Magyar Rendészet 2024/1. 89–105. DOI: 10.32577/mr.2024.1.6

A fizikai védelmi rendszerek és a biztonsági központ

GUBICS Frigyes[1] – HORVÁTH Tamás[2]

A modern fizikai védelmi rendszerek elterjedése és alkalmazásuk Magyarországon a rendszerváltozástól datálható, hiszen az átállás biztosította a hozzáférés lehetőségét addig nálunk nem látott, nem használt rendszerekhez. A technika fejlődése magával hozta az iparág fejlesztését is, illetve a telepítéshez és fenntartáshoz szükséges tudás megszerzése is igényként jelent meg. A kapitalizálódás megteremtette a vagyonvédelmi piacot, illetve szélesítette azt. A biztonsági kultúra kialakítása a magántulajdon megjelenésével elengedhetetlen volt, de ez a fajta megközelítés igazán a multinacionális vállalatoknál valósult meg, hiszen ezek megjelenésével hozták magukkal az anyacégeknél és a más országokban megszerzett tudást, tapasztalatot. A fizikai védelmi rendszerek komplexitása, egyre autonómabb működésük igényelte, hogy az irányítás, információk kezelése és analizálása centralizáltan történjen, a reakciók gyorsak és átláthatóak legyenek, így létrejöttek a biztonsági központok, amelyeknek kulcsszerepe van az objektum elvárt biztonsági szintjének fenntartásában.

Kulcsszavak: *fizikai védelem, biztonsági központ, kockázatelemzés, vagyonbiztonság*

Bevezetés

A biztonságtudomány viszonylag fiatal tudományág, amely az utóbbi néhány évtizedben indult rohamos fejlődésnek, köszönhetően a globális szintű változásoknak és a biztonsági iparágra is hatást gyakorló tendenciáknak.[3] A biztonságra egyre nagyobb az igény, és kormányzati szinteken, illetve a versenyszférában is felismerték ennek fontosságát, aminek köszönhetően nőtt a fejlesztésre ráfordított erőforrás, és hatékonyabb lett az üzemeltetés. A technikai haladás szintén kihatással van a tudományág és ezzel együtt az üzletág fejlődésére, ideértve az egyre intelligensebb rendszereket és a digitalizáció térnyerését is. A fizikai biztonsági rendszerek alapját képezik egy objektum védelmének, megfelelő tervezéssel az úgynevezett preventív biztonság alapkövei. Egy komplex rendszer – alapösszetevőit tekintve behatolásjelző, zártláncú kamerarendszer, beléptetőrendszer – üzemeltetése ma már egyé-

[1] Biztonsági igazgató, Lenovo Manufacturing Kft.

[2] Adjunktus, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Magánbiztonsági és Önkormányzati Rendészeti Tanszék; KÉSZ Csoport, fizikai biztonsági és csalásmegelőzési vezető.

[3] Lippai–Csaba 2021.

telműen olyan kompetenciákat igényel a biztonsági szolgálatok részéről, amelyek második pillérként szolgálnak, kapcsolódva a harmadik, de sorrendben inkább elsőként említhető biztonsági központhoz. A biztonsági központ létrehozása nem más, mint az alaptevékenységként végzett biztonsági szolgáltatás, tevékenység keretbe foglalása, egységesítése, az adatok feldolgozásának központosított formája. A bejövő információk jól detektálhatók, az egyes csatornákon érkező adatok fizikailag egy helyre érkeznek és összekapcsolhatók, összefüggéseikben értelmezhetők, kiértékelésük után pedig a válaszreakciók időben és adekvátan érkeznek. A támogató jogszabályi háttér és a szakmai képviselet segít a rendszerek üzemeltetésében, de a rugalmas és az élet változásaihoz igazodó jogszabály-módosítási gyakorlat még nem része a magyar jogalkotásnak.

A cikk címe alapján jogosan merül fel a kérdés: a fizikai rendszer mit is véd? Gondolhatnánk első látásra azt, hogy mindent, aminek fizikai létezése, megjelenése van. Ez részben igaz, azonban fizikai védelemre[4] szüksége van például az információknak is, hiszen érzékeny vállalati információk nem heverhetnek szabadon minden irodában, ahol bárki hozzáférhet. Először is azokat zárt ajtók mögött tároljuk – függetlenül attól, hogy elektronikus vagy papírformában érhetők el. Korlátozzuk a bejutást, így megtettük az első fontos lépést a fizikai védelem kialakítására. Természetesen a példában említett szenzitív adatok védelmét fokozhatjuk attól függően, hogy mennyire fontos számunkra, hogy illetéktelenek ne férjenek hozzá. Például, ha gyártástechnológiát szeretnénk védeni, nem szerencsés, ha a gyártóterület ablakai átláthatók, kívülről a belátást meg kell akadályozni függöny, roló, illetve speciális fólia alkalmazásával.

A fizikai biztonság tervezésekor figyelemmel kell lennünk a már rendelkezésre álló és a jövőben telepítendő technológiák integrálhatóságára, amelyeknek módszertanukban a belső vállalati szabályokon túlmenően jogszabályi oldalról is megfelelőnek kell lenniük.[5]

A biztonsági rendszerek egységes platformon történő kezelése a fizikai biztonsági rendszer hatékonyságának erősítését célozza, amely a megelőzés és felderítések eredményességében mérhető, a reakcióidők csökkentése mellett. Fontos szempont az úgynevezett „compliance",[6] vagyis az a fajta megfelelőség, harmonizáció, amely figyelembe vesz minden szempontot, a szakmai mellett a vállalat speciális, idevonatkozó szabályait, amelyeknek ugyancsak harmonizálniuk kell a hatályos jogszabályokkal. A fizikai védelem felépítését ezen elvek, szabályozók mentén kell végrehajtanunk. Cikkünkben a fizikai biztonság kérdéskörét kívánjuk körbejárni abból az aspektusból, hogy milyen módon érhetjük el a megkívánt biztonsági szintet, melyek azok az eszközök, amelyek rendelkezésre állnak, milyen előnyei, illetve ne-

[4] Fizikai védelem: célja a fizikai eszközök, erőforrások, személyek védelme jogosulatlan hozzáféréstől, sérüléstől, károkozástól.

[5] Tiszolczi 2019.

[6] Compliance: megfelelőség (valamilyen szabálynak, irányelvnek, előírásnak), amelynek célja, hogy egy vállalat, illetve szervezet külső és belső tevékenységét tekintve is megfeleljen az irányadó törvényi, szervezeti és olykor erkölcsi/társadalmi szabályoknak.

hézségei vannak a rendszer kiépítésének – a fizikai védelem személyi, szervezési, technológiai és eljárás-módszertani rendszerét helyezzük a fókuszba.

