítmény fizikai védelmi rendszerében a mélységi védelem kaialkítása nincs, vagy nem megfelelő.	5	1	5		
Létesítmény fizikai védelmi rendszerében biztonsági zónák, területek nincsenek, vagy nem megfelelően vannak meghatározva.	5	1	5		
Létesítmény közvetlen környezet nem átlátható, nem gondozott, a telekhatárok, külterületi objektumok rejtve megközelíthetőek.	1	1	3		

Veszélyek megnevezése	HOTEL PANORÁMA		Kockázati érték	Létesítmény együttható	ÁTLAG
Emberi munkavégzésből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**4**	
Az IT/ICT hálózat üzemeltetői a biztonságtechnikai hálózat üzemeltetői is egyben	1	1	**1**		
A biztonságtechnikai rendszerek felügyeletét szakmailag nem kompetens munkavállalóval látja el társaság	1	1	**1**		
Szabályzatokban rögzített folyamatok betartatása nem konzekvens.	1	1	**1**		
Biztonságtechnikai rendszerek karbantartását és javítását végző társaság munkavállalói munkavégzésének színvonala nem megfelelő	1	1	**1**		
Társaság biztonságtudatossági szintje nem ismert, vagy igen alacsony.	1	3	3		**1**
A be- és kiléptetésre, áruszállításokra vonatkozó szabályzatok nincsenek, vagy azok betartatása nem megfelelő részletességgel kidolgozottak.	1	1	**1**		
Biztonsági őrök tevékenységének ellenőrzöttsége, a munkavégzés szinvonala nem megfelelő.	0	5	0		
Meglévő fizikai védelmi rendszerek használtata nem napi rutin a társaság életében.	1	3	3		
Biztonsági rendszerek esemény- és hibaüzeneteire a társaság nem időben reagál.	1	1	**1**		
Biztonsági terület munkatársai képzése, továbbképzése nem megoldott.	1	1	**1**		
Kockázati együttható átlaga					**2**

8. SZ. MELLÉKLET

DUNA CSÓNAKHÁZ VAGYONVÉDELMI RENDSZERE BIZTONSÁGI KOCKÁZATAIT KIÉRTÉKELŐ TÁBLÁZATOK

Veszélyek megnevezése	DUNA CSÓNAKHÁZ		Kockázati érték	Létesítmény együttható	ÁTLAG
Működésből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**1**	
Tevékenységből adódóan vendégek fogadása (látogatók) van a létesítményben	1	1	**1**		
Közismert a létesítményben folyó tevékenység	3	1	3		
Közismert a létesítményen belüli környezet, alkalmazott technológia	3	1	3		
Létesítményben több intézmény/társaság tevékenykedik	0	0	0		
Lehetséges lakossági tiltakozás, akár erőszakos formában is, a létesítményben végzett tevékenysége elleni	0	0	0		**2**
A létesítmény ellen elkövetendő terrortámadás reális veszély	0	0	0		
Nincsenek kidolgozott szabályzatok, rutinok a krízishelyzetek kezelésére (ÜFT; Pandémiás terv; stb.)	1	3	3		
Nincsenek a létesítmény működéséhez kidolgozott és hatályba helyezett biztonsági szabályzatok	1	3	3		
Létesítménybe ellenőrzés nélkül léphetnek személyek és/vagy vihetnek be- és ki csomagokat	1	1	**1**		
Meglévő porta, recepciós, őrszolgálat csomagokat átvehet, őrizhet, továbbíthat.	1	1	**1**		

