OKOS RENDSZEREK LEHETŐSÉGEI ÉS BIZTONSÁGI KIHÍVÁSAI

OPPORTUNITIES AND SECURITY CALLANGES OF SMART SYSTEMS

BEREK TAMÁS[1]

ABSZTRAKT

A jövőben a populációnk meghatározó hányada városi környezetben fog élni. A nagy népsűrűség, a szűkülő élettér, a klímaváltozás számos olyan nehézséget fog támasztani, melyek megoldására intelligens rendszereket kell megalkotni a fokozódó hatások enyhítése érdekében. Ezek az okos megoldások könnyebbé teszik életünket, azonban számos biztonsági kihívást is generálnak, amelyre fel kell készülnünk.

Kulcsszavak: fenntartható fejlődés, okos megoldások, intelligens rendszerek, biztonsági kihívások

ABSTRACT

In the future, the majority of our population will live in an urban environment. The high population density, the shrinking living space, and climate change will cause many difficulties that need to be addressed by intelligent systems to mitigate the increasing impact. These smart solutions make our lives easier, but they also generate a number of security calls to be prepared for.

Keywords: sustaniable development, smart solutions, intelligent systems, security challanges

[1] berek.tamas@uni-nke.hu | ORCID: 0000-0001-8358-6139 | egyetemi docens, Nemzeti Közszolgálati Egyetem

BEVEZETÉS

A nagyvárosok lakosságának egyre nagyobb léptékű növekedése a jövőben is folytatódik egyebek mellett gazdasági versenyképességük révén. Ezzel egyidőben egyre növekvő a társadalmi igény az élhető környezet megteremtésére és fenntartására. Az antropogén eredetű környezeti tényezők mellett a klímaváltozás olyan hatásaival is számolni kell az előttünk álló évtizedekben, amelyek a városi környezetben fokozottan jelentkeznek és kedvezőtlenül befolyásolják életminőségünket. A különböző autonóm intelligens városi rendszerek fejlesztésével és azok térhódításával sorra alkalmazásba kerülnek a mindennapi életünket jobbító innovatív megoldások, melyek azonban közvetlen és közvetett hatással bírnak más rendszerekre, folyamatokra. Több más mellett ez is szükségessé tette azok összehangolását, valamint az okos város koncepció kidolgozását. A fenntartható városi mobilitás, az épületek energiahatékonyságának növelése és az életminőség javítása érdekében kifejlesztett intelligens rendszerek hozzá járulnak egyben a társadalmi ellenállóképességhez a klímaváltozás hatásaival szemben. Ezeknek az intelligens városi rendszereknek kiépítése és üzemeltetése azonban kihívásokat hív életre a biztonságtechnika területén.

Már jelenleg is többen élnek a városokban, mint vidéken, s ez az állapot az elkövetkező időszakban sem fog változni. A technikai fejlődésnek, s azon belül elsősorban a felhő alapú számítástechnikának, a big data elemzésnek, a mesterséges intelligenciának köszönhetően a városokban és a vidéken is egyre több okos megoldással lehet találkozni, a döntéshozatal megkönnyítése, a kényelem, a biztonság érdekében. Az intelligens települések koncepcióinak kidolgozása során vizsgálni szükséges a növekvő urbanizáció, az infrastruktúrák fejlesztésével, növekvő társadalmi és gazdasági elvárásokkal kapcsolatos problémaköröket a növekvő környezeti kihívások tükrében akkor is, ha technológiai képességek dinamikus fejlődése, illetve a csökkenő technológiai költségek egyre nagyobb mértékben képesek támogatni jobbító törekvéseket. (Kollár 2019)

Városi környezetben azzal a növekvő problémával kell szembe nézni, hogy az egészséget veszélyeztető mértékben növekszik a levegő szennyezettsége. Az emberi tevékenység következményeként levegőben lévő szennyező anyagoknak való kitettség egészségre gyakorolt hatása főleg tüdőt érintő súlyos rákos megbetegedések és az asztma gyakoriságának növekedését eredményezi. (Cohen et al 2004)

Ez széles skálán kihat a társadalom egészére és tekintettel arra a prognózisra, hogy a városok lakossága a jövőben növekedni fog az élhetőbb urbanizált környezet feltételeit megteremtő okos város koncepciók kialakítása kezdődött el.

