HADMÉRNÖK
BIZTONSÁGTECHNIKA

14. évfolyam (2019) 4. szám 35–45.
DOI: 10.32567/hm.2019.4.2

Pallagi András,[1] Kovács Tibor[2]

Kritikus infrastruktúrák komplex biztonságvédelmi rendszereinek tervezése, kialakítása, különös tekintettel a beléptetőrendszerek alkalmazására

Plan and Design of Complex Security Systems for Critical Infrastructures with Particular Regard to the Use of Access Control Systems

Napjainkban a modern társadalmak nagymértékben függnek a technikai és virtuális infrastruktúra komplex rendszereitől (energiaellátás, ivóvízellátás, informatikai hálózatok stb.). E rendszerek működési zavarai, illetve egyes elemeinek ideiglenes kiesése vagy megsemmisülése jelentős kihatással vannak mindennapi életünkre, a gazdaság és a kormányzat hatékony működésére.

Az állam, a gazdaság szereplői, valamint a lakosság részéről elvárás, hogy ezen alapvető létfontosságú vagy kritikus infrastruktúrák lehető legnagyobb biztonsággal működjenek. A kritikus infrastruktúra-elemek terrorcselekménnyel, természeti katasztrófákkal és balesetekkel szembeni védelme érdekében fontos, hogy az infrastruktúrák működésének megzavarása vagy manipulálása megelőzhető, kivédhető, illetve lehetséges mértékben rövid, kivételes és kezelhető legyen.

Jelen tanulmány a kritikus infrastruktúrák biztonságvédelmi rendszereinek tervezésével foglalkozik, kiemelten a beléptetőrendszerekkel szemben támasztott követelményekkel.

Kulcsszavak: **kritikus infrastruktúra, biztonsági megelőzés, beléptetőrendszerek**

[1] Óbudai Egyetem, Biztonságtudományi Doktori Iskola, doktorandusz, e-mail: pallagi.andras@phd.uni-obuda.hu, ORCID: https://orcid.org/0000-0002-6466-2631

[2] Óbudai Egyetem, egyetemi tanár, e-mail: kovacs.tibor@bgk.uni-obuda.hu, ORCID: https://orcid.org/0000-0001-7609-9287

Nowadays, modern societies are highly dependent on complex systems of technical and virtual infrastructure (e.g. energy supply, drinking water supply, ICT networks, etc.). The malfunctions of these systems and the temporary loss or destruction of some of their elements have a significant impact on our daily lives, on the efficient functioning of the economy and of the government.

The state, the economic actors, and the general public expect these essential critical infrastructures to operate with the utmost security. In order to protect critical infrastructure elements from acts of terrorism, natural disasters and accidents, it is important that disruption or manipulation of the operation of infrastructures should be prevented, further to the point, it should be managed with exceptional care and within a short time frame.

The present study deals with the design of critical infrastructure security systems, focusing on the requirements for access control systems.

Keywords: **critical infrastructure safety, prevention, access control system**

Bevezetés

Mit is értünk kritikus infrastruktúra alatt? Minden ország/kormány egy kicsit más-hogy fogalmazza meg, hogy számára mit is jelent. A magyar jogszabályi környezetben a következőképpen határozták meg:

„Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában"[1].

A jogszabály 11 fő ágat különböztet meg:

- energia;
- információs és kommunikációs technológiák;
- víz;
- élelmiszer;
- egészségügy;
- pénzügy;
- közbiztonság;
- polgári adminisztráció;
- szállítás;
- vegyipar és nukleáris ipar;
- űr és kutatás.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény alapján kijelölték a létfontosságú rendszerelemeket. Megkülönböztethetünk alapvető- és nemzeti létfontosságú rendszerelemet [2].

Alapvető rendszerelem lehet – a fenti ágazatok valamelyikébe tartozó olyan – eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú

társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.

Nemzeti létfontosságú rendszerelem e törvény alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése a létfontosságú társadalmi feladatok folyamatos ellátásának hiánya miatt jelentős hatása lenne Magyarországon.

Elsődleges célunk e rendszerelemek működőképességének, fizikai állapotának, valamint az ott dolgozó munkavállalóknak a védelme.