A biztonságról általánosan

A biztonság mint a fenyegetettség hiánya egyszerűen írja le a fogalmat, azonban túl elméleti a fogalom abban az esetben, amikor a biztonság megvalósításáról beszélünk.[7]

A biztonság kifejezés mindenkinek mást jelent, de talán nem véletlen, hogy a Maslow-piramis alsó részében találjuk, ez tehát az egyik legalapvetőbb igénye az embernek: bántódásmentesnek lenni és abban az állapotban meg is maradni. A biztonság tudománya multidiszciplináris[8] alapokon nyugszik. A biztonságtudomány egy kialakulóban lévő tudományág, amely a fizikai és információs vagyon, személyek biztonságát veszi górcső alá, hangsúlyozva, hogy a biztonság nemcsak az állami szervezetek, hanem a kisebb közösségek és az egyén felelőssége is.[9]

Abraham Maslow elméletében tehát előkelő helyen van a biztonságra való törekvés, annak vágya, hogy biztonságban legyünk, és realisztikusan átgondolva, semmilyen tevékenység nem végezhető hosszú távon, nyugodtan, akár félelem nélkül, ha az alapvető biztonsági igényünk nem teljesül. A fizikai szükségleteken túl tehát igényként merül fel a biztonságra történő törekvés mint alapelvárás.[10]

A biztonság léptékei

Különböző léptékekben kell gondolkodnunk a biztonságról: globális, országos, kisebb közösségi, lakóhelyi, személyes. Mikroszinten tehetünk a legtöbbet a biztonságérzetünkért, ami nem egyenlő az objektív biztonsággal. A biztonságérzet befolyásolója nagymértékben az állam és annak szervezetei. A vagyonbiztonság az, amelyről személyesen gondoskodunk különböző, hétköznapinak tűnő eszközökkel, mint kerítés, kulcsra zárt ajtó, riasztóberendezés stb.

A vagyonvédelem nagyobb léptékben a gazdasági társaságok, vállalatok életében jelenik meg és válik a közösség számára is fontossá, hiszen a vállalati vagyon megtartása elemi érdeke a cégtulajdonosokon kívül a munkavállalóknak is. A termelőeszközök hiányában veszélybe kerül a prosperitás, és ha nincs mivel termelni, nem lesz mit eladni a piacon és így a vállalat fizetni sem tud dolgozóinak, tehát veszélybe kerül az emberek anyagi biztonsága is.

---

[7] Christián 2014.
[8] Multidiszciplináris: több tudományágat, szakterületet érintő.
[9] Christián et al. 2019.
[10] Maslow 1954.

A biztonság gyökerei

Az emberi történelem során a valami ellen, jobbára a támadók elleni védekezés mindig is együtt járt az ember által generált és megélt konfliktusokkal. A fizikai védelem egyidős az emberiség kialakulásával és az egymás közti konflitusok létrejöttével. Amikor az egyenlőtlenség kezdett kialakulni és felütötte fejét az irigység, amikor még nem voltak etikai gátak, jogi normák, szankciók és semmi, ami visszatarthatta volna az embereket egymás tárgyainak, később vagyonnak nevezett értékeinek, embereinek, asszonyainak elbirtoklásától; az egyik oldalon megjelentek az eltulajdonítást elősegítő módszerek, a tulajdonosok, birtoklók pedig intézkedéseket tettek ennek megakadályozására. A földtulajdonnal elkezdtek kiépülni a tulajdon határát jelző „rendszerek", vagyis a kerítések. Ezen belül is védeni kellett a tulajdont, élőhelyet, és nem csak az időjárás viszontagságaitól. Erre szolgált a ház fala, a zárható ablakok és ajtók. A tehetősebbek embereket béreltek fel, hogy a birtokhatárokat vigyázzák, mai szóval talán a vagyonőr a leghelyesebb kifejezés erre a tevékenységre.

Klasszikusan az ember ember elleni harca során védekezés, majd visszatámadás következett. Az ókorban és az újkor hajnalán még kevéssé volt szabályozott a védekezéshez való jog a jogtalan támadásokkal szemben, jóllehet az angolszász jogrendszer hagyományon és precedenseken alapuló ítélkezési gyakorlatában ez megjelent, és a jogos védelem elfogadott volt. Korunkban, amikor a jog uralkodik a civilizált társadalmakban *(rule of law),*[11] az állam kötelezettsége megvédeni polgárait, amelynek az igazságszolgálatatáson és erőszakszervezetein keresztül szerez érvényt. Ki védi meg az állampolgárok tulajdonát? A tulajdon védelme alapvető emberi jog, amelyet az Alaptörvény deklarál. Kimondja, hogy személy, illetve tulajdon ellen intézett jogellenes támadás elhárításához mindenkinek joga van.[12]

A vagyonvédelem evolúciója

Minden olyan tevékenység, ami magánkezdeményezés, az államnak nem volt ráhatása és felügyelete, tiltott volt. Kifejezetten tilos volt, hogy a rendőrségen kívül más szervezet ellásson őrzés-védelmi feladatokat. Az 1960-as években kezdett átalakulni az ipari üzemek őrzése, és már nemcsak karhatalmi szervezetek tevékenykedtek, hanem kialakult az úgynevezett üzemrendészet, amely a belső rendet volt hivatott fenntartani, de hatósági jogosítványuk nem volt.[13] A mai értelemben vett objektumőrzés kialakulásának kezdete a rendszerváltáshoz köthető, hiszen ekkor kezdtek az állami cégek megszűnni, átalakulni, privát vállalatokká formálódni, ahol szükség volt a vagyon védelmére. Ehhez eleinte másodállású rendőrökből, nyugdíjas katonákból verbuváltak „vagyonőröket". Napjainkban a magánkézben lévő ipari ob-

[11] Rule of law: jogállam.
[12] Magyarország Alaptörvénye (2011. április 25.), V. cikk.
[13] Lippai 2021.

jektumok védelmét vagyonvédelemmel foglalkozó cégek látják el, sok esetben ezek a vállalkozások építik ki a fizikai védelemhez szükséges technikai rendszereket, így nem kizárólag az élőerős őrzés a feladatuk.

