Tóth Levente

A komplex objektumvédelem kihívásai napjainkban

A technológiai fejlődésnek köszönhetően egyre szélesebb eszközpark áll rendelkezésre a biztonságtechnikai piacon. A fejlesztések egy része azonban nemcsak biztonságunk növelésére szolgál, hanem ezekkel vagy ezeken keresztül újabb támadásoknak lehetünk kitéve. A megnövekedett eszközválaszték és az egyre intelligensebb rendszerek nagyobb szakismeretet, pontosabb tervezést, precízebb kivitelezést és karbantartást kíván a kivitelező cégek részéről, míg gondosabb és felkészültebb üzemeltetési feladatokat támaszt a felhasználókkal szemben. A rendszerek nagyságával párhuzamosan nő a bonyolultságuk, az összetettségük és a keletkező információk mennyisége. A hatékony üzemeltetés biztosítása érdekében különböző döntéstámogató algoritmusokat és szoftvereket fejlesztenek ki. Ezek egy része olyan kényelmi szolgáltatást is nyújt, amely újabb támadási felületet eredményezhet. Az új technológiák megjelenésével az objektumvédelem komplexitása további aspektusokkal egészül ki.

Kulcsszavak: drón, integrált felügyeleti rendszer, döntés támogató szoftver, M2M, IoT, UAV

Bevezetés

A rendszerváltozást megelőző időszakban a tulajdontárgyak döntő többsége, a termelőeszközök nagy egésze az állam tulajdonában volt. Ebből kifolyólag az állam mint közhatalmi szervezet látta el az állami vagyonvédelem mellett a tulajdonosi vagyonvédelmi feladatokat is. A rendszerváltást követően a tulajdonszerkezet gyökeres változáson ment keresztül. Az állami tulajdon hányada jelentősen csökkent, és a magántulajdon lett a gazdaság meghatározó tényezője. Ebben a helyzetben viszont az állam a magántulajdonosokat – egészen szűk kivételtől eltekintve – már nem kötelezheti vagyonuk védelmére, mert ezzel indokolatlanul beavatkozna a tulajdonos jogaiba. „Nemzetközi tendencia a magánbiztonság térnyerése, expanziója, amelynek hátterében többek között a rendőrségek kapacitásainak jobb eloszlása és a költséghatékonyság áll. Az államok, kormányok rájöttek, hogy a rendészeti monopólium szigorú fenntartása mellett, bizonyos feladatok, külö-

nösen egyes háttértevékenységek privatizálhatók, kiszervezhetőek." [1: 15] A fenti okok alapján hazánkban megváltozott a vagyonvédelem szabályozásának eddigi koncepciója.

A tulajdonosok részére az állam nem ír elő védelmi kötelezettséget, hanem a megalkotott és kihirdetett jogszabályok alapján lehetőséget biztosít a vagyonuk megvédésére. A különböző társadalmi csoportok közötti vagyoni különbségek növekedése, az országhatárok megnyitása, a szervezett külföldi bűnszövetkezetek megjelenése, a hazai bűnszövetkezetek kialakulása és megerősödésének természetes következményeként a mindennapi élet során egyre inkább előtérbe került a közrend, a közbiztonság helyzete, a bűncselekmények során megsokszorozódott vagyon elleni bűncselekményekkel szembeni hatékony védelmi rendszerek kialakításának igénye. Magyarország – a korábbinál sokkal intenzívebb – nemzetközi szerepvállalása, az Észak-atlanti Szerződés Szervezetéhez (NATO), illetve az Európai Unióhoz (EU) való csatlakozása egy új veszélyforrást idézett elő, amely tovább növelte a hazánk ellen irányuló külső fenyegetettséget is, amely elsősorban a modernkori terrorizmusban ölt testet. [2: 9]