Biztonságvédelmi rendszerek kialakítása

A komplex biztonságvédelmi rendszerek kialakítása során a helyi fizikai és kriminalisztikai „adottságok" elemzése, valamint az elérni kívánt célok meghatározása az első lépés [3]. A folyamatot a létesítményről szóló információk összegyűjtésével kell kezdeni, majd a fenyegetések, kockázatok meghatározásával zárni [4]. Ezt követően védelmi zónák kijelölése, majd az ehhez tartozó fizikai és logikai biztonsági rendszerelemek tervezése következik [5]. A tervezés után ezen elemek értékelése és szükség esetén újratervezése következik [6].

A védelmi rendszereink tervezésénél a támadásokkal szembeni ellenintézkedéseinket vesszük figyelembe. Alapvetően négyféle ellenintézkedési fázis lehetséges:

- elrettentés;
- észlelés;
- késleltetés;
- reagálás.

Az elrettenttetés során célunk a külső szemlélő számára láttatni, hogy a védett objektum megfelelő fizikai és elektronikus védelemmel van ellátva. Ezt a látszatott tovább lehet erősíteni folyamatosa járőrtevékenységgel.

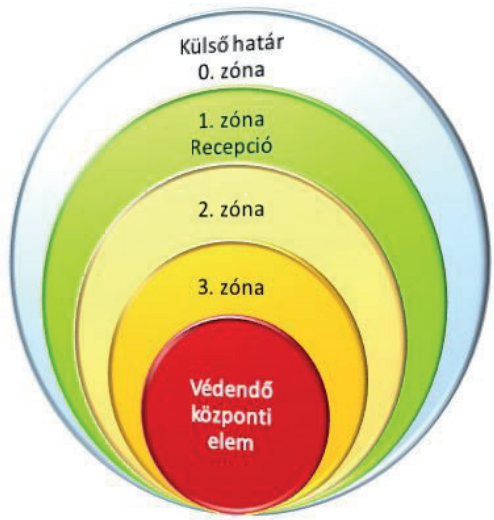
Az észlelés fázisában az elektronikus vagyonvédelmi eszközök jelzik a behatolási kísérletet. Ezek az eszközök lehetnek mozgás-, nyitás-, falbontás- vagy akár üvegtörés-érzékelők, valamint a beléptetőrendszer különböző elemei, illetve az informatikai rendszerhez tartozó védelmi megoldások (például tűzfalak).

A késleltetés fázisában leginkább jól megválasztott fizikai akadályokkal késleltetjük a behatolót a reagáló erők megérkezéséig. Ezek az akadályok rendszerint kerítések, ajtók, ablakok, zárak. Fontos, hogy a védelmi képességeik rétegesen épüljenek fel és folyamatosan biztosítsák a késleltetést a behatolás teljes szakaszában.

Az utolsó fázis a reagálás fázisa, ahol élő erővel reagálunk az észlelt behatolásra saját rendészeti állománnyal vagy hatósági erővel. Abban az esetben lesz eredményes az ellenintézkedésünk, ha az észlelt fenyegetéssel szemben arányaiban nagyobb az élőerős szolgálat kapacitása és képessége.

A fentiek figyelembevételével törekedni kell arra, hogy az egyes védelmi zónákhoz tartozó rendszerelemek egymásra támaszkodjanak és erősítsék egymást.

A biztonságvédelmi rendszer zónáit legjobban a hagyma, vagy másnevén PID (Protection-In-Depth) modellel (1. ábra) lehetne szemléltetni [7].



1. ábra
Hagyma-modell [szerzők szerkesztése]

A legfontosabb célja a modellnek, hogy a belső zónában a kritikus infrastruktúra működéséhez nélkülözhetetlen egységet helyezzük el.

Ennek a területnek a hozzáférése kívülről befelé irányban többszintes, a védett irányban növekvő hatékonyságú biztonsági intézkedések mellett legyen lehetséges. A biztonságvédelmi rendszer kialakításakor figyelemmel kell lenni arra, hogy a védelmi zónák/szintek közötti átjárás csak elektronikusan és fizikailag ellenőrzött körülmények és megfelelő adminisztratív módon történhessen meg [8].

Maria Lynn Garcia megfogalmazása szerint: „Egy jól tervezett rendszer mélységi és kiegyensúlyozott védelmet biztosít, minimalizálva a rendszerelemek meghibásodásának következményeit" [9].