Veszélyek megnevezése	DUNA CSÓNAKHÁZ		Kockázati érték	Létesítmény együttható	ÁTLAG
Műszaki problémákból adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**1**	
Villamos energia kiesése (áramszünet)	1	1	**1**		
Közvilágítással, világítással kapcsolatos üzemszünet (látási problémák)	1	1	**1**		
Nincs önálló hálózat (más hálózattól fizikailag elválasztott) kiépítve a biztonságtechnikai rendszerek számára (DEPEDENCIA)	1	1	**1**		
Természeti csapás (műszaki problémákat generált) miatt a létesítmény üzeme akadozhat, akár le is állhat	2	1	**2**		
Kiépített biztonságtechnikai rendszerek nincsenek.	1	1	**1**		**1**
Vannak kiépített elektronikus biztonságtechnikai rendszerek, de nincs rendszeres karbantartás, a szükséges javítások nem készülnek el időben.	1	1	**1**		
Nincs, vagy nem megfelelő a kiépített szünetmentes berendezés, illetve hálózat a biztonságtechnikai rendszerek számára	1	1	**1**		
Létesítmény kerítéssel nem, vagy csak részben van elválasztva a környezetétől. A meglévő kerítés állapota nem megfelelő	1	1	**1**		
Meglévő biztonságtechnikai rendszerek üzemideje meghaladta a 10 évet, és/vagy a gyártói támogatás megszűnt.	3	1	3		
A létesítményben veszélyes kategóriájú technológiai, biztonsági szempontból kockázatos anyagokkal, folyamatok zajlanak.	1	1	**1**		

Veszélyek megnevezése	DUNA CSÓNAKHÁZ		Kockázati érték	Létesítmény együttható	ÁTLAG
Bűnügyi fertőzöttségből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**1**	
Létesítmény környezetében a tulajdon ellen elkövetett cselekmények éves száma országos átlag, vagy az feletti	1	3	3		
Létesítményben végzett technológiai folyamatokat kurens (fekete gazdaság területén keresett és jól eladható) anyagokkal, szerszámokkal, gépekkel folytatnak.	1	1	**1**		
Társaság által használt gépkocsikban beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs	0	0	0		
Társaság által a technológiai folyamathoz használt gépjárművekben, gépekben beépített GPS nyomkövetővel működtetett biztonsági rendszer nincs.	0	0	0		
Létesítményben élőerős őrzést nem alkalmaznak, a biztonságtechnikai rendszerek üzemeltetése a munkavállalók feladata.	1	1	**1**		**2**
Létesítményben élőerős biztonsági szolgálat működik, de járőrözés nincs, vagy nem megfelelően van szervezve.	0	0	0		
Létesítménybe történő be- és kiléptetés nem, vagy nem megfelelően szabályozott, illetve az nem a szabályok szerint történik	1	1	**1**		
Létesítmény fizikai védelmi rendszerében a mélységi védelem kaialkítása nincs, vagy nem megfelelő.	5	1	5		
Létesítmény fizikai védelmi rendszerében biztonsági zónák, területek nincsenek, vagy nem megfelelően vannak meghatározva.	5	1	5		
Létesítmény közvetlen környezet nem átlátható, nem gondozott, a telekhatárok, külterületi objektumok rejtve megközelíthetőek.	1	1	3		

Veszélyek megnevezése	DUNA CSÓNAKHÁZ		Kockázati érték	Létesítmény együttható	ÁTLAG
Emberi munkavégzésből adódó biztonsági kockázatok	**ESÉLY**	**HATÁS**		**1**	
Az IT/ICT hálózat üzemeltetői a biztonságtechnikai hálózat üzemeltetői is egyben	1	1	**1**		
A biztonságtechnikai rendszerek felügyeletét szakmailag nem kompetens munkavállalóval látja el társaság	1	1	**1**		
Szabályzatokban rögzített folyamatok betartatása nem konzekvens.	1	1	**1**		
Biztonságtechnikai rendszerek karbantartását és javítását végző társaság munkavállalói munkavégzésének színvonala nem megfelelő	1	1	**1**		
Társaság biztonságtudatossági szintje nem ismert, vagy igen alacsony.	1	3	3		**1**
A be- és kiléptetésre, áruszállításokra vonatkozó szabályzatok nincsenek, vagy azok betartatása nem megfelelő részletességgel kidolgozottak.	1	1	**1**		
Biztonsági őrök tevékenységének ellenőrzöttsége, a munkavégzés szinvonala nem megfelelő.	0	5	0		
Meglévő fizikai védelmi rendszerek használtata nem napi rutin a társaság életében.	1	3	3		
Biztonsági rendszerek esemény- és hibaüzeneteire a társaság nem időben reagál.	1	1	**1**		
Biztonsági terület munkatársai képzése, továbbképzése nem megoldott.	1	1	**1**		
Kockázati együttható átlaga					**2**