A komplex vagyonvédelmi rendszerek

A bevezetőben felsorolt okok és indokok miatt egyre nagyobb igény jelentkezik a teljes körű vagyonvédelem kiépítésére, illetve a meglévő biztonságvédelmi rendszerek folyamatos fejlesztésére, bővítésére. E feladat megvalósításában kiemelkedő szerepet játszanak a komplex vagyonvédelmi rendszerek, azaz a mechanikai védelem, az elektronikai jelzőrendszerek, valamint az élőerős védelem és a különböző szervezeti intézkedések összessége. A felsorolt tényezők egy esetleges kárkövetkezmény enyhítését szolgáló biztosítással együtt optimális biztonságot képesek nyújtani a felhasználóknak. Teljes körű, 100%-os védelem még így sem valósítható meg, ezért számolnunk kell egy maradék kockázattal, amely a magánszemély vagy egy gazdasági szervezet esetén a menedzsment tudatos kockázatvállalását jelenti azzal, hogy az egyes veszélyforrásokra nem, vagy csak részben reagál védelmi megoldással. E kockázat egy káreseményt követően a visszaállítás során az egyénre vagy a gazdasági szervezetre háruló költségeket jelenti. „Kijelenthetjük, hogy a védelemmel szemben megfogalmazott követelmény kettős, egyfelől elvárás, hogy a védelem csökkentse a vagyon elleni szándékos jogellenes cselekmény elkövetésének valószínűségét a minimálisra, másfelől a cselekmény bekövetkezte esetén az elkövető kockázatát pedig növelje a maximálisra." [3: 8]

Az elektronikai jelzőrendszer, mint neve is mutatja, nem sorolható a klasszikus védelmi rendszerek közé. Ez a rendszer „csak" jelzi a behatolás tényét, illetve annak szándékát. Ezeknek a rendszereknek a feladata a különböző biztonságot veszélyeztető cselekmények detektálása, jelzése, az események nyomon követése, rögzítése, az illetéktelen személyek belépésének vagy a gépjárművek behajtásának gátlása, a különböző tárgyak, áruk, cikkek

be- és kivitelének ellenőrzése, valamint különböző – általában – automatikus vezérlések végrehajtása. Így tehát az elektronikai védelem a mechanikai-fizikai védelemmel szemben nem ad valós védelmet, hiszen nem tudja feltartóztatni a behatolót. Csupán jelzi az eseményt az élőerős védelemnek, aminek a feladata a bűncselekmény megakadályozása vagy az épületbe bejutott személy feltartóztatása, elfogása, vagyis a helyszínen való intézkedés. Az intézkedés végrehajtása viszont tervszerűséget, szervezettséget igényel. Ehhez elengedhetetlen az élőerős tevékenységet szabályzó rezsim (szervezeti) intézkedések megléte. [4]

A vagyonvédelem komplexitása, a védelmek közötti összefüggés úgy határozható meg, hogy az elektronikai védelemnek olyan előrejelzést kell biztosítania, hogy a mechanikai védelem képes legyen visszatartani a behatolni szándékozót az élőerős védelem kiérkezéséig. A védelmi rendszer kialakítása a védelem megfelelő ellátását szolgálja. A védelem folyamatos, komplex tevékenység, amelynek célja, hogy biztosítsa a biztonság kívánatos szintjének elérését, illetve fenntartását. [5]

Az objektumok biztonsága olyan állapotot, helyzetet jelent, amelyben az ott-tartózkodók életét, testi épségét, az anyagi javak és adatok létét, sértetlenségét, továbbá az objektum belső rendjét és működését sem külső, sem belső tényező nem sérti vagy veszélyezteti.

A biztonságot veszélyeztető veszélyforrások lehetnek természeti (villámcsapás, vízbetörés stb.) vagy technológiai eredetűek (elektromos kontakthiba, rosszul működő őrlángérzékelő stb.), illetve emberi közreműködéssel végrehajtott cselekmények. Ez utóbbi lehet tudatos (szándékos jogellenes magatartás) vagy gondatlan (többnyire figyelmetlenségből, hanyagságból keletkező veszélyek). A biztonságot veszélyeztető, emberi közreműködéssel szándékosan végrehajtott cselekmények közé sorolhatjuk a betörést, a lopást, a rablást, de tágabb értelmezésben az informatikai rendszerünk ellen elkövetett feltörést és adathalászatot is.