Beléptetőrendszerek

Jelen írásomban a kritikus infrastruktúrák beléptetőrendszereivel kapcsolatos elvárásokról, felépítéséről és lehetséges megoldásairól készítek egy összefoglaló anyagot. Ideértve a komplex beléptetési rendszerhez kapcsolódó egyéb berendezéseket is, mint például a fémdetektorkapukat, valamint a csomagvizsgáló berendezéseket is [10].

A beléptetőrendszerek fogalmát sokan és sokféleképpen határozták meg, de véleményem szerint Filkorn József írta körül a legjobban egy 2009. évi előadásában azt, hogy mi is a beléptetőrendszer: „Komplex elektromechanikai-informatikai rendszer,

amely telepített ellenőrzőpontok segítségével lehetővé teszi objektumokban történő személy- és járműmozgások hely-, idő- és irány szerinti engedélyezését vagy tiltását, az események nyilvántartását, visszakeresését." „A szerkezeti elemeken túl tartalmazza azokat az intézkedéseket és apparátusokat melyek az üzemeltetéshez és a beléptetés felügyeletéhez szükségesek" [11].

Összefoglalva a beléptetőrendszer lényege, hogy ellenőrizni tudjuk, ki, mikor és hova szeretne bejutni. Ezzel kontrolálhatjuk az engedéllyel rendelkező személyek és anyagok mozgását a létesítményben. Továbbá detektálni és késleltetni tudjuk a jogosulatlan személyek közlekedését és a nem engedélyezett anyagmozgást.

A beléptetési pontokat a védett objektum külső határán és belső védelmi zónák átjáró pontjainál egyaránt használhatunk.

A komplex biztonságvédelmi rendszer keretében alkalmazott belépést ellenőrző, felügyelő rendszereink alapvetően három célt szolgálnak:

- személyforgalom kontrollálása, csak a meghatalmazott személyek tudjanak be- és kilépni a zónákba;
- a kifelé és befelé irányuló anyag- és eszközmozgás felügyelete, ideértve a robbanóanyagoktól kezdve az adathordozókig mindent;
- a biztonsági személyzet folyamatos informálása az aktuális mozgásokról, helyzetekről a hatékony reakció érdekében.

A beléptetési pontok lehetnek egy- vagy kétirányúak. Az előbbi esetben csak a védett térbe befelé haladók jogosultságát vizsgáljuk, míg az utóbbinál mindkét irányt felügyeljük.

A rendszerben definiálhatunk egyszeres áthaladást biztosító pontokat, amelyek jellemzője, hogy az adott irányba csak egyszer lehet áthaladni, és amíg nem történt meg az ellenkező irányba is az áthaladás, addig blokkolja a belépést. Ezt anti-pass-back funkciónak nevezzük.

A beléptetési ellenőrzőrendszer felépítése a védett zóna irányába haladva a következőképpen valósulhat meg.

Az első zóna, a védendő terület határa

A külső héj jelen esetben a tervezett létesítményünk telekhatára vagy kerítése. Jellemzően az első zóna a munkavállalók és a vendégek számára kialakított parkolót tartalmazza. Ide általánosságban sorompón, valamint őrszolgálati ellenőrzést követően lehet behajtani. Egyes esetekben itt már blokkerek vagy süllyedő oszlopok gátolják a bejutást, valamint számos esetben előfordulhat alvázvizsgálat is.

2. ábra
Automatikus behajtásgátló [18]

A beléptetőrendszer ezen első pontját ki lehet egészíteni rendszám vagy arcgeometria-felismerő rendszerrel is, valamint az utóbbi időben már viselkedéselemzési módszereket is tesztelnek [12].

A második zóna, a recepció

A következő beléptetési pont általában a portaépület, ahol a személyenkénti beléptetést forgóajtó, forgóvilla, gyorskapu vagy akár személyzsilip használatával valósíthatjuk meg. Az azonosítás történhet egy fizikai adathordozó (kártya, id-tag) vagy kontaktusmentes biometrikus azonosító olvasása (arc-, kézgeometria stb.) alapján. Ritkábban találkozhatunk olyan megoldással is, ahol a belépési kérelem regisztrációját követően egy QR-kóddal rendelkező egyszer használatos azonosítókártyával lehet belépni az objektumba. A kártyán található azonosító vonalkód tartalmazza az összes információt a belépéssel kapcsolatban, a vendég adataitól kezdve addig, hogy ki, mikor, milyen célból kezdeményezte a beengedést [13].