Az intelligens rendszerek kialakítása jelentősen csökkentheti a környezeti ártalmakat és javíthatja életminőségünket, azonban számos olyan újabb biztonsági aspektusát mutatják meg jövőbeli környezetünknek, melyekre választ kell adnia a biztonságtechnikának is.

AUTONÓM RENDSZEREK ÉS BIZTONSÁGI KIHÍVÁSAIK

A jelenlegi világ népességi kilátások adatai alapján az urbanizáció hosszú távú hatásai már most is kitapinthatók. A városi területek népességnövekedése olyan társadalmi, technológiai és politikai feszültségeket okoz, amely a jövőben egyre nagyobb hatással bíró tényező

lesz. Az intelligens városi rendszerek kiépítésekor elengedhetetlen volt a globális megközelítés, hiszen a város fejlesztése során nyilvánvaló kölcsönhatások lépnek fel a különböző városi rendszerek között. A kiber-fizikai rendszerek már jelentős mértékben jelen vannak mindennapjainkban. A fizikai környezetet kiegészítő virtuális elemek folyamatos fejlesztése tapasztalható és ennek fényében számos, a biztonsággal összefüggő kérdés merül fel. A komplex számítógépes világ önmagában is új kihívásokat jelent a városi rendszerek számára, különösen az intelligens városi megvalósításokban. (Tokody-Schuster 2016)
Az információtechnológiában bekövetkező forradalmi változások lehetővé teszik a városi ellátási rendszerek nagy ütemű fejlesztését. Ezen a rendszerfejlesztések eredményeképp az alkalmazó szervezetek környezeti adatigénye jelentős.
A különböző ellátási szervezetek alkalmaznak olyan rendszereket, melyek a meghatározott mérőpontokról származó adatok gyors kiértése és feldolgozása révén azonnal be tudnak avatkozni raktározási, szállítmányozási vagy szolgáltatási folyamatokba az optimalizáció jegyében. Az adatok egyre nagyobb szerepet kapnak sikeres és biztos működés érdekében, így egyre nagyobb értéket is képviselnek. Ezeknél a folyamatoknál a biztonság mellett az információ-és adatbiztonságot támogató környezet megteremtése alapvető követelmény. A jelentős értéket képviselő adat és információ nem csak jogszabályok révén, hanem a szervezeti belső szabályzatokban foglaltak segítségével is védelmet kell, hogy kapjon. Ezek ki kell hogy térjenek a munkavállaló tudomására jutott bizalmas és titkos vállalati információk továbbadásának a tilalmára, a munkavállaló által használt informatikai és számítástechnikai eszközök használatára, a vállalati adatok tárolásának módjára, továbbá hozzáférés jogosultságaira is. (Kollár 2018)
A tapasztalatok azt mutatják, hogy a pontosan felépített, a felelősség- és jogköröket egyértelműen meghatározó szabályozók alkalmazása csak részben teremtik meg az érzékeny adatok védelmének feltételeit. Az alkalmazottak biztonságtudatos magatartása hatékonyan hozzájárul az emberi tényező, mint hibafaktor kockázatának csökkentéséhez. Tekintettel arra, hogy manapság az adatok gyűjtése, tárolása, feldolgozása és továbbítása informatikai eszközök segítségével történik, ezeknek az informatikai rendszerek védelme kiemelten fontos. A digitális kompetencia egyre nagyobb társadalmi fontossággal bír. Napjainkban a digitális eszközök és az internet elterjedése miatt elengedhetetlen alapszintű információbiztonsági ismeret. A kiber korszak csak néhány évtizedre nyúlik vissza. A kibertérben megjelenő támadások veszélyességét gyakran nem tudják felmérni helyesen. Hazai kutatás (Nyikes 2019) egyes eredményei is azt mutatják, hogy a Közép-Kelet európai lakosság biztonságtudatossági- és digitális kompetencia szintje szerteágazó. A lakóhely és az életkor alapján elkészített korrelációk segítségével meg lehet határozni azokat a gyenge pontokat, amelyek alapján akár kormányzati, vagy akár társadalmi összefogással szükséges segítséget nyújtani a felhasználók számára. Az informatikai rendszerek felhasználóinak jó biztonságtudatossági szintje elengedhetetlen az ipari termelés optimalizálása, valamint az intelligens ellátási rendszerek alkalmazásának kedvező hatásainak kiaknázásához.(Nyikes 2019)
A szenzitív adatokhoz történő jogosulatlan hozzáférést megakadályozó biztonsági eljárások fejlődése folyamatos. A biometrikus azonosítási módszerek alkalmazását lehetővé tevő technikai újítások azonban óriási mértékben gyorsították fel megbízhatóságuk fokozásával azok elterjedését.
A biztonságtechnika rohamosan fejlődő területe lett az ember biometrikus azonosítása. A biometrikus azonosítás eszközeinek használata életünk szerves részévé válhat a jövőben. Előnyös tulajdonságai révén olyan azonosítási módszert biztosít, amely esetében a modern