A felsoroltakból is jól látszik, hogy számtalan tényező veszélyezteti a biztonságunkat. Ebből kifolyólag a védelmi rendszerek eszközválasztéka is rendkívül széles skálát képez, így számos megvalósítási lehetőség áll rendelkezésre az objektumok komplex vagyonvédelmének megtervezésére és kialakítására.

Technológiai fejlődés

A technológiai piacon az 1950-es évek végétől, az integrált áramkörök (IC) megjelenésétől látványos és gyors fejlődésnek lehetünk szemtanúi. Az IC-k integráltsági foka 1,5 évente megduplázódik (Moore[1]-törvény). Ez a fejlődés kihatással van a biztonságtechnikai

[1] Gordon E. Moore, az Intel egyik alapítója.

piacra is. Számos, régebben mechanikai érzékelési elven működő berendezést mára már processzoros jelfeldolgozású szenzorok váltották fel (például üvegtörés és rezgésérzékelők). Különböző érzékelési technológiákat dolgoztak ki, amelyek tovább bővítették az objektumvédelem technikai eszköztárát. A megnövekedett eszközválaszték nagyobb szakismeretet, pontosabb tervezést, precízebb kivitelezést és karbantartást kíván a kivitelező cégek részéről, míg gondosabb és felkészültebb üzemeltetési feladatokat támaszt a felhasználókkal szemben. A rendszerek nagyságával nő azok bonyolultsága, összetettsége, ezzel együtt a hibaforrások és a kezelési hibák száma.

A különböző elektronikai jelzőrendszerek már nem csak önmagukban, azaz a rendszer alkotóelemeivel kommunikálnak, hanem képesek más rendszereknek információt továbbítani, vagy onnan fogadni és értelmezni. Megjelentek a piacon az úgynevezett M2M[2]-eszközök, amelyek intelligens módon képesek a keletkező adatokat feldolgozni és továbbítani más gépekhez vagy a felhasználóhoz. Mára már a rendszerek egymásba ágyazása, integrálása is sokkal mélyebben (szoftveres úton) történhet meg, szemben a tíz évvel ezelőtti relés kimenetek és bemenetek (hardveres) összekapcsolásával.

A komplex objektumvédelem kihívásai

A technológiai fejlődésnek azonban vannak árnyoldalai is. Egyrészt az új, korszerű berendezések nem csak a védelem, az elhárítás oldalán jelennek meg, másrészt pedig pont a kifelé zajló kommunikáció teremtett egy rést a kívülről jövő támadhatóságban. Szintén a fejlődésnek tudható be, hogy igen nagy mértékben megnövekedett az informatikai úton előálló adathalmaz, amelyek között lehetnek személyes, minősített vagy éppen ipari kémkedésnek kitett adatok is. Ebből fakad, hogy a védendő materiális értékek, javak egyre inkább kiegészülnek kevésbé kézzel fogható, de egyes esetekben igen nagy értéket képviselő információkkal, adatokkal is. Mindezekből következik, hogy tágabb értelmezésben a komplex objektumvédelem kialakításánál nemcsak a fizikai úton, erőszakos módon történt anyagi javak megszerzése ellen kell védekeznünk, hanem ugyanilyen fontos a kiberbűnözés elleni védekezés is.

A 21. század új, biztonságvédelem szempontú kihívása a pilóta nélküli repülőgép (UAV[3]), vagy más néven drón.[4] Bár katonai repülésre az 1960-as évek elejétől alkalmazzák, polgári elterjedése néhány éve számottevő.

Magyarországon polgári védelem, katasztrófavédelem, közbiztonság, közrendvédelem céljára több mint 10 éve használják. [6: 130] Az eszköz segítséget nyújt(hat) a zöldhatár figyelése során, az árvízi védekezésben, az erdőtüzek felderítésében, a közlekedési

[2] Machine-to-Machine: gépek közötti adatkommunikációs technológia.
[3] Unmanned Aerial Vehicle: pilóta nélküli repülőgép.
[4] Az angol drone szóból, jelentése here (méh).

helyzet ellenőrzésében, az elfogások, rajtaütések tervezésében és ezek távoli megfigyelésében, valamint a tömegrendezvények biztosításában. [7: 71–72]