A beléptetés során fémdetektorkapuk és csomagvizsgáló berendezések használata javasolt, elkerülve a területre történő illetéktelen anyagok, eszközök bejutását. A beviteli engedéllyel nem rendelkező vagy a tiltott eszközöket a csomagvizsgáló berendezésen keresztül történő ellenőrzést követően egy egyedi zárható szekrényben célszerű elhelyezni.

Ideértve a tiltott anyagokat is, legyen szó akár alkoholról vagy egyéb vegyi anyagokról is, amelyeket szintén a vizsgálat után az erre kijelölt, lehetőség szerint robbanásbiztos tárolódobozba célszerű elhelyezni. Az ismeretlen eredetű, feltételezhetően robbanóanyagokról a 142/1999. (IX. 08.) Korm. rendelet 2. § (1) bekezdése értelmében: „köteles azt haladéktalanul bejelenteni a helyi rendőri szervnek vagy ahol

ilyen nincs, ott a települési önkormányzat jegyzőjének, aki a bejelentésről köteles értesíteni a területileg illetékes rendőri szervet" [14].

A recepciónál telepített beléptetési pontot javasolt kiegészíteni egy véletlen kiválasztórendszerrel, amelynek segítségével a kiválasztott adott dolgozó légalkohol vagy akár droghasználati ellenőrzés alá kerül. E vizsgálatokat két tanú jelenlétében egy külön zárt helyiségben kell elvégezni, tekintettel a személyiségi jogokra.

A beléptetőrendszer eszközei

A következő védelmi zónákban, a létesítményen belül a beléptetési pontok általánosságban az alábbi eszközökből állnak:

- a beléptetést fizikailag akadályozó berendezés (ajtó, forgóvilla, forgókapu, gyorskapu, zsilip, lift);
- elektromechanikus zárszerkezet;
- azonosítóeszköz vagy biometrikus jellemzőt olvasó eszköz;
- ajtónyitó- vagy vésznyitó gomb;
- nyitás-, áthaladás-érzékelő;
- a fenti eszközök vezérlőegysége, kommunikációs eszköze;
- (ajtóbehúzók).

A beléptetést fizikailag korlátozó eszköz az objektumon belül a legtöbb esetben egy egyszerű vagy biztonsági ajtó. Azonban előfordulhat forgóvilla, forgókapu, gyorskapu, zsilip vagy lift. A kiemelten védett területek bejáratánál törekedni kell az egyszemélyes beléptetési pontok használatára. Ezek a berendezések nem teszik lehetővé sem a ráakaszkodással (piggy backing) sem a besurranással történő illetéktelen belépést. Számos esetben súlykontrolos személyzsilipet használnak erre a célra. Ennek nagy előnye, hogy a felhasználóról a beléptetőrendszerben tárolt súlyadatot összeveti a mért adattal. Abban az esetben, ha valaki más használja a kártyát, vagy ha többen akarnak belépni, vagy ha valami anyagot szeretne mozgatni a személyzsilipen keresztül, a rendszer megtagadja az áthaladást.

A következő eszközök a zárszerkezetek, amelyek kialakításuk szempontjából lehetnek:

- bevéső zárak;
- tartómágnesek;
- portálzárak;
- reteszzárak.

A zárszerkezeteket alapvetően két fő csoportra bonthatjuk életvédelmi és biztonságvédelmi típusokra. Az életvédelmi zárszerkezetek (fail-safe) fő jellemzője, hogy a tápellátás megszűnésekor automatikusan kiold. Ezért ezt a típust használják a menekülési/kiürítési útvonalba eső ajtóknál.

A biztonságvédelmi zárszerkezetek (fail-security) legfőbb jellemzője, hogy az energiaellátás lekapcsolásakor is reteszelve tartja a zárat. Ezt a funkciót nagybiztonságú

helyiségek bejáratánál használják leginkább, kiküszöbölve egy áramszünet, vagy akár egy szabotázs okozta könnyű bejutást a védett helyiségbe.