eszközöket tekintve nehéz biztonsági rést találni. A birtok, vagy a tudás alapú azonosítási módszerekkel szemben nagy előnye, hogy biometriai jegyeink folyamatosan rendelkezésünkre állnak. A modern technikai háttér fejlődése lehetővé teszi olyan biztonsági kockázatú területeken történő alkalmazását ahol a proxy kártyás, kód alapú rendszer nem alkalmazható. A kényelemhez és a megfelelő biztonsági szinthez mérten az élet minden területén alkalmazható a biometrikus azonosítás dinamikus terjedésére lehet számítani tehát a jövőben. (Kovács et al 2012)

Ezen a területen is kézelfoghatóan jelentkezik az egyének egyes biometriai jellemzőivel kapcsolatos adatainak biztonságos tárolása, melyre kiemelt figyelmet kell fordítani. A biometrikus azonosítási rendszerek térnyerésével egyre több pontos adat fog leképeződni az egyének mindennapi szokásairól, útvonalaikról stb,, melyek szenzibilitása okán további biztonsági kérdések merülnek fel. Megjegyzendő, a probléma nem újkeletű, évtizedekkel ezelőtt a térfigyelő kamerák terjedése hasonló problémákat vetett fel.

Az emberek magánéletének védettségét fenyegető újonnan megjelenő tényezők között számolnunk kell a különböző rendeltetésű pilóta nélküli repülőeszközök terjedésével is, továbbá a drónok bűnös célú használatának lehetősége a személy és vagyonvédelem területén már meglévő és a jövőben létesítendő fizikai védelmi rendszerek tervezése során is új gondolkodásmódot igényel.

A pilóta nélküli repülőeszközök polgári célú alkalmazása kezdetekben lehetővé tette elsősorban különböző rendezvények dokumentálását, katasztrófa sújtotta területek felmérését, különböző kutatási feladatok, térinformatikai alkalmazások támogatását. A fejlesztések és tapasztalatok feldolgozása lehetővé teszi a drónok alkalmazását a nagyvárosok által teremtett környezet különböző vizsgálati szempontok mentén történő feltérképezésében. A településrendezési tervezés támogatásával fel lehet mérni és módosítani a településszerkezetet, vagy akár a városi környezetben kialakuló hősziget jelenség és a hőhullámok idején megnövekvő hűtési kapacitás hatékonyságának elősegítésének érdekében épületenergetikai felméréseket lehet segítségükkel végezni.