9. SZ. MELLÉKLET

DETEKTÁLÁSI VALÓSZÍNŰSÉG, KÜLÖNFÉLE ÉRZÉKELŐK ÉS BEHATOLÓ FELSZERELTSÉG MELLETT

Adattartalom átvéve: IAEA International Training Course on the Physical Protection of Nuclear Material and Nuclear Facilities (2016. november 11-22.), Albuquerque, NM; USA [10]

Érzékelő tipusa	Érézkelési rendszer megnevezése	Behatolási kísérlet módja				
		Eszközök nélkül (P_D)	Szerszámokkal		Robbanó-anyaggal (P_D)	Gépjárművel (P_D)
			Kézi (P_D)	Elektromos (P_D)		
Kültéri érzékelők	Szezmikus érzékelő földalatti kábel	0,50	0,50	0,50	0,50	0,90
	Elektronos-tér érzékelő	0,50	0,30	0,30	0,50	0,90
	Infravörös érzékelő	0,80	0,40	0,40	0,50	0,80
	Mikrohullámú érzékelő	0,80	0,70	0,70	0,70	0,90
	Videó mozgásérzékelő	0,80	0,60	0,60	0,70	0,90
	Egymás nem kiegészítő érzékelők	0,90	0,80	0,80	0,80	0,99
	Egymást kiegészítő érzékelők	0,99	0,95	0,95	0,99	0,99
Beltéri érzékelők	Akusztikus érzékelő	0,50	0,50	0,50	0,50	Nincs adat
	Kapacitví érzékelő	0,50	0,50	0,50	0,50	Nincs adat
	Vodeó mozgásérzékelő	0,50	0,50	0,50	0,50	Nincs adat
	Infravörös érzékelő	0,50	0,50	0,50	0,50	Nincs adat
	Mikrohullámú érzékelő	0,50	0,50	0,50	0,50	Nincs adat
	Videó mozgásérzékelő	0,50	0,50	0,50	0,50	Nincs adat
	Egymás nem kiegészítő érzékelők	0,75	0,75	0,75	0,75	Nincs adat
	Egymást kiegészítő érzékelők	0,90	0,90	0,90	0,90	Nincs adat
Helyzetérzékelők	Állapotkapcsoló	0,50	0,20	0,20	0,20	Nincs adat
	Kiegészített mágneses kapcsoló	0,80	0,80	0,80	0,80	Nincs adat
Kerítésre telepíthető érzékelők	Megfeszített kábeles érzékelő	0,50	0,25	0,25	0,75	0,85
	Rezgésérzékelő	0,50	0,10	0,10	0,75	0,85
	Deformáció érzékelő	0,10	0,10	0,10	0,10	0,90
	Elektromos-tér érzékelő	0,50	0,40	0,40	0,75	0,90
	Többszörözött érzékelők	0,75	0,50	0,50	0,80	0,90
Sorompóként használatos szernzorok	Rezgésérzékelő	0,90	0,40	0,40	0,90	Nincs adat
	Üvegtörés érzékelő	0,90	0,60	0,60	0,90	Nincs adat
	Vezetőszalagos érzékelő	0,80	0,20	0,20	0,90	Nincs adat
	Rácshálózat	0,90	0,60	0,60	0,95	Nincs adat
	Többszörözött érzékelők	0,99	0,90	0,90	0,95	Nincs adat
Helikopteren telepítrett érzékelők	Radar technológiát alkalmazó érzékelő	0,10				
	Akusztikus érzéeklő	0,10				