A magántulajdonon alapuló társadalmakban a tulajdonos kötelessége gondoskodni a vagyonvédelemről. Magyarországon és a többi, keleti blokkhoz tartozó országban a múlt rendszerben a „nép közös tulajdonát" nem kellett védeni, hiszen a bűnözés mint olyan hivatalosan nem, vagy csekély mértékben létezett. Ennek megfelelően a védelmi potenciál is alacsony volt, ha egy termelőszövetkezet vagy egy gyár értékeit kellett megvédeni, sőt sok esetben a rendészek is közreműködtek, még ha csak passzívan is, egy-egy vagyon elleni cselekmény végrehajtásában. A lopás a szocialista rendszerben is bűn volt, mindemellett sok elkövető azzal az ideológiával mentette fel magát, hogy ami mindenkié, az lényegében senkié, így az enyém is lehet, tehát jogom van elvinni. Ezt a hiedelmet, „népszokást" szakította meg a rendszerváltás, amikor hirtelen, sokkszerűen megváltozott a gazdasági környezet, ezzel együtt az érdekek is, és előtérbe helyeződött az egyének, tulajdonosok vagyoni érdeke. A privatizáció és ehhez kapcsolódóan a kárpótlás új alapokra helyezte a vagyoni viszonyokat. Az évek alatt kialakult új gazdasági rend mellett átrendeződött a társadalom is, alapvetően szintén gazdasági alapon. A vagyontárgyak centralizálva kezdtek megjelenni, és megszületett egy új, tehetős réteg, akik kezében elég érték összpontosult ahhoz, hogy legyen mit megvédeni, most már valódi tulajdonosi alapon és érdekek mentén. Innentől kezdve a védelmet nem látszólagosan, hanem hatékonyan és számonkérhetően kellett megszervezni, hiszen vagyonvesztés esetén nem a nép mint közös tulajdonos állt helyt, hanem sok esetben az egyszemélyi tulajdonost érte kár. A kockázat tehát már valódivá vált, és ehhez kellett felzárkóztatni a hatékony védelem kialakítását, amely jogszabályi oldalon is megteremtette a modern vagyonvédelem alapjait. A törvényalkotó ezen a téren is adott feladatot a Rendőrségnek.

Jogszabályi háttér

A jogalkotó a gazdasági tevékenység keretében, személy- és vagyonőri tevékenység végzéséhez történő hatósági engedély kiadását, a szakmai és adminisztratív ellenőrzést, szankcionálást a rendőrség hatáskörébe utalta.[14]

Ezzel extra terheket tesz a Rendőrségre úgy, hogy plusz erőforrást ehhez nem rendel. Ennek köszönhetően az ellenőrzések végrehajtása mennyiségben és minőségben korlátozott. Másfelől azonban kérdésként merül fel a szakmai hozzáértés, tehát hogy rendelkezik-e a Rendőrség megfelelő szakértelemmel és szakembergárdával e tevékenységek érdemi szakmai ellenőrzéséhez, irányításához. A feltett kérdések költőiek, hiszen aki a privát biztonsági területen dolgozik, érzékeli, hogy a hatósági és szakmai irányítást más szemszögből kellene megközelíteni. A több nyugati

[14] 1994. évi XXXIV. törvény, 28. §.

országban sikerrel alkalmazott, pozitív példaként felhozható szakmai kamarának lehet szerepe, amely képes szakmai alapon ellátni az említett feladatokat. Ezzel párhuzamosan a Rendőrség ellenőrző szerepe megmarad, de a szakmát, képzéseket, továbbképzéseket és hatósági igazolványok kiadását, regisztrációt, nyilvántartást a kamara végzi. Ez a megoldás hatékonyan megosztja a magánbiztonsági területen adminisztratív és ellenőrző tevékenység során felmerülő és kötelező feladatokat, meghagyva a jogot az államnak, hogy ellenőrzést gyakoroljon a Rendőrségen keresztül. Ehhez a modellhez törvénymódosítás lenne szükséges, amely megváltoztatja a 2005. évi CXXXIII. törvényt.

Fizikai biztonsági rendszer

A fizikai védelmi rendszer egymásra vagy egymás mellé épülő eszköz vagy eszközök összessége, amely hatékonyan tudja biztosítani a védelmi képességet. Rendszerré akkor válik, amikor képes egymást hatékonyan kiegészítve ellátni a tervezésükkor kitűzött célt. A védelmi cél, illetve annak mértéke határozza meg, hogyan tervezzük egységes rendszerré a külön-külön is működőképes eszközeinket, melyek együttműködése során érjük el a magasabb biztonsági szintet. Preventív hatást ér el egy koncepcióját tekintve jól átgondolt biztonsági rendszer, amely a felhasználó szubjektív biztonságérzetét is javítja.

A biztonság optimális szintjének eléréséhez meg kell határozzuk, hogy mi a szükséges és elégséges szint. Ehhez kockázatelemzést kell végeznünk, amelynek során, mintegy a módszer eredményeként, az elérni kívánt biztonsági szint meghatározható.

Kockázatelemzés

Az objektumvédelem megszervezése és tervezése szempontjából az egyik legfontosabb feladat felmérni az összes lehetséges kockázatot, tekintettel arra, hogy a jövőbeni bekövetkezések esetlegesek, illetve több komponens együttállása, illetve egymásra hatása esetén következik be, amit szintén lehetetlen megjósolni, ezért az egyes komponensekre is figyelemmel kell lennünk. Az objektumban végzett tevékenység profilja alapján kockázatelemzést kell végezni, amely megelőzi a tervezést és a költségek meghatározását.[15] Kockázati modellek alkalmazását hívhatjuk segítségül, hogy minél életszerűbb legyen a kockázatkezelésünk. Tekintettel arra, hogy a biztonsági rendszer felépítése kockázatarányos, a kiépítés költsége arányosan növekszik a kockázattal és a védelmi rendszer szofisztikáltságával. A kockázatokat tehát valamilyen módon számszerűsíteni és a valósághoz minél jobban közelíteni szükséges kvalitatív és kvantitatív elemzéssel. A felmerülő kockázatok közül kiemelten kell kezeljük

[15] Horváth 2021.

a humán kockázatokat, mert minden rendszer leggyengébb láncszeme az ember, amely a „normál" kockázatok mértékét képes eltorzítani, ennek eredményeképpen a valós kockázat magasabb lesz a vártnál, illetve az előzetesen kalkuláltnál. A rendszerszintű, folyamatbeli intézkedések hivatottak csökkenteni a humán kockázatot, amelyeknek társulniuk kell egy hatékony ellenőrzési rendszerrel.

