HADMÉRNÖK

XIII. Évfolyam 1. szám – 2018. március

MOBIL BÁZISÁLLOMÁSOK VAGYONVÉDELME

PROPERTY PROTECTION OF MOBILE BASE STATIONS

TEMESVÁRI Zsolt

(ORCID: 0000-0001-8309-7992)

zsolt.temesvari@gmail.com

Absztrakt

A rádiós bázisállomások folyamatos és hibamentes üzemelése elengedhetetlen a hang és adatszolgáltatás biztosítása érdekében. A bázisállomás, azaz a végberendezés többféle objektumra telepíthető, így a megfelelő vagyonvédelmi eszközökről különböző módon szükséges gondoskodni. A mobil szolgáltatás kiesése jelentős kockázatokat jelent vészhelyzet esetén, legyen az publikus vagy nemzetbiztonsági felhasználás, ezért a szolgáltatók mindent megtesznek annak érdekében, hogy ez elkerülhető legyen. A kimaradás lehet műszaki jellegű vagy külső beavatkozás okozta, utóbbi esetre többféle védelmi mechanizmust alkalmaznak, mely műszaki biztonságtechnikai megoldások feldolgozásra kerülnek a cikkben. A folyóirat végén a következtetések levonásra kerülnek, valamint ajánlást kínál a bázisállomások objektumvédelmének további fejlesztési lehetőségeire.

Kulcsszavak: *bázisállomás, objektumvédelem, biztonságtechnika*

Abstract

The continuous operation of mobile networks is definitely necessary for ensuring voice and data services. The base station, so the access equipment could be installed on several objects, therefore there is a need to take care of security measures in different ways. The loss of mobile services could cause high risk in emergency situations, be it public or national security use, thus the service providers try to do everything to avoid it. The outage can be caused by technical problem or external intervention. In the latter case several defence mechanisms can be used that are processed in this article. The technical security solutions are also discussed, as the recommendations as well for developing and increasing security levels of mobile base station object protection.

Keywords: *base station, object protection, security technology*

A kézirat benyújtásának dátuma (Date of the submission): 2018.01.02.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.03.20.

BEVEZETÉS

A mobilhálózatok védelme napjainkban egyre fontosabb szerepet kap, hiszen mobil terminálunk használata elengedhetetlen, legyen az akár a munkavégzés, az ismerőseinkkel való kapcsolattartás, vagy tájékozódás a körülöttünk folyó eseményekről. Sajnos a terrortámadások száma egyre fokozódik a világban, az információszerzés viszont elengedhetetlen ilyen vagy egyéb katasztrófa események során.

Napjainkban például a vegyipari gyártó és szállítási kapacitás volumenének növekedése veszélyes anyagok kiáramlásának kockázatát eredményezi ország területének jelentős részén annak ellenére, hogy a veszélyes anyagok szállítása veszélyes tevékenységnek minősül, és a tevékenység jogi szabályozása alaposan átgondolt. [1]

A távközlési hálózatok létfontosságú szerepet játszanak a vészhelyzetekben, különösen az egészségügyi szolgáltatások, a közigazgatás, a védelem tekintetében. Ezek közül egyik sem lehetséges megbízható és elérhető távközlés nélkül. A vészhelyzeti kommunikáció többek között a közcélú távközlési infrastruktúrából származó megosztott erőforrásokon keresztül valósulhat meg. [2]

Vészhelyzetben a hang és adatszolgáltatások elérhetőségére hatalmas szerep hárul, hiszen a lakosság ilyen esetben vezeték nélküli rendszerek segítségével érhető el a legkönnyebben, látható el védelmi információval, valamint a biztonsági szervek (pl. tűzoltóság, rendőrség, katasztrófavédelem, mentőszolgálat) is csak ezen a csatornán keresztül tudnak megfelelő tájékoztatást nyújtani.