FOGALOMTÁR A FIZIKAI BIZTONSÁG TÉMAKÖRÉHEZ

Ajtóvezérlő

Az a beléptető rendszer működése szempontjából igen fontos szünetmentes tápegységgel is ellátott rendszerelem, amely a beolvasott azonosítók kódolt továbbítását a vezérlő szerver felé biztosítja, illetve kapcsolat megszakadása esetén azok feldolgozását elvégzi, majd sikeres ellenőrzést követően az általa vezérelt ajtót naplózott módon nyitja, vagy éppen blokkolja, és erről (megfelelő konfiguráció esetén) az olvasó terminálon keresztül információt nyújthat a belépni szándékozó részére.

Behatolásjelző rendszer

Az biztonságtechnikai berendezés, amelye a védett területre történő, az érvényben lévő rezsim intézkedéseket figyelmen kívül hagyó, illetve illetéktelen személy belépését az előre beállított feltételek szerint jelzi, arról meghatározott személyek, a kezelő személyzet, és/vagy a távfelügyeleti központ részére információt, illetve különböző berendezések, beavatkozó egységes, alrendszerek részére jeleket (indító impulzus - trigger) biztosít. A kiépítettség, lefedettség szintje minden esetben a védett létesítmény, objektum biztonsági kockázatától, az tulajdonos és/vagy az üzemeltető információ igényétől függ.

Belépőkártya

A telepített beléptető rendszer azonosításra használt birtoklás alapú eszköze a belépőkártya, amelyet az adott létesítmény belső szabályozói szerint megszemélyesítéssel látunk el.

Beléptető rendszer

Beléptető rendszernek nevezzük azokat az elsődleges intézkedéseket, amelyek a védett létesítménybe történő belépést a belépési jogosultság ellenőrzésével lehetővé teszik. Az elsődleges intézkedéseket az adott, védendő létesítmény számára az Objektumvédelmi Terv részletezi. A fizikai védelem tekintetében a beléptető rendszer első lépcsője az elektronikus beléptető rendszer, amely valamilyen jellemző, vagy jellemzők együttesét ellenőrzi.

Biztonság fogalma

A biztonság egy olyan pillanatnyi helyzet, illetve relatív állapot, amikor az adott védendő létesítmény, objektum normál, üzemszerű működést semmilyen külső, vagy belső veszély nem fenyegeti, vagy a veszélyeztetettség szintje az elfogadott határok között tartható.

Csapdaszerű védelem

Csapdaszerű védelemről akkor beszélünk, ha a telepített behatolásjelző rendszer oly módon kerül tervezésre, telepítésre, hogy az engedély nélküli behatoló az egyes, az épületet határoló helyiségekbe jelzés kiváltás nélkül beléphet, de a helyiségekből történő kilépés már érzékelőkkel védett területre történik (például az épület emeleti folyosója érzékelőkkel védett, de az egyes helyiségben érzékelő nem kerül telepítésre). A csapdaszerű védelem részleges védelemnek minősül.

Digitális Videó Rögzítő (DVR)

Általánosan analóg kamera jeleket fogadó képfelvevő berendezés, amely az archivált képeket digitális formában, háttértárakon, merevlemezeken tárolja.

Dome kamera

Azokat a kamerákat, amelyek gyártásban egy félgömbszerű házban kerülnek telepítésre Dome kamerának nevezzük.

Egységes Beléptető Rendszer (EBR)

Az MVM Csoport környezetében az Egységes Beléptető Rendszer az országos biztonságtechnikai hálózat alaprendszerét biztosító kártyás beléptető rendszer elnevezése. Az EBR informatikai alaphálózata egy minden IT hálózattól fizikailag is elválasztott rendszer, amely IT hálózat valamennyi, az MVM Csoportban alkalmazott biztonságtechnikai rendszer alaphálózatát képezi.