A személy- és vagyonvédelem területén, különösen az objektumvédelem ágazatban kedvező lehetőségekkel kecsegtet a pilóta nélküli repülőeszközök alkalmazása, melyek térnyerése a mind a gazdasági, mind pedig a játékipar területén óriási léptékű volt az elmúlt évtizedben. A katonai és más egyéb célú alkalmazás mellett ezeknek az eszközöknek, különösen az alkalmazásorientált kialakítású és felszerelésű specializációinak a fejlesztését követően a magánbiztonsági célú alkalmazása várható már a közeljövőben. Az intelligens megoldások alkalmazásával, megfelelő algoritmusok révén sokoldalúan alkalmazható mobil ezközévé válhat a vagyonvédelemnek.

A pilóta nélküli repülőeszközök elterjedésével azonban a védelmi rendszereink képességeinek bővítése mellett is számolnunk kell annak biztonsági kihívásaival is a jövőben. Ezek a berendezések ugyanis eszközként jelenhetnek meg a bűnös célú elkövetők tárházában is.

A technológiai fejlődés következtében megjelenő új típusú veszélyforrások között kell számon tartani tehát drónokkal elkövetett cselekményeket. Első körben a kiemelten fontos objektumoknál szükség lehet észlelő és elfogó berendezések telepítésére. Ehhez azonban a jelenlegi technológiák fejlesztésére van szükség, elsősorban azok hatótávolságának növelése érdekében. Az előbbi mellett kihívásként jelentkezik az objektumvédelemben alkalmazott eszközök kibertámadással szembeni sérülékenysége is. Egyre több olyan berendezés kerül alkalmazásra amely önálló intelligenciával és döntési képességgel van felruházva és

emellett valamilyen felügyeleti szoftverrel folyamatosan kommunikálnak. Ez olyan támadási felületet eredményez, amely védelme érdekében a pontosabb tervezés, precízebb kivitelezés mellett gondosabb üzemeltetési magatartást kell megkövetelni a felhasználóktól. Megfelelő informatikai tudás birtokában egy külső behatoló akár mesterszintű felhasználói jogosultságokkal felülvezérelheti a komplex védelmi rendszert. Ezért a komplex objektumvédelemnek ki kell terjednie megfelelő szintű informatikai védelemre is. Figyelemmel kell tehát lenni arra, hogy az objektumvédelemben alkalmazott korszerű alrendszerek kényelmi szolgáltatásai mellett újabb támadási felület jelenhet meg, így az objektumvédelem komplexitása további aspektusokkal egészül ki. (Tóth 2018)

Az objektumvédelem, különösen egy stacioner jellegű létesítménycsoport esetében egy jól körülhatárolható terület köré szerveződik, a védelmi eszközrendszer olyan arányban történő szervezésével, amely a várható támadási irányoknak megfelelően kiépítve a veszély nagyságával arányos védelmet képes biztosítani. A jogosulatlan behatolás elleni védelemnek az utóbbi időkig néhány speciális (főleg a kritikus infrastruktúrákhoz köthető) eset kivételével elsősorban a perimétervédelmet ellátó fizikai védelmi rendszer túloldaláról indított, annak megbontásával, vagy más úton történő leküzdésével végrehajtott behatolásokra kellett felkészülnie. A pilóta nélküli repülőeszközök magánszférában történő rohamos terjedése azonban további lehetőséget nyújt a jogosulatlan behatolást elkövetők számára, ami az objektumvédelem fejlesztésének új dimenzióját nyitja meg egyben.

A drónok használata az elmúlt évtizedben jelentősen megnőtt. Különböző területeken történő felhasználásuk egyre jobban bővült. A filmipar, a térképészet, távérzékelés, és a védelmi szektor (határőrség, katasztrófavédelem) mellett a hobbi célú alkalmazása is megjelent napjainkra. A személy-és vagyonvédelem egyik legnagyobb területe az objektumvédelem. Az objektumok védelmére kiépített komplex rendszerek alkalmasak a földfelszíni és felszín alatti eredetű támadások elhárítására. A légtérből érkező támadások elhárítását nem minden szervezet tudja magának biztosítani. Ez a veszélyforrás napjainkra egyre kézelfoghatóbb a megfizethető drónok megjelenésével. A növekvő drónhasználat szükségessé teszi az objektumvédelem területén új technológiák kidolgozását és bevezetését, melyek a nem kívánatos repülőeszköz használat elhárítását szolgálják. (Heller 2017)