A rendszer megtervezéséhez azonosítjuk a felmerülő kockázatokat, tehát azt, hogy milyen előre látható, a biztonságot befolyásoló történés következhet be a normál működéshez képest, ezek az incidensek mennyi ideig tartanak, milyen megelőző vagy korrektív lehetőségünk van a hatások csökkentésére, semlegesítésére. Az objektum tervezése során a tevékenységgel kapcsolatos kockázatokra is készülünk. Amennyiben már meglévő objektumról van szó, ebben az esetben az adottságokhoz kell igazodnunk. Sok esetben átalakításra, a biztonsági szempontok és kockázatok figyelembevételére nincs lehetőség, illetve a költség/haszon elv nem mindig érvényesül. A tervezési időszakban a tevékenységi profil természetéből adódó kockázatokat is felismerjük és a biztonsági rendszert ezek figyelembevételével tervezzük meg. A tervezési időszakban szükséges biztonsági audit és kockázatelemzés elvégzése után értékelünk, és javaslatot dolgozunk ki a védelmi rendszer kialakítására. A kockázatokat rangsoroljuk a bekövetkezés valószínűsége alapján, illetve figyelembe kell vegyük a bekövetkezés során elszenvedett károk mértékét, valamint, hogy időben mennyire nehezíti meg és lehetetleníti el a normál működéshez történő visszatérést. Ez utóbbit, például a termeléskiesést bele kell számoljuk az elszenvedett kár mértékébe. A bekövetkezés valószínűségét múltbeli adatok, a vállalatcsoporton belül már bekövetkezett, biztonságot érintő események, illetve az iparágban a múltban tapasztalt incidensek elemzése alapján számíthatjuk.

1. táblázat: Kockázati katalógus

Kockázatok azonosítása és hatásaik, bekövetkezés megelőzése/Risk assessment and action plan													
Folyamat leírása/Process description								**Osztály/Department**			**Osztályvezető/ Department leader**		
Folyamat azonosító száma								**Dátum/Date**					
Azonosító szám/ID number	Folyamat (rész) megnevezése/Flow or part of the flow	Fellépő kockázat/Possibly risk	Detektálhatóság/Detectability	Bekövetkező kockázat hatásai/ Consequence if the risk occurs	Kockázat mértéke/Risk level LOW MEDIUM HIGH	Esemény bekövetkezésének okai/ Causes of occurence	Kontroll/Control				Határidő/Deadline	Teljesítettség %/Level of performance	Státusz/Status
							Bekövetkezés detektálása/ Detection of occurence	Intézkedések bekövetkezés esetén/Actions in the case of occurence	Megelőző intézkedések/Preventive actions	Felelős személy/Responsible name			

Forrás: a szerzők szerkesztése

A fentihez hasonló formanyomtatványt használva a kockázatok jól rendszerezhetők, áttekinthetők, a lista karbantartása során újabb kockázati elemek kerülnek bele, illetve tűnnek el attól függően, hogy a biztonsági és egyéb folyamatok milyen irányba tolják el az egyes elemeket. A cél, hogy minden kockázat minimálisra, illetve kezelhető mértékűre csökkenjen, és az újabb elemek felvétele minél előbb megtörténjen, ezzel egy időben pedig a megelőző intézkedések is megszülessenek. A kockázatelemzés lényegében dinamikus folyamat, tevékenység, szemlélet, amellyel dolgozni kell nap nap után az elvárt biztonsági szint fenntartásához.

Tervezés és felkészülés biztonsági eseményekre

A fizikai védelmi rendszerek struktúráját a védendő objektum vagy leendő objektum adottságaihoz igazítjuk. Ezeket földrajzi elhelyezkedés, környező épületekhez, településhez való viszony, domborzati viszonyok, tereptárgyak elhelyezkedése alapján mérjük fel, tervezzük meg (építészeti objektumvédelmi megoldások). Fontos bevonni a tervezési fázisba a biztonsági vezetőt, hogy a helyszín kiválasztását érdemben képes legyen befolyásolni a biztonsági szakmai szempontok érvényesítésével. A projektek nagy részében a helyszín kiválasztása inkább anyagi megfontolások alapján történik – például az, hol olcsó a telek, vagy hogy melyik önkormányzat ad olyan vonzó „csomagot", amely ösztönzi az új beruházásra készülő cégeket, vállalkozásokat.

A megrendelői igényeket és a rendelkezésre álló anyagi forrásokat is be kell határolni a tervezés során. A vállalatok sok esetben a biztonságra a legszükségesebb mértékben költenek, tehát alapvetően anyagi megfontolások alapján döntenek a beruházásról. A védelem szintjének megfelelő behatárolása a későbbiekben jelentkező problémákat előzhet meg.[16] Az alultervezés növeli a biztonsági kockázatot, a túlbiztosítás pedig aránytalan költségnövekedést hoz magával. A biztonsági rendszer tervezésekor kész forgatókönyvet[17] kell készítenünk arra vonatkozóan, hogy miként előzhetjük meg az azonosított kockázat vagy kockázatok által elszenvedett veszteséget, ezt hívjuk alapvetően preventív biztonsági tevékenységnek. Biztonsági incidens bekövetkezése esetén a helyreállítást, az eredeti vagy közeli állapothoz való visszatérést is terveznünk kell, kidolgozzuk a hasonló biztonsági események bekövetkeztekor követendő eljárásrendet, a bekövetkezett esemény tanulságai alapján módosítani kell az eredeti protokollt, amennyiben az szükséges. A kockázatok minél pontosabb azonosítása, illetve mértékének meghatározása szolgál a megfelelő szintű biztonság kidolgozásának alátámasztására és annak megvalósítására. Biztonsági esemény bekövetkezése esetén, a gyakorlati tapasztalatok alapján szükséges meg-

[16] Berek–Bodrácska 2010.

[17] Forgatókönyv-elemzés (Scenario Analysis): a lehetséges körülmények összegyűjtése, majd a felmerülő biztonsági kockázatok azonosítása, amelyek előfordulhatnak az egyes események együttes bekövetkezése során. IEC/ISO 31010:2009 Risk management. Risk assassment techniques magyar nyelvű változata, MSZ EN 31010 (2010), Kockázatkezelés. Kockázatfelmérési eljárások.

tenni a változtatásokat biztonsági szervezeti és eljárásrendi szinten is. Kritikus a reakcióidő, amely alapvetően attól függ, hogy milyen detektálási rendszer áll rendelkezésre, illetve hogy az e rendszerben helyet foglaló szereplők milyen hatékonysággal képesek ellátni a vészhelyzeti, illetve biztonsági folyamatokban megfogalmazott feladataikat. Ehhez szükséges a jártasság megszerzése, amely gyakoroltatás és tesztek végrehajtása útján lehetséges. Ennek egyik módszere a különböző, szimulált biztonsági eseményekre történő előzetes felkészülés, gyakoroltatás.