Azonosítóeszközök, kártyák, biometrikus megoldások

A személyek egyedi azonosítását jellemzően névre szóló belépőkártyával és a hozzá tartozó kártyaolvasóval valósítják meg, de egyre nagyobb teret hódítanak a biometrikus jellemzőket érzékelő olvasóegységek is [15]. A korábbi optikai kontaktusos ujjnyomat-azonosítás helyett napjainkban a kéz-/arcgeometria, a vénaszkenner, valamint a kombinált ujjnyomat és vénaszkenner kezd elterjedni. Ritkábban szivárványhártya- vagy retinaszkennelés is előfordul, valamint mozgás- és hangazonosítás is [16].

A belépőkártyák, azonosítók fejlődése során a mechanikai megkülönböztetéstől (lyukkártya), a mágnescsíkos kártyákon keresztül eljutottunk az aktív és a passzív azonosítókig.

A rádiófrekvenciás egyedi azonosítók kommunikációs csatornái lehetnek:

- 120–150 kHz: ezek a legegyszerűbb rendszerek elemei;
- 13,56 MHz: ez a legelterjedtebb kommunikációs csatorna, ahol már megjelennek a nagybiztonságú egyedi kódolású azonosítók: Mifare, Desfire;
- 433 MHz: az aktív, tápellátással rendelkező nagy hatótávú (1–100 m) azonosítók;
- 865–868 MHz, 902–928 MHz: nagy hatótávú (1–12 m) azonosítók;
- 2480–5800 MHz (mikrohullám): WLAN, Bluetooth;
- 3,1–10 GHz (mikrohullám): nagy hatótávú (akár 200 m-ig) aktív azonosító.

A fizikai azonosítókat elláthatjuk – akár többszintű – titkosítással is. Ezek között találkozhatunk az e-passport jellegű titkosítással, amelynél megfelelő kulcspár hiányában minden egyes olvastatásra más és más kódsorozatot kapunk vissza.

Az azonosítókat többféle egyéb funkcióra is használhatjuk. Például a beléptető- és az informatikai rendszer összekötésével elérhető, hogy csak azok a dolgozók tudjanak belépni a személyi számítógépükbe, akik ténylegesen be is léptek az épületbe. Egy másik hasznos tulajdonsága, hogy azonosítóként lehet használni nyomtatóknál, valamint cafeteria keretében. Természetesen a bérszámfejtés alapja is lehet a beléptetőrendszer.

A beléptetőrendszer következő eszközei az ajtónyitó és a vésznyitó gomb. A lényegi funkciója ugyanaz mindkettőnél, csak az előbbinél ez egy pillanatnyi nyithatóságot, míg az utóbbinál tartós nyithatóságot eredményez. A védett oldalon helyezik el mindkét eszközt, de ajtónyitót csak az egyirányú beléptetési pontoknál használunk. Működési elve egyszerű, az elektromos zárszerkezet tápellátásába avatkozik bele. Legtöbb esetben elveszi a feszültséget közvetlenül, de vannak olyan ajtónyitó gombok, amelyek a központi vezérlőegységen keresztül vezérlik meg a zárszerkezeteket annak érdekében, hogy az áthaladás biztosított legyen.

A nyitás- és az áthaladás-érzékelők több biztonságvédelemmel összefüggő feladatot is elláthatnak. Az első ilyen az anti-pass-back szabály kontrollálása. Amennyiben az azonosítást követően nem történt áthaladás, akkor a rendszer csak azonosításként tárolja az eseményt és nem áthaladásként. A második nagyon fontos feladat

a beléptetési pont állapotfigyelése. Ki van-e támasztva az ajtó, esetleg blokkolják-e a bezárását. Számos esetben a nyitásérzékelő visszajelzése alapján az azonosító olvasó fény- és hangjelzéssel értesíti a környezetet a hibás működésről. Ezen eszközök az elektronikus behatolásjelző rendszer részét is képezhetik.