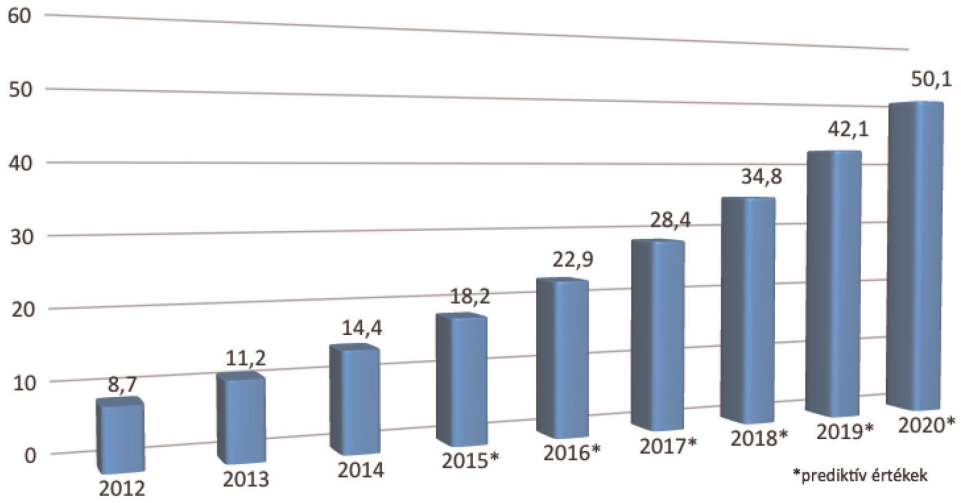
Az eszköz hazai magánbiztonsági felhasználása még nem számottevő, pedig ezen a területen is számos feladatra bevethető. Hatékonyan és jól képes támogatni a nagy kiterjedésű objektumok kerítésvédelmi rendszerét. A rendszer jelzése esetén a célra repülve, gyorsan kiszűrhetjük a téves riasztásokat, illetve rögzíthetjük és nyomon követhetjük az eseményeket. Az őrzési szolgáltatás minőségének javítása érdekében használhatjuk őrjárat ellenőrzésére, vagy éppen ennek kiváltására, azaz kültéri járőrözés végrehajtására.

Fontos kiemelni, hogy a drónok nem csak védelmi berendezésként használhatók. Napjainkban sokkal nagyobb kihívást jelent az ellenük történő védekezés. Jelenleg az Európai Unióban nincs egységes szabályozás a drónok használatáról (ennek tervezett bevezetése: 2018), bár az Európai Repülésbiztonsági Ügynökség (EASA[5]) már kidolgozott egy szabályozási javaslatot. Az átmeneti időszakban a tagállamok egymástól független, nemzeti szabályozásba kezdtek.

Független a törvényalkotás miként jétől, annak megjelenése csak a „jó szándékú" reptetést szabályozza és nem gátja a különböző bűncselekmények végrehajtására bevetett drónoknak. Jelenleg a kereskedelemben kapható drónok sebessége már meghaladja a 110 km/h-át. A jelenlegi megfizethető árú drón észlelési technológiák (radar, termokamera, hang) csak maximum egy-két kilométeres hatótávolságot tesznek lehetővé. Ez azt jelenti, hogy ilyen sebesség mellett kb. 1 perc áll rendelkezésre az észleléstől a megsemmisítésig. Ez még kevesebb is lehet, ha a drón már olyan területre ért, ami felett nem lehet lelőni (például tömegrendezvény).

A technológiai fejlődés másik nagy kockázata biztonság szempontból az egyre nagyobb számban megjelenő IoT,[6] azaz az interneten keresztül elérhető eszközök. A Cisco Internet Business Solutions Group (IBSG) tanulmánya 2020-ra 50 milliárd IoT-eszközt prognosztizál. [8] Ezzel egyetértésben, de ezen is túlmutat az SMA[7] 2014-es kutatása, amely 2035-re 1000 milliárdra prognosztizálja az IoT-eszközök darabszámát. [9]

[5] European Aviation Safety Agency.
[6] Internet of Things: Dolgok Internete, de használatos még az „Internet ott tárgyak" kifejezés is.
[7] Strategy Meets Action.