Ezek egyben a legérzékenyebb kommunikációs csatornák is, melyek magas technológiai színvonalat képviselnek és működtetésük érzékeny technológiai biztosítást igényel. Veszélyhelyzet esetén e rendszerek leterheltsége a legnagyobb. Az SMS-ben elküldött figyelmeztető információk, a cellaüzenetek, az interneten közzétett adatok, a közösségi oldalak, levelezőrendszerek kulcsfontosságúak a vészhelyzeti kommunikációban. A rendszer részleges vagy teljes kimaradása (pl. jelentős kiterjedésű áramkimaradás) esetén a rendszerek, valamint a felhasználó oldali kliensek sem képesek üzemelni. Ilyen eset volt a 2003-as észak-amerikai „black out” is, mely során a telekommunikációs rendszer napokon keresztül óriási problémákkal küzdött. Az internetelérés stabil maradt, nem esett áldozatul az eseményeknek, viszont a felhasználók és számítógépeik elszigetelté és elérhetetlenné váltak, valamint a telefonos rendszerek is megbénultak, beleértve a vezetékes és a mobilhálózatot is. [3]

A bázisállomások elhelyezkedésének sűrűsége nagyban függ a domborzattól, a beépítettség mértékétől, valamint az ellátandó felhasználószám nagyságától. A városokban több bázisállomással találkozhatunk, mint a vidéki településeken. Egy-egy bázisállomás esetleges kimaradása városi környezetben ezért nem okoz akkora problémát, mint a vidéki területeken, mert bázisállomások sűrű elhelyezkedéséből adódóan a szomszédos állomások pótolni tudják a kimaradó bázisállomást. Ez persze rosszabb minőségben tehető csak meg, illetve nagy valószínűséggel csak a kültéri ellátottságot illetően. Vidéki környezetben viszont, ahol a szomszédos bázisállomások nagyobb távolságok adódhatnak, ott ez nem jelent megoldást.
Vészhelyzetben azonban a legnagyobb biztosítható kapacitásra, lefedettségre és minőségre volna szükség, így a bázisállomások bűncselekményből adódó kimaradását (például egy terrortámadás esetén) feltétlen szükséges megelőzni. A szolgáltatók különböző objektumvédelmi megoldásokat alkalmaznak, mely biztonságtechnikai mechanizmusok a következőkben olvashatóak, de az alkalmazott védelmi eszközök előnyei, hátrányai, valamint gyengepontjai is említésre kerülnek.

A BÁZISÁLLOMÁSOK ALKALMOZOTT VAGYONVÉDELMI ESZKÖZEI

Katasztrófa, vészhelyzet vagy terrortámadás esetén a mobilhálózatok kihasználtsága nagymértékben megváltozik, így azt a hálózati rendszerek megfelelő optimalizálása mellett sem lehet minden esetben kezelni. Ilyen esetekben egy-egy bázisállomás leállása egyébként is kritikus helyzetet teremthet elő, de lefedettségi problémákat is előidézhet. Műszaki jellegű hiba esetén az hálózatüzemeltetési mérnökökre hárul a feladat, hogy mielőbb megoldják az adott problémát. Külső, illetéktelen beavatkozás, rongálás, lopás vagy szándékos jogellenes cselekmény elkövetése esetén viszont különböző biztonságtechnikai, védelmi eszközöket és rendszereket szükséges alkalmazni. A bázisállomások hordozó objektuma számtalan formában megjelenhet, lehet az háztető, kémény, templom, stb., de a legelterjedtebb a tornyos megvalósítás, melynek vagyonvédelmi rendszerei a következőkben kerülnek tárgyalásra.

Első lépésként a várható biztonsági kockázatokat kell értékelni, milyen biztonsági kockázati tényezők, hogyan és milyen időtartamra változhatnak. Már az objektumvédelmi rendszer tervezési időszakában szükséges állapotfelmérés és kockázatelemzés elvégzése, ezek alapján lehetséges az értékelés és a javaslat kidolgozása. [4]

A kockázatelemzés során az adott tevékenységekkel kapcsolatban előforduló lehetséges biztonsági kockázatok azonosítását és értékelését kell elvégezni. Az elemzés során a kockázatok bekövetkezési valószínűségét, okozott hatását, illetve a kockázat bekövetkeztének elkerülését, lehetővé tevő intézkedéseket kell megvizsgálni. [5]

Mechanikai objektumvédelmi rendszerek

Mechanikai védelem

A mechanikai védelem az egyik legrégebben alkalmazott területe a vagyonvédelemnek. A komplex személy- és vagyonbiztonság egyik meghatározó elemeként, mindazon építészeti és gépészeti eljárások, eszközök és technológiák összessége, amelyek a személy vagy a vagyon létét, vagy a rendeltetésszerű működését veszélyeztető szándékos jogellenes cselekményt késlelteti, akadályozza, esetleg megakadályozza. [6]