Tapasztalatunk, hogy a munkautasításokban rögzített feladatok megtanulása nem elégséges, mert a biztonságot fenyegető incidensekre a hatékony reagálás akkor lehetséges, ha időszakosan, célzottan beépítjük a gyakorlatokat a biztonsági személyzet magas szintű éberségének fenntartása érdekében. Vagyonbiztonság esetében ilyen lehet például a „trap test",[18] életbiztonságra vonatkozóan pedig a kiürítési gyakorlatok. Mindkét esetben a hangsúly a feladatok előre történő meghatározásában és a rendszeres gyakoroltatáson van. Itt szükséges megjegyezni, hogy a vagyonvédelemre az utóbbi években jellemző magas fluktuáció miatt oda kell figyelnünk, hogy a személyzet összes tagja le legyen oktatva és gyakoroltatva, különösen az új alkalmazottak, akikre lehet, hogy nem került még sor a tervezett időszakos tréningek során. Biztonsági incidens esetén annyira hatékony a szervezet reagálása, amennyire hatékonyan dolgozik a leggyengébb tagja a szervezetnek. Tehát törekednünk kell rá, hogy mindenkiből a lehető legtöbbet hozzuk ki az adott körülményekhez képest – ha egy szintre nem is hozhatjuk őket, hiszen különbözők az alapképességek. Az sem mindegy, hogy a biztonsági csapat mennyire állandó, mennyire tudnak jól együtt dolgozni. Éppen ezért törekedni kell rá, hogy minél kisebb mértékű legyen az elvándorlás és egy stabil stáb álljon rendelkezésre, összeszokott csapatmunkával. Tekintettel arra, hogy a fluktuáció magas lehet, ami rombolja a stabilitást és az állandóságot, a középvezetői szint (váltásvezetők)[19] megtartása és megbecsültsége megfelelő kell legyen, hiszen ők az alappillérei egy jól felépített élőerős csapatnak, és rajtuk múlik, milyen szakmai minőségű reagálóerőt sikerül menedzselni.

Ezen túlmenően meg kell vizsgálnunk a lehetséges technikai megoldásokat, amelyekkel segítséget nyújthatunk az élőerő munkájához a telephelyen, illetve bizonyos tevékenységeket lecserélhetünk-e, kiválthatunk-e a használatukkal. A fizikai védelmi szervezet felépítése, feladatok szétosztása, felelősségek tisztázása fontos alapkövei a hatékony működésnek.

Sennewald elképzelése alapján az alábbi alapelvek segítenek a kiépítésben:

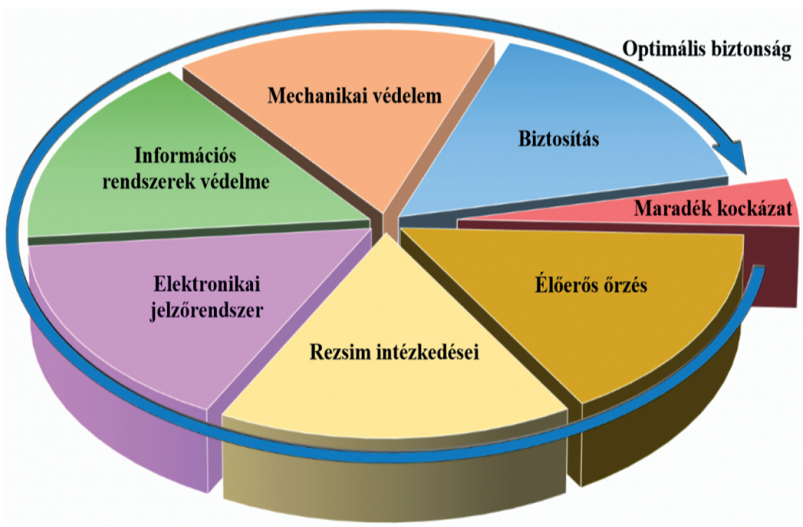
1. A munkát valamilyen logika szerint kell felosztani.
2. A hatásköröket és a felelősséget a lehető legvilágosabbá és legközvetlenebbé kell tenni.
3. Egy felügyelő csak korlátozott számú embert tud hatékonyan irányítani, és ezt a korlátot nem szabad túllépni. (Ezt az elvet vezérlési tartománynak nevezik.)

[18] Trap test: szimulált biztonsági incidens a rendszerek működésének ellenőrzésére.
[19] Váltásvezető: a biztonsági személyzet munkáját koordináló személy egy műszakon belül.

4. A szervezetben „a parancsegység elve” érvényesüljön.
5. Felelősség nem vállalható arányos hatáskör átruházása nélkül, és elszámoltathatónak kell lennie a rábízott feladatokért.
6. Az alegységek és a személyzet minden erőfeszítését össze kell hangolni, hogy együttműködjenek a szervezet céljainak elérésében.[20]

A biztonság megteremtésének eszközei

Létezik-e százszázalékos biztonság? Milyen módon tudjuk csökkenteni a kockázatokat? Az 1. ábra szemlélteti, milyen eszközöket veszünk igénybe a fizikai védelem megteremtéséhez. Az ábrán láthatjuk a maradék kockázatot, amely mindig ott lesz, függetlenül attól, mennyire szigorú és hatékony védelmi intézkedéseket vezetünk be. A maradék kockázat mértéke nem mindegy, és a rendelkezésre álló – az ábrán is látható – eszközökkel tudjuk csökkenteni azt. Az eszközök használhatósága, egymáshoz képesti aránya nem minden esetben ugyanannyi, sőt, általában eltér, néhány esetben pedig aránytalan egymáshoz képest, bizonyos helyzetekben pedig nem is mindegyiket vagyunk képesek használni, a védendő objektum adottságaitól függően. Ilyenkor meg kell erősítenünk a többi intézkedésünket annak érdekében, hogy kompenzáljuk a kiesett vagy kisebb hatékonysággal használható összetevőt.



1. ábra: Optimális biztonság

Forrás: a szerzők szerkesztése

[20] Sennewald 2011.