A vezérlőegység kétféle üzemmód szerint működhet. Online működés esetén az olvasóterminál adatait folyamatosan a szerver felé továbbítja, illetve a szervertől érkező adatok alapján megadja az olvasóterminálnak az aktuális állapotot, illetve vezérli az áteresztési pont elektromechanikus zárszerkezetének működését. Ha offline működésű a vezérlőegység, akkor a memóriájában tárolt adatok alapján közvetlenül dönti el az áthaladás lehetőségét, és ennek megfelelően küld adatot az olvasóterminálnak és az elektromechanikus zárszerkezetnek. A vezérlőegység alapvetően online és offline működésű: az adatkapcsolat megszakadásakor a vezérlőegység önműködően offline üzemmódra vált és korlátozott funkciókkal működik, majd az adatkapcsolat helyreállásával elküldi a naplóeseményeket a szervernek, frissíti a saját adatait és online működik tovább.

A teljes beléptetőrendszer működését egy központi egység irányítja, szervezi. A tárolt és a vezérlőegység által küldött adatok összehasonlítása alapján dönt az áthaladás engedélyezéséről vagy tiltásáról, ennek megfelelően vezérli a vezérlőegységeket és a perifériákat.

Itt történik:

- a jogosultságok meghatározása,
- a vezérlőegységek programozása,
- a rendszer működésének ellenőrzése,
- az információk megjelenítése, dokumentálása stb.

A beléptetőrendszerek működtetésével kapcsolatban azonban biztonsági kockázatok is felmerülnek.

Biztonsági kockázatok

A leggyakoribb biztonsági kockázatok és azok kivédésének lehetséges megoldását mutatja az első táblázat.

1. táblázat

Kockázatok és ellenintézkedések [a szerzők szerkesztése]

Biztonsági kockázat	Lehetséges megoldás(ok)
Besurranás: valaki jogosultsággal rendelkezőt követve bejutni a védett területre.	Szervezeti megoldás: őrszolgálat szervezése a beléptetési ponthoz. Technikai megoldás: forgóvilla, forgókapu vagy súlymérős személyzsilip használata.
Piggybacking: a jogosult személy a hátán viszi be a jogosulatlan személyt.	Szervezeti megoldás: őrszolgálat szervezése a beléptetési ponthoz. Technikai megoldás: forgóvilla, forgókapu vagy súlymérős személyzsilip használata.

Biztonsági kockázat	Lehetséges megoldás(ok)
Személyiséggel való visszaélés: valaki jogosult azonosítójának megszerzésével a védett területre történő belépés.	Szervezeti megoldás: őrszolgálat szervezése a beléptetési ponthoz. Technikai megoldás: biometrikus azonosítás használata, vezérelt zsilip használata.
Kiékelés, zárás, blokkolás: a védett térbe vezető ajtó záródásának véletlen vagy szándékos meggátlása.	Szervezeti megoldás: biztonságtudatosság növelése, szankciók meghatározása, járőrtevékenység. Technikai megoldás: ajtóbehúzók és nyitásérzékelők telepítése, fény- és hangjelzés használata.
Informatikai hálózat külső támadása.	Technikai megoldás: a külső hálózattól teljesen független rendszer kialakítása, külön VLAN használata, MAC-cím-vizsgálat.
Informatikai hálózat belső támadása.	Technikai megoldás: a belső hálózattól teljesen független rendszer kialakítása, külön VLAN használata, MAC-cím-vizsgálat.
Fizikai azonosító másolása.	Szervezeti megoldás: tiltott a fizikai azonosító kivitele a létesítmény területéről, azonosítást követően kerül átadásra a belépés előtt. Technikai megoldás: több lépcsőben titkosított fizikai vagy biometrikus azonosító használata.
Szabotázs: energia és hálózati kapcsolat megszakítása, EMC-támadás.	Technikai megoldás: többszörös energiavételi betáplálás kialakítása, offline üzemelésre képes beléptetőrendszer használata, rendszerelemek szünetmentesítése, központi szerverek EMC-védett helyiségbe telepítése.
Természeti katasztrófák, tűz.	Szervezési intézkedések: katasztrófahelyzeti terv létrehozása. Technikai megoldás: oltórendszerek használata, tűzvédelmi előírásoknak megfelelő menekülési irány biztosítása a beléptetési pontokon keresztül.

Összefoglalás, következtetések

A kritikus infrastruktúrák kialakításánál, mint optimális esetben minden más beruházásnál is, már a tervezési fázis elején célszerű kialakítani a biztonságvédelmi koncepciót. Ezzel a lépéssel a kivitelezésnél nagyságrendileg is mérhető költségeket lehet megtakarítani.