A mechanikai védelem fő területei közé tartozik a kültéri védelem (kapuk, kerítések, sáncok, árkok, akasztók stb.), az építményvédelem (falazat, födém, padozat, tetőzet, ajtók, ablakok, rácsok, redőnyök, fóliák stb.), valamint a mechanikai tárgyvédelem (lemez- és páncélszekrények, széfek, trezorok, zárható bútorok és ládák stb.). Mindhárom terület meghatározó elemei a különböző zárak, lakatok és reteszek, ezért azok alkalmazására célszerűen komoly figyelmet kell fordítani. [7]

Kültéri védelem alkalmazása

A bázisállomások végberendezésinek legelterjedtebb tartószerkezete torony formájában valósul meg. Minden tornyos bázisállomás esetén alkalmazásra kerülnek speciális vagyonvédelmi eszközök, melyek feladata a jogtalanul belépni akaró személyek bejutásának megakadályozása. A mobil telephelyeket minden esetben egy betonalappal rendelkező kerítés veszi körbe, mely ~ 1,6 m magas, anyagát tekintve drótháló. A kerítés hatékonyságát és megbízhatóságát kiegészítve a sorokban széthúzva kifeszített tüskés drótot is alkalmaznak, a kerítés tetejétől számolva további 0,4 m-es magasságban, így a kerítés, valamint a szögesdrót együttesen 2 m-es magasságot tesz ki. [6]

A bázisállomás hardveres eszközeit a gyártó kültéri speciális szekrénye vagy konténer védi, de az utóbbi felhasználás gyakoribb. A kerítésen belülre, a bázisállomásokat és műszaki berendezéseket fizikailag tartalmazó konténereket vagy szekrényeket egy 2 m-es fémkapun át lehetséges megközelíteni, melyet egy biztonsági lakat véd.

Kültéri szekrények esetén a gyártóspecifikus kilincsek alkalmazásával, a zárperselyek deaktiválását követően vagy a már említett nagy biztonsággal bíró zárok megnyitásával

lehetséges a berendezésekhez jutni (a szekrény gyártója határozza meg az alkalmazott zárszerkezet típusát).

Építményvédelem és mechanikai tárgyvédelem

Különböző objektumtípusokat alkalmaznak a mobil szolgáltatók a tartóelemet illetően. A bázisállomások csak bizonyos részei (pl.: antennák, erősítők, stb., de a hardver és egyéb elemek nem) kerülnek fel a tartóelemre. Nem tornyos állomások esetén az objektumvédelem függ a telephely típusától. Speciális, például háztetőre vagy templom ablakokba épített bázisállomások esetén az épületre jellemző mechanikai védelemről beszélhetünk, például kerítéses védelem vagy falazat, födém, ajtók, ablakok, rácsok, redőnyök, stb. alkalmazása. Az épületbe való belépés az objektumhoz tartozó zárszerkezet(ek)hez tartozó kulccsal lehetséges. A kulcsszéfet speciális, magas biztonsággal és megbízhatósággal bíró zárak védik és őrzik a bázisállomáshoz vezető ajtók, kapuk kulcsait. Az ilyen típusú állomások főleg nagyvárosi környezetben jellemzőek.

Elektronikai objektumvédelmi rendszer elemei

Beléptető rendszerek

A megfelelően tervezett és kivitelezett beléptető rendszer több funkcionális területen is hatékonyan támogathatja az objektumvédelmet. A belépési pontokra telepített terminálok illetéktelen forgalom-csökkentési biztonsági funkciójukon túlmenően számos információs funkcióval bírnak. Az RFID kártyák installálásakor a dolgozó minden szükséges adatát meglehet adni. Jól kiépített rendszer esetében folyamatosan figyelemmel kísérhető a beléptető rendszer által felügyelt területen történő mozgások és egyéb felügyelt események. Idő és dátum mentésével minden esemény másodperc pontosan lekérdezhető, minden információ visszagyűjthető, kártyánként, ajtónként, valamint kártyaolvasónként is. [8]

Konténerek alkalmazása esetén általában legalább két zárszerkezet felnyitására van szükség: egy kisebb zárrendszer egy fali-széfet nyit meg (ez biztosítja a konténer elsődleges védelmét), egy nagyobb pedig a másodlagos őrizetért felel hagyományos zár formájában.