1. grafikon – IoT-eszközök darabszáma (milliárdban) 2012 és 2020 között [10]

Az eszközök választéka már jelenleg is széles körű. A már szinte hétköznapinak számító okostévén túl találhatunk okoshűtőszekrényt, -mosógépet, -kazánt, de még -kávéfőzőt is. Egyre népszerűbbek az „intelligens ház" (smart home) kialakítások, amelyeknek szerves részét képezik az IoT-eszközök. Egy ilyen rendszernél interneten keresztül mobiltelefon vagy táblagép segítségével vezérelhetjük a különböző otthoni berendezéseinket, vagy felügyelhetjük a fűtést/hűtést, a világítást, a kamerát vagy a behatolást jelző rendszereinket. Ezek a funkciók nagyon kényelmesek, viszont számos veszélyt hordoznak magukban. Mobiltelefonunk ebben a szerepkörben egy teljesen új értelmezést nyert. Ebbe az eszközbe integrálódik a teljes biztonságunk. Ezen egyetlen eszközön keresztül elérhetjük otthoni és céges levelezéseinket, hálózati tárolónkat, fizethetünk vele vagy felügyelhetjük a kameráinkat, ki- és bekapcsolhatjuk a riasztónkat, illetve használhatjuk beléptetőrendszerben kártya helyett, de vezérelhetjük vele a bejárati ajtónk zárját is. Egyes gépkocsiknál már lehetőség van a telefonon keresztüli nyitásra, illetve zárásra. Mindezen funkciókhoz hozzáférhetünk egy kifigyelhető jelkód vagy a születési évünkre beállított jelszó birtokában.

1. ábra – Mobiltelefonos applikációk (a szerző saját szerkesztése)

Ráadásul ez csak az egyik veszélyforrás. A piaci pozíciók stabilizálása érdekében a gyártók felgyorsított fejlesztési, gyártási és tesztelési fázisokat alkalmaznak, amelynek következtében nemcsak a minőség, a tartósság szenved csorbát, hanem kevesebb figyelem jut az eszközök kiberbűnözéssel szembeni védelmére is. Ez utóbbi pedig közvetlenül vagy közvetve is súlyos kockázatot hordoz egy biztonsági rendszer komplexitásában. A gyártó által véletlenül (vagy szándékosan) nyitva hagyott rejtett hozzáférés (backdoor) közvetlen lehetőséget biztosít a teljes kontroll átvételére az adott eszköz felett. Közvetve pedig – e bejáratot kihasználva – megnyílik a lehetőség más, szintén az adott belső hálózatra csatlakozó eszközök elérésére is, amelyről azt gondolnánk, hogy biztonságban van, mivel direkt módon nem csatlakozik az internetre. A cseh Biztonsági Információs Szolgálat (BIS) már a 2014-es évi jelentésében az alábbiakat írta: „Az elmúlt évekhez hasonlóan, a BIS olyan készülékek és technológiák felderítésére összpontosított, mely a biztonságot fenyegető potenciális veszélyt rejt magában. 2014-ben a BIS vizsgálata kiterjedt többek között az IP-kamerákra is (hálózatos kamerákra, webkamerákra). A BIS-hez eljutott információkat megerősítették a saját megállapításaik is, mely szerint egy IP-kamerában olyan firmware-t találtak, amely nem dokumentált rendszergazda fiókot (backdoor) is

tartalmazott. A hálózatra történő csatlakozást követően a kamera kommunikálni próbált egy előre beállított domain szerverrel, ami valószínűleg egy nagyobb felhőtároló része lehetett. Hackerek a böngészőbe beírt lekérdezési karakterlánc segítségével a fent említett backdooron keresztül elérhetik a kamerát." [11]

A fenti észrevétel nem egyedi. Az interneten több olyan esettel is találkozhatunk, ahol – többnyire kínai – gyártókat támadnak azzal, hogy adathalászás vagy kémkedés céljára fenntartott backdoorokat tartalmaz az eszközt működtető firmware-jük. [12] [13]