Élőerős védelem

Az *objektumvédelem* egyik meghatározó területe, amikor a védett létesítménybe történő jogszerű, be-, illetve kilépés ellenőrzését, annak biztosítását szakképzett biztonsági őrök végzik.

Fedővédelem

Fedővédelemnek nevezzük azt a biztonságtechnikában gyakran alkalmazott rendszerkialakítási módot, amikor egy adott védelmi megoldást egy második, tőle lehetőleg technológiában is különböző, védelmi módszert is alkalmazunk.

Forgókereszt (Forgóvilla)

Azt az elektromechanikus rendszerelemet, amely biztosítja, hogy egy személy belépési jogosultsága ellenőrzését követően lehetővé teszi annak belépését forgókeresztnek, vagy forgóvillának (teljes magasságú, nem átmászható kivitel) nevezzük.

Hangjelző (Hangjelzés)

Olyan, többek között a biztonságtechnikában széles körben alkalmazott eszköz, amely meghatározott körülmények között, a központi egység konfigurációjának megfelelően hangjelzést, esetlegesen különböző hangjelzéseket képes szolgáltatni. A kialakításának megfelelően saját szünetmentes tápellátással is rendelkezhet.

Hőkamera

Azokat a kamerákat, amelyek az emberi szem számára nem látható 6-12 μm hullámhossztartományban működő, az emberi test, járművek hősugárzását érzékelő kamera, amely képelemző program segítségével rossz látási viszonyok között is képes az emberi, járműmozgások detektálásra, megjelenítésére.

Infra sorompó

Olyan, többek között a biztonságtechnikában széles körben alkalmazott eszköz, amely meghatározott körülmények között, és az adott egységre jellemző beállításoknak megfelelően a rendszer központi egysége részére képes jelzést szolgáltatni. Működéséhez különböző mennyiségű, irányítottságú infra tartományú fókuszált sugarat használ.

IP alapú rendszer

Akkor beszélünk IP alapú videó rendszerről, rendszerelemről, amikor a kameraképeket szabványos TCP/IP protokoll szerint átalakítást követően juttatják el központi egységre. Az adatkommunikáció formáját ez határozza meg.

Kamera

A videó technikai rendszerek egyik alapeleme, amely képes a képfelvevő elemére érkező jelek megfelelő átalakításra és továbbításra a központi egysége felé.

Kerítésvédelem

Kerítésvédelemről akkor beszélhetünk, amikor a létesítmény mechanikai védelmét ellátó telepített kerítésen történő áthatolás, vagy annak kísérlete esetén (meghatározott biztonsági kockázatok meglétekor már a megközelítéskor is) biztonságtechnikai rendszerközpont, esetleg központok számára az jelzést biztosít.

Kezelőegység

Olyan, többek között a biztonságtechnikában széles körben alkalmazott eszköz, amely segítségével a hozzá kapcsolt központi egység számára kódok, parancsok beadása lehetséges, illetve a kijelzőjén keresztül a rendszer üzemállapotairól – a központi egységben beépített jogosultság kezelő algoritmusok szerint - információkat képes szolgáltatni.

Kültéri védelem

Kültéri védelemnek nevezzük a biztonságtechnikai rendszerekből, alrendszerekből kialakított védelmi megoldásokat, amikor valamennyi védett terület, esetleg felület nem zárt térben található. A telepített rendszerelemek kiválasztásánál, azok telepítési módjánál az időjárási körülmények meghatározó szerepet játszanak.

Mechanikai védelem

Azokat a védelmi intézkedéseket, amelyek a védett létesítménybe, védett épületben, épületrészbe, vagy helyiségbe történő ellenőrzött bejutást mechanikai eszközökkel (rács, kerítés, falazatok, nyílászárók, stb.) szabályozzák, korlátozzák, vagy éppen megakadályozzák, mechanikai védelemnek nevezzük.