A széfpanel megnyitásával egy beléptető rendszerhez juthatunk, mely egy PIN kód panelt, valamint egy RFID olvasót tartalmaz. Ennek feladata, hogy a belépési jogosultságot megállapítsa, valamint azonosítja a belépni kívánt személyt és szabályozza az áthaladást. A beléptető rendszer része a központi egység, az olvasó terminál, valamint a vezérlő berendezés. Az eszköz képes azonosítani a belépő személy jogosultságait és a felhatalmazás megléte vagy hiánya függvényében vezérli az ajtó elektromechanikai zárszerkezetét. Az azonosítás a személyre szóló kártya RFID érzékelőhöz való érintésével működik. A sikeres autentikációt követően a kártyához tartozó PIN kód megadása, majd a fent említett konténer zárrendszerének kinyitása szükséges a bejutáshoz. [9], [10]

Napjainkban a jogosultság megállapíthatóságán kívül elvárható igény a jogosultság időben és térben történő lehatárolhatósága és változtathatósága. A beléptető rendszer személykövetési funkciója is lényeges, mellyel a belépésre jogosult személy tartózkodása nyomon követhető, valamint arról is információt nyújt, hogy az ellenőrzött terekben hányan az mennyi időt tartózkodtak. [11]

Távfelügyeleti eszközök

A konténerekbe való belépések minden esetben regisztrálásra kerülnek a hálózatüzemeltetési központban (a továbbiakban NOC[1]), ahol minden behatolást akceptálnak, amennyiben az tervezett munkához kapcsolódik, nem pedig külső behatolásból adódik. Ez a gyakorlatban úgy néz ki, hogy a bázisállomáshoz kapcsolódó tervezett karbantartási munkákat előre bejelentik a NOC részére, s amennyiben a belépési riasztás nem köthető valamely tervezett fejlesztési vagy szerelési munkához, valamint a behatolás nem felderíthető, úgy a hálózatfelügyeleti mérnökök haladéktalanul értesítik a rendőrséget az illetéktelen behatolás tényéről.

Ez önmagában a szándékos jogellenes magatartás elhárítása érdekében nem képes reagálni. Napjainkban a fejlesztők egyre több olyan megoldáson dolgoznak, melyek által bizonyos reagáló képességet biztosíthatunk a rendszernek emberi beavatkozás nélkül. [12]

Videofelügyeleti és mozgásérzékelős rendszerek

A célnak megfelelő kamera kiválasztását számos tényező befolyásolja. Meg szükséges vizsgálni azt, hogy az egyes kameráknak milyen környezetben kell működni, illetve milyen felbontású képet kell közvetíteni. Ez természetesen meghatározza az optika kiválasztását is. A felbontást megvizsgálva általánosan elmondható, hogy a nagyfelbontású képet szolgáltató kamerák drágák, ezért a kamerákat feladat szerint optimalizálni kell. [13]

A bázisállomások körbekerített területén általában mozgásérzékelővel ellátott lámpák kerülnek telepítésre, mely a sötétben végzett munkavégzés elősegítése mellett, adott esetben a jogtalanul oda merészkedő személyek elijesztésére is szolgálhat.

Kamerarendszer alkalmazása a magas költségek miatt nem igazán elterjedt, kiemelt vagy nagy jelentőségű telephelyek esetén viszont minden esetben alkalmazásra kerül. Az alkalmazott kamerák típusa eltérő, de mindegyik beépített infra LED-es megvilágítást használ, mely éjszaka is jól használható.

Tűz és füstjelző rendszerek

Mint minden területen, távközlési objektumok esetében is hatékony tűzjelző és evakuálási rendszert szükséges alkalmazni. A műszaki megoldások manapság széleskörű lehetőséget biztosítanak a munkavállalók és a technológiai folyamatok biztonsága érdekében. [14]

A bázisállomások tűz- és füstjelző rendszerekkel vannak ellátva. Amennyiben az adott telephelyet robbanás vagy tűz éri, a rendszerek haladéktalanul jelzik a NOC számára a problémát, akik a riasztásokat feldolgozva döntenek a tűzoltóság értesítéséről.