Megelőző védelmi intézkedések

Ezek az intézkedések garantálják, hogy a zárt folyamatok kiküszöböljenek minden olyan lehetséges hibát, amely vagyoni hátrányt, veszteséget eredményezhet. Minden szabály, kidolgozott folyamat természetesen annyira hatékony, amennyit betartanak belőle. Természetesen ebben az esetben is az ember a folyamat leggyengébb láncszeme. Nem minden esetben szándékos mulasztás vagy direkt károkozás kapcsán fordul elő az emberhez köthető hiba, lehet a folyamat kidolgozatlansága vagy az ellenőrzés nem megfelelősége, vagy ha valamely ponton a védelem nem az elvárt biztonsági szintet teljesíti. Ezt a folyamatok időnkénti ellenőrzésével, frissítésével, külső és belső auditok segítségével javíthatjuk, emellett fontos a megfelelő személyzet kiválasztása is az egyes munkafázisokhoz, védelmi intézkedések végrehajtásához, ellenőrzéshez.

Az ellenőrzési folyamatok implementálását és időnkénti felülvizsgálatát, az eredmények értékelését kiemelkedő fontosságúnak tartja a hatékony élőerős folyamatok fenntartása terén.[21]

Az emberi kockázat mérséklését célozza meg a kiválasztás folyamata. Mind a biztonsági szolgálat, mind pedig a vállalat dolgozóinak kiválasztása során igyekszik a cég minimalizálni azokat a biztonsági kockázatokat, amelyek azok kezelését nehezítenék, vagy akár el is lehetetlenítenék. (A kompetenciaalapú kiválasztás kiterjesztésével a biztonsági kockázatok szignifikáns mértékben csökkenthetők.)

Idetartozik még az egyes folyamatok kialakítása, felülvizsgálata. Felmerül a biztonsági szolgálat direkt bevonása egyes termelési, raktári folyamatokba. Ezek preventív jellegüknél fogva alkalmasak arra, hogy a rendszerszintű hibákra, biztonsági résekre felhívják a figyelmet, és korrektív intézkedések bevezetésével megelőzzék adott területen a vagyonvesztést.

A szolgálat bevonása lehet állandó vagy ideiglenes. A vagyonvesztés nem kizárólag szándékos, bűnös cselekmény következtében léphet fel, hanem az egyes folyamatok hiányosságaira is visszavezethetők, például az időszakos leltárak során feltárt esetlegesen fellépő hiányok, eltérések. Ez lehet könyvelési probléma, vagy az áru hanyag kezeléséből adódó „hiány", ami annyit jelent, hogy az adott anyagot a számára kijelölt helyen nem találják, vagy nem annyit találnak meg, amennyinek a könyvek szerint lennie kell. A rendszabályok betartása és betartatása minden dolgozó feladata, jóllehet klasszikusan gyártói környezetben a Biztonsági Osztálytól várják el kizárólag. A dolgozói felelősség és tudatosság kialakításáról a humán kockázat részben bővebben szólni fogunk.

Ahogy fentebb említettük, a védelem akkor hatékony, ha a rendelkezésre álló eszközök mindegyikét felhasználjuk, függően attól, hogy mik a helyi adottságok, körülmények. Tekintettel arra, hogy a technikai fejlődés a biztonsági területet sem kerüli el, a digitalizáció, illetve az információátvitel sebessége és a célba jutás ideje töredé-

[21] Christián 2014.

kére csökkent az évekkel ezelőttihez képest, a különböző forrásokból érkező adatok feldolgozása kikényszerítette, hogy azokat központosítva, lehetőleg fizikailag is egy helyen fogadják, dolgozzák fel, majd az elemzéseket követően viszontválaszt adjanak a helyzetértékelésnek megfelelően. A biztonsági központok tehát manapság szükségszerű velejárói egy modern, nagyméretű rendszer kialakításának, üzemeltetésének. Domján András a folyamatok frissítésével, átalakításával, a megváltozott környezet okozta fenyegetettségi szint változásával újabb és mélyebb ismeretek elsajátítását tartja szükségesnek a hatékonyság további fenntartása érdekében. Így a klasszikusan értelmezett, pusztán a jelenléten alapuló objektumvédelem már nem elégséges.[22]

Biztonsági központ

A régebben csak monitorszobának nevezett helyiség neve utal arra, hogy kizárólag a kameraképek fogadásával és megfigyelésével voltak megbízva az ott szolgálatot teljesítő munkatársak. A manapság SOC elnevezéssel *(Surveillance Operations Center)* megjelölt operációs központok története, gyökerei eredetileg a kiberbiztonsági tevékenységekhez kapcsolhatók, hiszen az első SOC-k *(Security Operations Center)* ezt a területet szolgálták ki, tevékenységük közvetlenül ide kapcsolódott.

A technika fejlődésével egyre több eszköz áll rendelkezésünkre, amelyeket a biztonsági szint emelésre használhatunk, azonban ezek alkalmasak arra is, hogy kaput nyissanak a kívülről érkező támadásoknak. A biztonságos üzemeltetés tehát szélesebb körű, és új ismereteket kíván meg az üzemeltető személyzettől.[23]

A biztonsági központok elterjedése először az informatikai rendszerek felügyelete területén valósult meg, elsősorban az angolszász országokban. Az Európai Unió javítani kívánja tagjai között az együttműködést a kibervédelem hatékonysága terén, ezért a biztonsági központok egyfajta együttműködését irányozta elő, nem utolsósorban a kutatás-fejlesztés elősegítése céljából. Az ennek jegyében kiadott rendelet 2021 és 2029 között kívánja meg a közös tevékenységet a tagállamoktól, hacsak a rendelet felülvizsgálata során másként nem rendelkeznek, tehát ez a határidő kitolható annak függvényében, hogy milyen szakmai eredmények születnek, illetve annak, hogyan alakulnak a fenyegetettségi, a kitettségi és a kiberbiztonsági kockázatok.

A 2013-ban kiadott stratégiát 2017-ben vizsgálták felül, a „Közös közlemény az Európai Parlamentnek és a Tanácsnak Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése" című anyagban. Ekképpen értékelték az Európai Unió előrehaladását, amelynek főbb megállapításai a következők:

[22] Domján 2017.
[23] Tóth 2018.