Mikrohullámú sorompó

Olyan, többek között a biztonságtechnikában széles körben alkalmazott eszköz, amely meghatározott körülmények között, és az adott egységre jellemző beállításoknak megfelelően a rendszer központi egysége részére képes jelzést szolgáltatni. Működéséhez különböző mennyiségű, irányítottságú mikrohullámú tartományú sugárzást használ.

Monitor

A kamerák által továbbított, illetve a már archivált képek megtekintését biztosító berendezés. A monitorfal több monitor modulból a gyártó által összeépített, hozzá való megjelenítést biztosító eszközöket, berendezéseket is tartalmazó képmegjelenítő, amely megjelenítő felülete, a konfigurációnak megfelelően használható.

Mozgásérzékelő

Olyan, többek között a biztonságtechnikában széles körben alkalmazott eszköz, amely meghatározott körülmények (érzékelési technológiának, kialakítási módjának megfelelően) között képes az érzékelő által lefedett területen belül megjelenő emberek mozgását egy központi egység számára jelezni.

Nyitásérzékelő

Olyan, többek között a biztonságtechnikában széles körben alkalmazott eszköz, amely a kialakításánál, működésénél, felszerelési módjától fogva képes nyílászárók, szekrények, egyedi módon nyíló, záródó felületek pillanatnyi állapotáról egy központi egység számára jelzést biztosítani.

Objektumvédelem

Azon intézkedések összessége, amelyek a védendő objektum biztonsági helyzetét biztosítva a nem várt, a védett létesítmény biztonságát befolyásoló események bekövetkezését akadályozzák, bekövetkezés esetén az okozott károk hatásait mérsékelik, a létesítmény üzemszerű működésének helyreállítását a lehető legrövidebb időn belül biztosítják.

Olvasó (terminál)

Azokat a technikai eszközöket, amelyek a telepített beléptető rendszer által elfogadható elsődleges azonosító adatok rendszerbe történő beolvasását végzik.

Optika

A kamera látószögét alapvetően befolyásoló eszköz, amely a beállításnak megfelelő irányból és képkivágásból a fényt a kamerában lévő képfelvevő elemre juttatja.

Optikai kábel

Olyan jelátviteli kábel, amely mind az analóg, mind a digitális jelek továbbítására alkalmas. Az elektronikus jelek (pl. videó képek) átalakítást követően fényimpulzusok formájában haladnak a rendszerint üvegből, illetve műanyagból készült kábelen.

Partíció

Egy behatolás-jelző rendszer logikailag kialakított alegysége, amely a felhasználó számára önálló behatolásjelző alrendszerként működtethető.

PIN kód tasztatúra

Kódtasztatúrának nevezzük azt a biztonságtechnikai rendszerelemet, amely segítéségével előre meghatározott, adatbázisban őrzött kódok, mint azonosító elemek vihetők be a beléptető rendszerbe.

PTZ kamera

PTZ a Pan-Tilt-Zoom (fordul-bólint-zoomol) funkciókból adódó, a távvezérelhető, nem Dome kialakítású kamerák esetében használatos elnevezés. Fontos megjegyezni, hogy a kamerákat ilyen módon telepített berendezés esetében a vízszintes szint fölé is pozícionálhatók.

Rezgésérzékelő

Olyan, többek között a biztonságtechnikában széles körben alkalmazott eszköz, amely meghatározott körülmények között képes a környezetében megjelenő rezgéseket, vibrációkat egy központi egység számára jelezni.

Szabotázsvédett (szerelési mód)

Szabotázsvédett szerelési módról akkor beszélhetünk, amikor a telepített biztonságtechnikai rendszer valamennyi rendszereleme olyan módon került beépítésre, hogy annak bármilyen jellegű manipulálása, illetve annak kísérlete legalább a központi oldalon szabotázsjelzést generál.