Napjaink tűzjelző berendezéseiben a kimeneti oldali feladatok jelentős részét a tűzeseti vezérlések teszik ki. Ezek megtervezése, összehangolása az egyes szakágakkal, valamint a vezérlési koncepció kidolgozása és működtetése komoly kihívást jelenthetnek nagyobb létesítmények esetén. Megfelelő működésük azonban alapvetően befolyásolja a tűzvédelmi berendezések hatékonyságát. [15]

Az alkalmazott védelmi rendszerek sebezhetősége

Az objektumvédelmi rendszerek célja, hogy a feltörést és behatolást, valamint rendeltetésszerű működést vagy szándékos jogellenes cselekményt akadályozza, késleltesse vagy teljesen megakadályozza [6]. Alapvetően a vagyonvédelmi eszközök viszont kijátszhatóak, amennyiben a behatolók megfelelő kompetenciával, ismerettel rendelkeznek a feltörni kívánt eszközökről. A hatékonyságot ár-érték arányban kell meghatározni attól

[1] NOC: Network Operation Center

függően, hogy milyen kockázatot rejt az adott helyszínre való behatolás, a beruházás mértéke arányos a biztosított védelemmel.

Speciális bázisállomások esetén a kulcsszéfet rejtő objektumba való bejutást követően a széf zárjának feltörése szükséges ahhoz, hogy a bázisállomás megközelítéséhez szükséges kulcsokhoz hozzájussanak. Biztonságtechnikai szempontból magas védelmet nyújtó zárberendezés révén ehhez szintén gyártói kompetencia szükséges, sebezhetősége minimális. A széf leszerelése a felszerelés módja miatt összetett, amennyiben mégis kivitelezésre kerülne, úgy azt csak drága acélvágó eszközök segítségével lehet megtenni. Egy esetleges illetéktelen behatolási szándék esetén ez a megoldás általában nem reális veszély tekintve a cselekmény nagy zajhatását, figyelemkeltő mivoltát. Mint az korábban említésre került a speciális bázisállomások (panelházak, különböző épületek házteteje, stb.) városi környezetre jellemzőek, ahol egy bázisállomás hatástalanítása esetén - a sűrű mobilhálózati betelepítettség miatt - a környező bázisállomások jó eséllyel át tudják venni a kiesett telephely területét, s továbbra is képesek kültéri lefedettséget biztosítani. A széf vagy zárjának feltörése tehát kis kockázatot képvisel, a bázisállomás számára bérelt objektum (pl. egy panelház bázisállomáshoz vezető fémajtajának zárja) feltörése nagyobb kockázatot jelent, mint az ehhez szükséges kulcsok megszerzése, de a bázisállomás hardverei ezt követően sem megközelíthetőek a fent taglalt speciális acél szekrények megléte miatt.

Tornyos bázisállomások alkalmazott kültéri védelme talán a legsebezhetőbb, ugyanis erővágó alkalmazásával könnyen feltörhető a kerítés, s ezzel a kerítés kiegészítésének számító szögesdrót funkciója is értelmét veszti. Gyártóspecifikus kültéri szekrények alkalmazása esetén az acél zártárcsák körbevágásával van csak esély azok felnyitására, melynek fizikai megvalósítása nagy feltűnést kelt, nem reális a kivitelezése. Amennyiben a bázisállomás konténerben került elhelyezésre, úgy egy sok ponton záródó acélajtó zárrendszerének feltörésére van szükség, ami alapos szakmai ismereteket igényel, valamint igen időigényes, nagy az esélye annak, hogy az jogtalanul behatolni szándékozó személyt észreveszik a cselekmény során. Az ajtó acélból készült tartóelemeinek kivágása szintén kevés eséllyel kivitelezhető anélkül, hogy a bűncselekményt végző személyt ne észleljék valamilyen formában. Amennyiben mégis megtörténne, a távfelügyelet segítségével azonnal megjelenik a hálózatüzemeltetési központ riasztási listáján az adott behatolás (RFID azonosítás és PIN kódos védelemnek, valamint a direkt bekötésnek köszönhetően a NOC felé) és a készenléti szervek értesítésre kerülnek. Ez a biztonságtechnikai óvintézkedés tehát kisebb kockázatot jelent, hiszen kevés a sebezhető pontja. A tornyon lévő rádiós berendezésekhez és az antennákhoz a feljutás általában akadályozva van (a megközelítéshez szükséges létra első néhány méterére lezáró borítást tesznek), a rádiós kábelek pedig olyan magasságba kerülnek szerelésre, hogy azok ne legyenek megközelíthetőek.