- 2017 őszére a Bizottság egy kiberbiztonsági csomagot ad ki a tagállamok részére, bemutatva a jól bevált gyakorlatokat.
- Erősíteni kell az együttműködést és az információcserét a közszféra és a magánszféra között.
- A kritikus ágazatokban látható előrelépés az információcserét illetően. Megalakult az Európai Repülési Kiberbiztonsági Központ, illetve az energetikában is létrehoztak információcsere és -elemző központokat.
- Az ENISA[24] támogatja a folyamatokat.[25]

A fentiek alapján láthatjuk, hogy a biztonság, ezen belül pedig a kiberbiztonság nemcsak a privát szférát foglalkoztatja, hanem a kormányzatok is gondot fordítanak rendszereik megvédésére, hiszen a közfeladatok ellátásának biztosítása kritikus infrastrukturális kérdés. A kiberbiztonsági központok tehát jelentős szerepet játszanak ma is, és várhatóan a jövőben még nagyobb nyomás alatt fognak dolgozni a környezetünkben tapasztalható feszültség és háborús események miatt, hiszen annak egy része láthatatlanul, a kibertérben zajlik. Az jól kötrvonalazható, hogy milyen speciális képességekkel kell rendelkeznie egy CSOC-nak *(Cyber Security Operations Center),*[26] amelyek alapjában határozzák meg az ott folyó tevékenységet, és a személyzet képzettségére, szakmai tapasztalatára is speciális igényeket támasztanak. Ehhez képest egy fizikai védelmi képességekre berendezkedett biztonsági központ tevékenységében eltérő, a valódi fizikai támadások megelőzésére, elhárítására hivatott. Mivel azonban a fizikai biztonsági központban is IT-eszközöket alkalmazunk, azokat is védeni kell a kibertámadásokkal szemben, az informatikai szakembereket be kell vonni a központ tervezési és kivitelezési munkálataiba, hogy a központ sérülékenységeit feltárjuk, illetve informatikai eszközökkel védjük azt meg. Alapos tervezés előzi meg a fizikai biztonsági központ kialakítását és épületen belüli integrációját. A központ fizikai védelméhez annak elhelyezésekor figyelemmel kell legyünk az épület infrastrukturális kialakítására, például nem célszerű vizesblokk vagy vízcsőhálózat közelében felépíteni a központot, hiszen egy esetleges csőtörés esetén a helyiség a kiáramló víz miatt használhatatlanná válhat, extrém esetben zárlat következtében súlyos károkat szenvedhetnek a berendezések, illetve a személyzet testi épsége is veszélybe kerül.

Az SOC-védelem[27] alapvető eszközei:

- fizikai elhelyezkedés;
- falazat/plafon védelme;
- üvegfelületek védelme (fizikai és belátás elleni);
- bejutás elleni védelem;

---

[24] ENISA: European Union Agency for Cybersecurity – Európai Uniós Kiberbiztonsági Ügynökség.

[25] Közös Közlemény az Európai Parlamentnek és a Tanácsnak, Ellenállóképesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése, Brüsszel, 2017. szeptember 13.

[26] CSOC: Cyber Security Operations Center – Kiberbiztonsági Védelmi Központ.

[27] MSZ EN 50 518: Riasztásfogadó központok.

- a bejutás korlátozása szabályokkal, intézkedésekkel;
- beléptető;
- behatolásjelző;
- kamerarendszer;
- interkom;
- pánikgomb;
- belső kommunikációs rendszer és alternatív kommunikációs csatornák;
- vészhelyzetekre, incidensekre előre kidogozott folyamatok.

2. ábra: Modern SOC

Forrás: a szerzők felvétele

Hatékonyság

A fizikai védelmi rendszerek hatékonyságának mérése fontos szempont a megbízó oldaláról, hiszen amennyiben egy megfelelően felépített és szofisztikált rendszerről van szó, azt szeretnék látni, hogy a befektetett és a fenntartásra költött forintok megtérülnek, de legalábbis elérik a kitűzött célokat. Arra tekintettel, hogy a biztonságra általában csak „pénznyelőként" tekintenek, fontos megteremteni a hatékonyság méréséhez szükséges feltételeket. Klasszikusan tehát ez is egy olyan szakterület – sok más mellett –, ahol nem elég jól dolgozni, azt meg is kell valamilyen módon mutatni. A preventív biztonság hatékonyságmérése sok összetevős.

Amennyiben a biztonsági rendszer kiépítése vagy megerősítése egy adott vállalatnál reaktív elemként valósult meg, úgy azt mindenképpen tudni érdemes, mi vál-

totta ki ezt a reakciót a menedzsment részéről. Ezek általában a biztonságot érintő jelentősebb események köré csoportosíthatók, jellemzően nagyobb vagyonvesztés, leltár eltérése/hiánya, illetve nemzetközi vállalat esetében az anyacég belső szabályzói azok, amik kiváltják egy hatékonyan működő objektumvédelmi rendszer kialakításáról meghozott döntést. A hatékonyságot tehát valamilyen kiinduláskori helyzethez kell viszonyítsuk. A KPI-k[28] meghatározásánál tehát figyelembe kell vegyük a speciális helyi viszonyokat. A KPI-kat alapvetően két csoportra osztanám. Az egyik esetében az élőerős őrzés teljesítményét mérem, a másik pedig a technikai biztonsági rendszer működését vizsgálja különböző szempontok alapján. Itt fontos megjegyezni, hogy mind az élőerő, mind pedig a technika működhet saját üzemeltetésben, valamint kiszervezett tevékenységként, mintegy szolgáltatásként.

2. táblázat: KPI

	Dátum	**Név**	**Poszt**	
	KPI	**Leírás**	**Értékelés leírása**	**Értékelés**
6	Poszt ellenőrzése – Professzionalizmus	Felszerelés teljes és működőképes (rádiók, lámpák stb.) Semmilyen tiltott eszköz (olvasási anyag, étel, e-eszközök stb.) Professzionális megjelenés (egyenruha stb.) Tiszta terület, rendetlenségtől mentes, lehetővé teszi a munkát Speciális felszerelés jelen van (pecsét, vágók, esőkabátok stb.)		0
7	Poszt ellenőrzése – Kiterjesztés / Eszkaláció	Ki, mi, mikor, hol, miért, hogyan terjeszti ki x szituációt: tűz, WPV, lopás, SP Annak megértése, hogy mit jelentsen, és mit terjesszen fel a vezetőknek felülvizsgálatra, eszkalációra	A/B = %; 69% vagy kevesebb = NEM MEGFELELT	0
8	Poszt ellenőrzése – Kritikus feladat	A pozíciófeladatok teljes bemutatása úgy, mint a kijárat ellenőrzése, szállítási dokk, POD és plombálási folyamat, kapunál kamion-felülvizsgálat, hozzáférés ellenőrzése, laptop/telefon ellenőrzése, NPI-terület stb.	A/B = %; 69% vagy kevesebb = NEM MEGFELELT	0
9	Poszt ellenőrzése – Kockázattudatosság	Konkrét kockázat tudásának és tudatosságának bemutatása a poszton, úgymint alkatrészlopások magas rizikója, valószínű problémák a rakodásokkal/beérkezésekkel, a „helyi" kockázat definiálása a poszton, úgymint hamis belépőkártya, tiltott tárgy bevitele/kihozatala stb.	A/B = %; 69% vagy kevesebb = NEM MEGFELELT	0
10	Poszt ellenőrzése – SOP	A vonatkozó sztenderdek és SOP bemutatása Badge, jogosult személyek, nyomonkövetési papírmunka stb. A papírmunka naprakész, pontos és olvasható	A/B = %; 69% vagy kevesebb = NEM MEGFELELT	0

Forrás: a szerzők szerkesztése

[28] KPI (Key Performance Indicators): kulcsfontosságú teljesítménymutatók.