A pilóta nélküli légijárművek, mint a védelmet segítő mobil eszközök használata a biztonságtechnikában előirányoz néhány alapvető feltételt. Az ezen a területen alkalmazandó pilóta nélküli légijárművekkel szemben támasztott speciális követelmény az irányításhoz való hozzáférés valamint az adatok védelme, azaz, hogy az irányítópult és a drón közötti kapcsolatot úgy kell kialakítani, hogy az ne legyen zavarható, továbbá lehallgatás védett legyen. (Kovács- Viplak 2017)

A fenti és minden olyan programozható biztonságkritikus rendszer tervezése és kialakítása során a funkcionalitás elvét szem előtt tartva kiberbiztonsági szempontokat is figyelembe kell venni tehát a jövőben.

Ez a biztonsági kihívás fokozottan jelenik meg a közlekedésbiztonság területén tekintettel arra, hogy a járműiparban az autonóm, önvezető járművek fejlesztése intelligens közlekedési rendszerek kialakítása mellett viharos gyorsasággal zajlik.

Az okos város koncepciója mentén kutatások folynak az intelligens közlekedési infrastruktúra feltételeinek vizsgálata terén is. Az okos közlekedési rendszerek, mint innovatív üzleti megoldás hozzájárulnak fenntartható fejlődéshez és azon túl kényelmi funkciókkal is szolgálnak.

Az intelligens járművek, járműrendszerek elterjedésének feltétele az intelligens közlekedési infrastruktúra. Az intelligens közlekedési rendszerek alkalmazásának egyik célja lehet a gazdaságosság a szállítási kapacitás növelése révén, a kevesebb baleset elérése, és a károsanyag-kibocsátás csökkentése. Az autonóm intelligens járművek terjedésének össztársadalmi az előnyösségük. A járművek közötti kommunikáción kívül a V2X (Vehicle-to-everything) kommunikáció hozzájárul az okos város koncepcióhoz. A járművek fizikai rendszerei mellett egyre hangsúlyosabb szerep jut a kiber-fizikai komplex rendszereknek. Az autóipari fejlesztések kiberbiztonság szempontú megközelítése új és fejlődő terület. A járművek és járműrendszerek biztonságorientált alkalmazása nem csak a tervező feladata. Ahogy a hagyományos járművek is esetében is, az autonóm járműrendszerek üzemeltetői is felelősek járművük biztonságáért, így a járművek és járműrendszerek kiberbiztonságára is figyelemmel kell lenniük a jövőben. (Tokody et al 2018)

Az okos város koncepció intelligens autonóm rendszereivel számos területen a városközösség számára kedvező és hasznos kényelmi megoldásokat kínál, azonban fel kell készülnünk annak biztonsági kihívásaira is. Az egyes függetlenül, eseménvezérelten működő rendszerek, alrendszerek – akár egy objektumfelügyeleti rendszer esetében - egymásra hatással vannak mely hatásokat vizsgálni és tanulmányozni szükséges. A rendszerek védelméért felelős biztonsági vezetőknek a jövőben olyan kihívásokkal kell szembe nézniük, melyekre tudatosan fel kell készülni.

A felhasználók biztonságtudatos magatartása kialakítása mellett hangsúlyos szerepet kell, hogy kapjon a biztonságtechnikai szakembergárda felkészítése. A biztonsági vezetőnek ki kell terjesztenie az adott objektumra szakosodott biztonsági ismereteit új irányokba képzések során. Széleskörű ismeretek ugyanis elengedhetetlenek ezen a területen. (Szabó-Rajnai 2017)

A fenntartható fejlődést is szolgáló intelligens, energiahatékonyságot is szolgáló megoldások mellett is nagy bizonyossággal prognosztizálható az, hogy a társadalom energiaigénye növekedni fog. A folyamatos és üzembiztos energiaellátás kulcseleme az okos város koncepciónak. Az energetikai rendszerek - ide értve az elosztóhálózatot is – védelme fontos marad a jövőben is. Az energiaszektor sérülékenységének csökkentése és az energiahatékonyság növelése mellett jelentős erőfeszítéseket kell tenni a hálózatbiztonság területén is, ugyanis egy energetikai kollapszus bekövetkezése rendkívüli mértékű szerteágazó kihatással bír akár regionális szinten is.