A tűzvédelmi eszközök a konténerek és szekrényeken belül helyezkednek el, így az előzetes hatástalanításuk az ajtók és zárak feltörése nélkül nem kivitelezhető. A füstjelzőknek köszönhetően egy esetleges robbantásos vagy gyújtogatásos merényletet a NOC haladéktalanul észlel és a rendvédelmi szervek azonnal értesítésre kerülnek. Ez a bűncselekmény nagy veszélyt hordoz magában a bázisállomások folyamatos működését illetően, és jó eséllyel sikerrel hatástalanítja az adott állomást.

Videorendszerek alkalmazása esetén az adott illegális belépési szándék rögzítésre kerül, így a bűncselekmény későbbi bizonyításában jelentős szerepet tud játszani, nem beszélve arról, hogy a lelepleződés veszélye miatt a cselekmény megkísérlése is meghiúsulhat, szemben egy olyan állomással, ahol kamerarendszer nem került telepítésre. Hátránya ezeknek a biztonságtechnikai intézkedésnek, hogy az egyszerűbb analóg kamerák hatástalaníthatóak, például egy kő vagy egyéb tárgy kameraképernyőbe való hajításával. A korszerű, elemző szoftverrel támogatott videófigyelő rendszerek képesek ugyan szabotázsérzékelésre, a kamera

érzékeli a letakarást, a festékkel való lefújást, de azt is, ha elmozdítják, elfordítják vagy megrongálják. Ezek a rendszerek azonban költségesek. [12]

KÖVETKEZTETÉSEK

A mobil bázisállomások kiesése veszélyhelyzetben nagyon súlyos következményekkel járhat. Ezen ágazat teljes vagy részleges megsemmisülése fennakadást okozhat egy állam működésében. Napjainkra a technológiai szektor jelentős mértékű fejlődést mutat, illetve hozott magával. Életünket is egyszerűbbé teszik, és kölcsönös függést eredményeznek a felhasználó és az adott terület között. Így ezek hiánya a morál jelentős csökkenését okozza a társadalomban. [16]

Egy előre eltervezett terrorcselekmény esetén a bázisállomásokat a terroristák hatástalaníthatják annak érdekében, hogy a támadás során a rendvédelmi és nemzetbiztonsági szervek munkáját ellehetetlenítsék, valamint a mentési folyamatokat akadályozzák.

A bázisállomások felsorolt biztonsági óvintézkedéseinek kiterjesztésével, illetve további biztonságtechnikai fejlesztésekkel felkészültebben lennének kezelhetőek az esetleges terrorcselekmények. Az alkalmazott vagyonvédelmi rendszerek anyagi vonzata magas, de nagyobb beruházások esetén a mobilhálózatok objektumvédelme is nagyobb biztonsági fokozatot élvezhetne.

Távfelügyeletű (a kamera képe központilag monitorozható) kamerarendszer kiterjesztése az összes bázisállomásra vonatkozólag jelentősen csökkenthetné a kockázatot az állomások hatástalanítását illetően. Ily módon minimálisra csökkenhetne az idő, amely annak eldöntésével telik, hogy valóban illegális behatolásról beszélhetünk és nem pedig emberi mulasztásból adódó, előre nem lejelentett műszaki munkáról van-e csak szó. Ezáltal probléma esetén a készenléti szolgálatok szinte azonnal akcióba léphetnének, megakadályozva ezzel a nagyobb károk kialakulását.

Kisebb beruházás árán a távfelügyeleti kamerarendszert kiegészítve hangszórók vagy riasztószirénák kerülhetnének telepítésre, melyek az illetéktelen behatolás tényének beazonosítását követően bekapcsolásra kerülhetnének, és ezzel elriaszthatnák a bűncselekmény elkövetőit.

Szintén a jogosulatlan belépés esélyét csökkentené, ha a szolgáltatók egy országos infrastruktúrával rendelkező biztonsági céget bíznának meg az állomások felügyeletével. Az őrök így a rendőrségnél már hamarabb, akár bizonytalan esetben vagy téves riasztásra is a helyszínre küldhetőek lennének ellenőrzés céljából.

Fentiekben összefoglalt védelmi, biztonsági eszközök, eljárások együttes, komplex alkalmazásától várhatjuk el, hogy a magas szintű mobil távközlési szolgáltatások egyik fontos alap pilléreként szolgáló bázisállomások akár terrorhelyzetekben is, a hatástalanítás veszélyét minimalizálva, megbízhatóan működjenek.