A magyar fizikai védelmi piacon az utóbbi elterjedettebb, illetve létezik még egyfajta „kombó" megoldás is, miszerint az élőerős őrzést vagyonvédelmi cég látja el, a technika pedig saját üzemeltetésben van. A fentiektől függetlenül a hatékonyságmérés elengedhetetlen akkor is, ha bármelyik tevékenység saját szervezésben történik. Ilyen esetekben a Biztonsági Osztály mintegy „belső szolgáltatóként" tevékenykedik, szolgálja ki a biztonsághoz kapcsolódó folyamatokat, tevékenységeket. A KPI-k eredményétől függően lehet meghatározni a közép- és hosszú távú célokat, illetőleg megtenni korrektív intézkedéseket, amennyiben azok szükségesek.

A hatékonyság mérésekor, a mérőrendszer kialakításakor súlyozni kell, hogy mik azok a mérőpontok, amelyek hangsúlyosak, és igenis hatással vannak a napi operatív munkára és a biztonsági szintre, illetve melyek sorolhatók hátrébb, mert közvetlen hatásuk nincs a biztonságra. Például fontos, hogy egy vagyonőrnek kifogástalan legyen az egyenruhája a napi munka során, de ennél jóval előrébb van a rangsorban, hogy a biztonsági zóna elhagyásakor a dolgozók átvizsgálása szabályszerűen és szakszerűen történjen, hiszen érdemben ez befolyásolja a biztonsági szintet.

Összefoglalás

A fizikai védelmi rendszerek, jóllehet külön-külön is elláthatnak bizonyos részfeladatokat és sok esetben egyes rendszerelemek hangsúlyosabban vesznek részt a fizikai biztonság megteremtésében és fenntartásában, ám leghatékonyabban egymásra épülve tudják kifejteni tevékenységüket, és végeredményben ez hozza a várt hatást, vagyis a szükséges és elégséges biztonsági szint fenntartását. Ma már a technika olyan fejlettségi szintet ért el, amely képes élő időben detektálni, más rendszereknek átadni, feldolgozni az információkat, analitikus funkcióiknak köszönhetően pedig kiszűrni azokat az eseményeket, amelyek nem tartoznak a védelmi reakciót kiváltó történések körébe, ekként tehát csak a valós, a biztonságot veszélyeztető eseményekre koncentrálhat az élőerő is, fenntartva ezzel az éberséget azáltal, hogy minél kevesebb téves riasztásra kell reagálniuk.

Napjainkban, amikor a vagyonőrök megfelelő szintű kiképzése, a jártasság fenntartása, illetve maga a toborzás is kihívásokkal küszködik, fontos „előremenekülési" lehetőség a technikai megoldások alkalmazása a létesítményvédelem területén. Az ez irányú fejlődés törtetlen, igaz, sok megoldás még kísérleti fázisban van, illetve ami még visszatartó erő a beruházóknak, az új technológiák sok esetben igen magas költségei. Jó példa erre az úgynevezett robotjárőr alkalmazása, amely ugyan első látásra meghökkenést kelthet a járókelőkben és a vállalat dolgozóiban, de hatékonyságban felveszi a versenyt az emberrel, ám ebben a pillanatban hazai körülmények között még biztosan nem piacképes, hiszen jelenleg többszörösébe kerül a fenntartása egy vagyonőr költségeihez képest.

Felhasznált irodalom

A Rendőrségről szóló 1994. évi XXXIV. törvény

Berek Tamás – Bodrácska Gyula (2010): Az élőerős őrzés az objektumvédelem építőipari ágazatában. *Hadmérnök*, 5(4), 38–49.

Christián László (2014): *Létesítményvédelem*. Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar.

Domján András (2017): A kiemelten védett objektumok biztonsága a fenyegetettség tükrében. *Hadmérnök*, 12(3), 26–36.

Horváth Tamás (2021): Mechanikai védelem mint késleltetés a fizikai védelemben. *Hadmérnök*, 16(1), 23–32. Online: https://doi.org/10.32567/hm.2021.1.2

Lippai Zsolt (2021): Az üzemőrségtől, a fegyveres biztonsági őrségig. In Kovács István – Frigyer László – Tirts Tibor (szerk.): *Globális kérdések – globális válaszok: rendészettudomány a hallgatók szemével*. Budapest: Magyar Rendészettudományi Társaság, 133–144.

Lippai, Zsolt – Zágon, Csaba (2021): The Borderline Between Private and Public Security. *AARMS*, 20(3), 5–19. Online: https://doi.org/10.32565/aarms.2021.3.1

Maslow, Abraham H. (1954): *Motivation and Personality*. [H. n.]: Harper and Row.

Sennewald, Charles A. (2011): *Effective Security Management*. [H. n.]: Butterworth-Heinemann.

Tiszolczi Balázs Gergely (2019): Fizikai biztonsági kontrollok tervezésének és alkalmazásának gyakorlata az ISO/IEC 27001 szabvány elvárásainak tükrében. *Magyar Rendészet*, 19(2–3), 23–32. Online: https://doi.org/10.32577/mr.2019.2-3.12

Tóth Attila – Tóth Levente (2014): *Biztonságtechnika*. Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar.

Tóth Levente (2018): A komplex objektumvédelem kihívásai napjainkban. *Bolyai Szemle*, (1), 35–45.

ABSTRACT

Physical Security Systems and Surveillance Operations Center

Frigyes GUBICS – Tamás HORVÁTH

Using modern physical security systems started when economy system changed in Hungary, around 1990. It was a chance to develop security infrastructures with new and never seen technical solutions. Security industry also improved and requested to get new knowledge to implement and operate new systems. The industry made and got wider by capitalization in the country. Private property system evolution followed by the security culture formalization as well. This kind of culture came from multinational companies as headquarters and other country experiences were summarized and brought into Hungarian sister sites. Complexity of physical security systems, automated working order requested centralized control, gather of information and analization, quick reactions and proactive actions with tranparency, forced to make surveillance operations center as key participant in the field of high level of security services.

Keywords: *physical security, surveillance operations center, risk management, asset protection*