Amennyiben a szándékosságot kizárjuk, akkor feltételezhetnénk azt is, hogy a biztonságtechnikai eszközgyártók szoftverfejlesztői kevésbé jártasak a szoftverírásban, vagy hanyagság, időhiány miatt nem írják meg megfelelő biztonsági szinten a programot. Bár találhatunk erre is példát (például amikor a hozzáférési jelszót titkosítás nélkül, sima szövegként tárolják, vagy webes hozzáférés esetén egyes aloldalak autentikáció nélkül is elérhetők), mégsem csak erről van szó. 2016 nyarán került napvilágra, hogy a világ 67 országában jelenlévő informatikai nagyvállalat eszközeiben szoftveres biztonsági rést találtak, amely több mint 120 különböző típusú berendezést, köztük biztonságtechnikai eszközöket és kamerákat is érint. [14] A gyártó a honlapján elismerte a hibát, [15] és körülbelül másfél hónap alatt megszüntette a biztonsági rést.[8] Ekkora cégnél, ilyen fejlesztői háttérrel nem beszélhetünk hozzá nem értésről. Ebben az esetben egy beépített kényelmi szolgáltatás (az eszközök távoli elérése a cég szerverén keresztül) okozta az alapproblémát. A túl sok eszközhöz rendelt funkció, a beállítási lehetőségek széles skálája és persze a gyors piaci megjelenés miatt valószínűleg nem történt mindenre kiterjedő, alapos sérülékenységi vizsgálat.

Elgondolkoztató és egyben aggasztó előadást tartott az idei Las Vegasban megrendezett DEF CON hacker konferencián Anthony Rose és Ben Ramsey. [16] A két biztonsági szakember 16 db kereskedelemben kapható, bluetooth-vezérelt „okoszárat" vizsgált meg. Néhány száz dolláros eszközparkkal, különböző módszerekkel a zárak 75%-át (12 db-ot) szoftveresen feltörték. A maradék négyből egyet pedig egy csavarhúzó és fogó segítségével, erőfeszítés nélkül nyitottak ki. [16] Négy különböző zárat találtak, ahol a mobiltelefon és a zár közötti kommunikáció titkosítás nélkül zajlik. Az adatforgalmat egy irányított antennával több száz méter távolságból vették és rögzítették. Egyszerű szöveges üzenetekkel a felhasználó által beállított jelszó felülírható, és ezzel a felhasználó kizárható a hozzáférésből. Alapállapotba visszaállítani a zártestbe szerelt elemek eltávolításával lehet, ami viszont csak a zár nyitott állapotában hajható végre.

A gyártó a honlapon úgy reklámozza a zárat, hogy biztonságosabb, mint a kulcs vagy a kód, mivel ezt nem lehet elveszíteni vagy lemásolni. A gyanútlan felhasználó ezért azt gondolja, hogy bár az eszköz lehet, hogy többszöröse a legjobb minőségű mechanikai

[8] Arra vonatkozóan nincsenek pontos adatok, hogy valójában hányan töltötték le a frissítést és szüntették meg a hibát.

zárnak, de legalább biztonságosabb. Eközben távolról, zajtalanul egy szempillantás alatt nyitható.

Összegzés

A technológiai fejlődés következtében új típusú veszélyforrások jelentek meg a komplex objektumvédelemben. Ezek közül az elkövetkező évek egyik nagy kihívása a drónok elleni védekezés lesz. A hamarosan bevezetendő jogszabályi szigorítás nem fogja megakadályozni az ártó szándékú reptetéseket, ezért a kiemelten fontos objektumoknál szükség lehet észlelő, elfogó/megsemmisítő berendezések telepítésére. Ehhez azonban a jelenlegi technológiákat még fejleszteni, hatótávolságukat növelni kell.