Fokozottabb mértékben kerülnek előtérbe a szolgáltatás folyamatos biztosításának kérdései veszélyhelyzeti szituációban. Ilyen esetben további műszaki megoldások bevetésére is szükség van, hogy a stratégiailag fontos távközlési rendszer a rendfenntartó szervek, valamint az esemény károsultjai számára végig problémamentesen használható legyen az esemény során. Ezen kérdések egy következő publikáció témája lesz.

FELHASZNÁLT IRODALOM

[1] BEREK L.; SOLYMOSI J.: *Veszélyes anyagok szállításának biztonsága;* Bolyai Szemle 24. 2. (2015) http://archiv.uni-nke.hu/uploads/media_items/bolyai-szemle-2015-02.original.pdf

[2] MIKLÓS S.; MAROS D.: *International Regulations of Interoperation of The Telecommunication Networks in Emergency Situations;* Academic and Applied Research in Military Science 3. 5. (2004) pp. 707-714.

[3] VASS A.; MAROS D., BEREK L.: *Veszélyhelyzeti infokommunikáció az energetikai black out alatt;* Bolyai Szemle, 24. 2. (2015) 63-76. o.

[4] BEREK T.; HORVÁTH T.: *Fizikai védelmi rendszerek dinamikusan változó környezetben*; Hadmérnök IX. 2. (2014) 16. o. http://www.hadmernok.hu/142_02_berekt.pdf

[5] UTASSY S.: *Vagyonvédelmi rendszerek tervezése, telepítése;* Detektor Plusz, 14. 8-9. (2007) 18-20. o.

[6] BEREK L.: *Biztonságtechnika*; Nemzeti Közszolgálati Egyetem, Magyary Program, (2014) 11-29. o.

[7] BEREK T.; ELEK I.: *Zárszerkezet, mint a mechanikai védelem sebezhető pontja*; Műszaki Katonai Közlöny XXV. 3. (2015) 47-58. o.

http://www.hhk.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/PDF_2015_3_sz/2015_3sz.pdf

[8] BEREK T.; TAKÁCS Z.: *RFID technológia mint a kórházbiztonság területén megvalósuló intézményi rend biztosításának eszköze*; Hadmérnök VIII. 2. (2013) http://www.hadmernok.hu/132_01_berekt_tz.pdf

[9] LUKÁCS Gy.; GÁBOR L (szerk.): *Új Vagyonvédelmi Nagykönyv*; CEDIT 2000 Kft., Budapest, 2002. ISBN 963 8180 39 0. 204-241. o.

[10] ABAD, I.; CERRADA, C.; CERRADA, J. A.: *METAPEDCAS: Introduction Semantic RFID Data ManagemenT;* In: G. URZAIZ, S. F. OCHOA, J. BRAVO, L.L. CHEN, J. OLIVERIA (Eds.): 2013 Ubiquitous Computing and Ambient Intelligence; Carillo, Costa Rica. pp. 199-206.

[11] BEREK T.: *ABV (CBRN) analitikai laboratórium beléptetőrendszere a biztonságos üzemeltetés szolgálatában;* Hadmérnök VI. 2. (2011) 21-36. o. http://www.hadmernok.hu/2011_2_berek.pdf

[12] BEREK L.; BEREK T.; BEREK L.: *Személy- és vagyonbiztonság*; ÓE-BGK 3071, Budapest, 2016. ISBN:978-615-5460-94-4

[13] BEREK T.: *Vagyonvédelmi koncepció kialakításának sajátosságai veszélyes anyagok vizsgálatát biztosító létesítmények esetében;* Hadmérnök VI. 4. (2011) http://hadmernok.hu/2011_4_berek.pdf

[14] MOHAI Á. ZS.: *Active fire safety on construction sites;* Műszaki Katonai Közlöny XXVII. 4. (2017) 55-69. o.

[15] MOHAI Á. Zs.: *A tűzjelző berendezések riasztási hatékonysága;* Műszaki Katonai Közlöny XXVII 3. (2017) 20-37. o.

[16] BEREK L., VASS A., MAROS D.: *Az interdependencia kérdése az energetikai rendszer és a hiradástechnika esetén a kritikus infrastruktúra biztonsága érdekében:* Bolyai Szemle 24. 3. (2015) 9-32. o.