Switch

Az informatikai hálózatok egyik alapeleme, amely aktív elemként képes különböző rácsatlakoztatott eszközök között az adatáramlást biztosítani.

Távfelügyelet

Távfelügyeleti (riasztás vételi) rendszerről akkor beszélhetünk, ha a telepített behatolásjelző rendszer jelzése esetén a távfelügyeletet üzemeltető társaság a berendezés jelzéséről elektronikus úton információt kap, majd az elsődleges intézkedéseket megteszi.

Távvezérlő

A távvezérelhető kamerák mozgatását, a teljes rendszer vezérlését ellátni képes eszköz, amelylyel az élő képek közötti váltásra, az archivált anyagok visszanézésére, stb. alkalmas.

Teljes körű védelem

Teljes körű védelemről akkor beszélünk, ha a védendő építménybe, illetve létesítménybe tervezett, illetve telepített behatolásjelző rendszer az épület, létesítmény valamennyi, a külvilággal határos helyisége védett, azokba felület és/vagy térvédelem céljából érzékelőket tervezünk, és telepítünk. A helyiségek bármelyikébe történő szabályszerű belépés kizárólag a behatolásjelző rendszer részleges, vagy teljes kikapcsolása esetén lehetséges. Kialakításnak megfelelően beszélhetünk teljes körű felület, vagy térvédelemről, illetve egyéb fizikai védelmet is integráló rendszer esetén komplex védelemről.

Térvédelem

Térvédelemről akkor beszélhetünk, amikor a tervezett, vagy telepített biztonságtechnikai rendszer rendszerelemei a védett területre történő behatolás esetén (jellemzően mozgó) objektumok, tárgyak, állatok, emberek a rendszer konfigurációjának megfelelően, jelzéseket okoznak.

Védelmi zóna, zónák

Az adott védett létesítményben a biztonsági kockázatok alapján megkülönböztethető területek, épületek, épületrészek, vagy egyes helyiségek, melyeket a biztonsági kockázatokkal szinkronban meghatározható védelmi igényeknek megfelelően sorolunk be.

Vésznyitó

Az a biztonságtechnikai eszköz, amely a beléptető rendszer meghibásodása estén az ellenőrzött területről történő naplózott kijutást biztosítja.

Videoanalitika (képelemzés)

Olyan számítástechnikái környezetre kifejlesztett program, amely különböző mozgások, cselekvések detektálására, azonosításra, és riasztások kiváltásra alkalmas.

Videó megfigyelő rendszer (CCTV rendszer)

Az a biztonságtechnikai berendezés, amely a védett területen, illetve annak közvetlen környezetében történő, a védett létesítménnyel kapcsolatos mozgás, tevékenység vizuális megfigyelésére szolgál. A rendszernek képesnek kell lennie más alrendszerek jeleinek fogadására, illetve jelzések, képek, videó folyamok továbbítására meghatározott berendezések, beavatkozó alrendszerek, egységek részére. A kiépítettség, lefedettség szintje minden esetben a védett létesítmény, objektum biztonsági kockázatától, a tulajdonos és/vagy az üzemeltető információ igényétől függ.

Zóna

Olyan létesítményi terület, helyiség, helyiség-együttes, amely védelmére telepített érzékelők logikailag egy egységet alkotnak. A behatolásjelző rendszerek telepítése tekintetében a berendezés egyetlen érzékelője által felügyelt terület, felület, nyílászáró, tárgy, stb.

Zónaáthidalásnak nevezzük azt a tevékenységet, amikor behatolásjelző (esetleg más vagyonvédelmi rendszer) berendezés üzemeltetője olyan beállítást végez, amikor az érzékelőkből kialakított védelmi hálózat egyetlen zónáját (alapesetben „egy zóna – egy érzékelő” elvet kell követni mind a tervezés, mind a telepítés során) valamilyen számára nyilvánvaló oknál fogva úgy állítja be, hogy annak jelzése riasztást ne okozzon.