Szintén a technológiai fejlődésnek köszönhető, hogy egyre több önálló intelligenciával és döntési képességgel rendelkező berendezések állnak a vagyonvédelem szolgálatába. Ezek az eszközök egymással vagy egy felügyeleti szoftverrel folyamatosan kommunikálnak. Ez folyamatos (online) jelenlétet igényel, amely egy újabb támadási felületet eredményez. A piaci pozíciók erősítése és stabilizálása érdekében a gyártók felgyorsított fejlesztési, gyártási és tesztelési fázisokat alkalmaznak. Ez utóbbinak köszönhetően megnövekszik az eszközök kibertámadással szembeni sérülékenysége. Megfelelő informatikai tudás birtokában egy külső behatoló akár mesterszintű felhasználói jogosultságokkal – a valós felhasználót kizárva – vezérelheti a komplex védelmi rendszert. Ezért nagyon fontos, hogy a komplex objektumvédelmünk megfelelő szintű informatikai védelemmel is kiegészüljön.

Irodalomjegyzék

[1] Christián L.: *A magánbiztonságelméleti alapjai*. Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[2] Tóth A. – Tóth L.: *Biztonságtechnika*. Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[3] Berek L.: *Biztonságtechnika*. Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[4] Berek T. – Bodrácska Gy.: Az élőerős őrzés az objektumvédelem építőipari ágazatában. *Hadmérnök,* 5. évf. 4. szám, 2010.

[5] Berek L. – Berek T. – Berek L.: *Személy és vagyonbiztonság.* Óbudai Egyetem, Budapest, 2016.

[6] Vránics D. – Üveges A.: Pilóta nélküli légi járművek fejlődése. *Felderítő Szemle,* 14. évf. 2. szám, 2015.

[7] Petrétei D.: A drónok kriminál technikai és rendészeti felhasználása. *Magyar Bűnüldöző,* 6. évf. 1-3. szám, 2015.

[8] The Internet of Things. www.cisco.com/c/dam/ en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (a letöltés ideje: 2016. 12. 27.)

[9] The Internet of Things: Creating a Connected World. https://strategymeetsaction.com/about-sma/ (a letöltés ideje: 2016. 12. 27.)

[10] Internet of Things (IoT): Number of connected devices worldwide from 2012 to 2020 (in billions). www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (a letöltés ideje: 2016. 12. 27.)

[11] Annual report of the Security Information Service for 2014. www.bis.cz/annual-reports/annual-report-of-the-security-information-service-for-2014-9d082374.html (a letöltés ideje: 2016. 12. 27.)

[12] Is the World's Biggest Surveillance Camera Maker Sending Footage to China? www.voanews.com/a/hikvision-surveillance-cameras-us-embassy-kabuk/3605715.html (a letöltés ideje: 2016. 12. 27.)
[13] Dahua DVR Authentication Bypass – CVE-2013-6117. https://depthsecurity.com/blog/dahua-dvr-authentication-bypass-cve-2013-6117 (a letöltés ideje: 2016. 12. 27.)
[14] Serious Vulnerability Affects Over 120 D-Link Products. www.securityweek.com/serious-vulnerability-affects-over-120-d-link-products (a letöltés ideje: 2016. 12. 27.)
[15] Regarding Senr.io Vulnerability Affecting Many D-Link Products. www.dlink.com/uk/en/support/support-news/2016/july/15/senrio-vulnerability (a letöltés ideje: 2016. 12. 27.)
[16] Have a smart lock? Yeah, it can probably be hacked. www.cnet.com/news/have-a-smart-lock-yeah-it-can-probably-be-hacked/ (a letöltés ideje: 2016. 12. 27.)

Today's Challenges of Complex Property Protection

Levente Tóth

Due to technological progress, there is an ever wider range of tools available in the security technology market. Besides increasing security, however, a part of these developments may expose us to new attacks. The increased range of tools and the ever more intelligent systems require a higher degree of expertise, more accurate design and more precise implementation and maintenance from the implementing companies, and more careful and skilled operation from the users. The complexity of the systems and the amount of information generated increases in proportion to their size. In order to ensure efficient operation, various decision-supporting algorithms and software are developed. Some of these also provide comfort services that may contain new vulnerabilities. With the appearance of new technologies, the complexity of object protection is extended with new aspects.

Keywords: Drone, Integrated Management System, Decision Support Software, M2M, IoT, UAV