Számos, az elmúlt évtizedben bekövetkezett áramkimaradást a kánikula, valamint az ebből adódó, a légkondicionálók ellátásához szükséges energiaigény váltotta ki. A rendszer gyenge pontjait gyakran az elavult technológiával felszerelt rendszerelemek jelentették és emberi mulasztások sorozata vezetett az összeomláshoz. Ezek az események több tízmillió embert érintettek. Az anyagi károk általában jelentősek voltak, repülőtereket kellett lezárni, forgalomirányító rendszerek maradtak felügyelet, valamint irányítás nélkül. A vasúti közlekedés is összeomlott. A kórházakban jelentősen megnövekedett az egészségügyi krízisesetek száma, ami elsősorban a légzőszervi megbetegedésben szenvedőket érintette. Számos haláleset is történt az idős emberek körében a létfenntartó gépek hiánya miatt. Az ivóvízrendszer szinte teljesen megbénult, a szivattyútelepek nem működtek. Ezért a víztisztító rendszerek sem voltak képesek ellátni feladatukat. (Vass et al 2015)

Az energetikai rendszer összekapcsolása a folyamatos fejlesztéseknek köszönhetően az 1880-as évektől kezdve zajlik. Az európai hálózat növekedése is a két világháború időszakától eltekintve folyamatos. Azonban annak végével és a vasfüggöny megszűnésével a rendszer elérte jelenlegi állapotát. A következő nagy lépés az Európát Észak-Afrikával valamint az Arab-félszigettel összekötő interkontinentális hálózat elkészítése jelentené. Jelen koncepció alapján ez a megvalósulás 2020-ra valósulhat meg. Az így megépülő architektúra jóval rugalmasabb, stabilabb több tartalékot tartalmazna, mint a korábbi hálózaté. Az Észak-Afrikai területek jóval magasabb lefedettséggel rendelkeznének, mint jelenleg ami részben növelné az ellátás biztonságát és olcsóbbá tenné a villamos energiát is. Azonban a nagyobb kiterjedés potenciálisan nagyobb támadási felületet is jelentene az Európán kívüli területek felől. Ezért egy olyan szigetekre bontás szükséges mely megvalósulása esetén a hálózat nem áll le teljesen, hanem adott területekre válik szét. Az így kialakult kisebb mikrogridek önműködően tartják fenn magukat egészen az újbóli szinkronizációig.(Berek et al 2018)
Az energiabiztonság jegyében kiemelt szerepe van energiahatékony megoldások fejlesztésének és alkalmazásának a jövőben. Az épületenergetikai hatékonyságot nagymértékben támogathatják a létesítményekben kiépített és üzemeltetett biztonságtechnikai rendszerek valamint épületfelügyeleti rendszerek integrált alkalmazása, mely során a vagyonvédelmi komplexum elektronikai alrendszerének érzékelői segítségével az épülethasználatra vonatkozó adatok kinyerésével és feldolgozásával közvetlenül lehet módosításokat végrehajtani épületüzemeltetési alrendszerek működésében és energiafelhasználásukban.