Napjainkban, a terroristacselekmények számának növekedésével kiemelten foglalkozni kell a humán faktorral.

Ahogy Kevin D. Mitnick és William L. Simon fogalmazta meg a legjobban ezt a kérdést, az ember a leggyengébb láncszem a biztonságban [17].

Számos lehetőség van a humán biztonsági kockázatok csökkentésére. Ilyenek például a célzott felvételi eljárások, valamint a kiemelt személyi ellenőrzések (NBH) lehetősége. Másik fontos lehetőségünk a biztonságtudatosság folyamatos növelése, emelt szinten tartása, továbbá a megfelelő szabályozási és adminisztrációs rendszer kidolgozása. Le kell fektetni és egyértelművé kell tenni, hogy kinek mihez van jogosultsága, kinek milyen kötelezettségei vannak.

Célom létrehozni egy olyan segédletet, amely segítséget nyújt a tervezőknek, a megrendelőknek és a kivitelezőknek abban, hogy az adott típusú objektumban, az adott feltételek mellett milyen beléptetőrendszer telepítése ajánlott biztonságszakmai szempontok alapján. Ezzel elérhetővé válhat egy biztonságosabb infrastruktúra-üzemeltetés.

Hivatkozások

[1] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról
[2] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
[3] T. L. Norman, *Integrated security systems design: concepts, specifications, and implementation.* Oxford: Elsevier Inc., 2007. DOI: https://doi.org/10.1016/B978-075067909-1/50042-1
[4] R. Ross, J. C. Oren and M. McEvilley, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems.* Gaithersburg: National Institute of Standards and Technology, 2016. DOI: https://doi.org/10.6028/NIST.SP.800-160
[5] J. Kingsley-Hefty, *Physical Security Strategy and Process Playbook*. Oxford: Elsevier Inc. 2013. DOI: https://doi.org/10.1016/C2012-0-07743-5
[6] L. Brotherston and A. Berlin, *Defensive Security Handbook.* Sebastopol: O'Reilly Media Inc., 2017.
[7] E. Wheeler, *Security Risk Management.* Sebastopol: Elsevier Inc., 2011. DOI: https://doi.org/10.1016/B978-1-59749-615-5.00012-8
[8] R. N Reid, *Facility manager's guide to security: protecting your assets.* Lilburn: Fairmont Press, 2005.
[9] M. L. Garcia, *Design and Evaluation of Physical Protection System (PPS).* Burlington: Butterworth–Heinemann, 2013.
[10] D. M. Bowers, *Access control and personal identification systems.* Burlington: Butterworth–Heinemann, 1988. DOI: https://doi.org/10.1016/B978-0-409-90083-5.50008-5
[11] J. Filkorn: *Beléptető rendszerek.* Székesfehérvár: Seawing Kft, 2009. [Online]. Elérhető: https://doksi.hu/get.php?lid=6516 (Letöltve: 2019. 12. 01.)
[12] Homeland Security Digital Library, "Defense Advanced Research Projects Agency (DARPA), Perimeter Security Sensor Technologies Handbook," *Homeland Security Digital Library,*1997. [Online]. Elérhető: www.hsdl.org/?abstract&did=451638 (Letöltve: 2019. 12. 01.)
[13] K. M. Hess, *Introduction To Private Security.* Wadsworth: Cengage Learning, 2009.
[14] 142/1999. (IX. 8.) Korm. rendelet a tűzszerészeti mentesítési feladatok ellátásáról
[15] L. Berek, *Biztonságtechnika.* Nemzeti Közszolgálati Egyetem, Magyary Program, 2014.
[16] D. Dobkin: *The RF in RFID.* Oxford: Newnes, Elsevier Inc., 2012.
[17] K. Mitnick and W. Simon, *The Art of Deception: Controlling the Human Element of Security.* Indianapolis: Wiley Publishing, 2002.
[18] "Automatic Rising Road Blocker," indiamart.com, [Online]. Elérhető: www.indiamart.com/proddetail/automatic-rising-road-blocker-12778514562.html (Letöltve: 2019. 12. 01.)