A társadalom fejlődését biztosító és a kutatások egyik jelentős hátterét jelentő tudásbázis megőrzése és védelme mindig is fontos feladatot jelentett. Napjainkra a világban zajló tudományos kutatások eredményei óriási számban látnak napvilágot, így ez a tudásbázis rohamos gyorsasággal bővül, amelynek gondozását hivatott, a közhiteles adatbázisokat üzemeltető könyvtárak feladata napról napra bővül különös tekintettel arra, hogy az azok által szolgáltatott adatmennyiség jó része elektronikusan tárolt és hálózati elérésű.
Az elektronikus információs rendszerek, és a könyvtári infokommunikáció jelentősége fokozódik, hiszen egyre fontosabb elemeivé válnak a 21. század könyvtárainak. Már a jelenkorban is, de a jövőben a könyvtárakban szolgáltatott állomány egyre nagyobb része lesz elérhető elektronikus, hálózaton keresztül, így a biztonsági kérdések és megoldások súlya is egyre növekszik. A könyvtári infokommunikáció biztonsága annak rendeltetésszerű működését veszélyeztető cselekmények, események és a velük szemben támasztott intézkedések együtthatása. A könyvtár által archivált és szolgáltatott elektronikus dokumentumok mennyisége már ma is meghaladja a hagyományos, fizikai hordozón megjelent állományrészt, ami a biztonságos szolgáltatás és a hosszú távú megőrzés feltételrendszerének kialakítását, biztosítását követeli meg. Sorra kell venni a fenyegetettségre adandó válaszokat, tehát a könyvtári infokommunikációs biztonság fenntartása érdekében tett intézkedéseket és eszközöket. (Berek Rajnai 2015)

ÖSSZEFOGLALÁS

A jövőben az okos-, mobil eszközök térhódítása az infokommunikációs technológiában egyértelműen megmutatkozik. Környezetünkben olyan szenzorok érzékelik folyamatosan különböző folyamatok állapotait, melyek képesek kommunikálni egymással az interneten keresztül. A technológia fejlődésének köszönhetően az internetre csatlakozó eszközök száma folyamatosan emelkedik az IoT terjedése révén, ami lehetővé teszi, hogy a mindennapos használati tárgyaink is az internetre kapcsolódjanak. Az IoT megjelenik az okosváros koncepciókban de a kritikus infrastruktúrában, is. (Haig 2018)
Az okos rendszerek a jövőben számos, a mindennapi életünket meghatározó és hatással bíró folyamatot fognak felügyelni hozzájárulva egyebek mellett kényelmünkhöz, az élhető környezetünkhöz, a fenntartható fejlődéshez, valamint a biztonsághoz. A biztonságosabb életet lehetővé tevő megoldások azonban újabb és újabb biztonsági kihívásokat keltenek, melyekre a biztonságtechnika területén is fel kell készülnünk.

FELHASZNÁLT IRODALOM

Berek László - Rajnai Zoltán (2015): A könyvtári infokommunikáció biztonsága HADMÉRNÖK 10 : 2 pp. 199-208.
Berek Lajos - Szabolcsi Róbert - Vass, Attila (2018) The Splitting of an Energy System HADMÉRNÖK (XII) I 1/2018 pp. 9-19.
Aaron J. Cohen - H. Ross Anderson – Bart Ostro - Kiran Dev Pandey - Michal Krzyzanowski – Nino Künzli - Kersten Gutschmidt - C. Arden Pope III, Isabelle Romieru - Jonathat M. Samet – Kirk R. Smith (2004): Urban air pollution in Comparative Quantification of Health Risks Global and Regional Burden of Disease Attributable to Selected Major Risk Factors Volume 1 Edited by: Majid Ezzati, Alan D. Lopez, Anthony Rodgers and Christopher J.L. Murray World Health Organization Geneva
Haig Zsolt (2018): Információs műveletek a kibertérben Budapest, Magyarország : Dialóg Campus Kiadó ISBN: 9786155945052 ISBN: 9786155945045
Hell Péter (2017): Drónelhárító rendszerek az objektumvédelemben HADMÉRNÖK 12 : 3 pp. 37-47.
Kollár Csaba (2018): A vezető személyes márkaépítésének információbiztonsági problémái JEL-KÉP: KOMMUNIKÁCIÓ KÖZVÉLEMÉNY MÉDIA 2018/I. pp. 97-108.
Kollár Csaba (2019): Az okos város és az okos vidék szimbiózisa: Utópia, fikció, vagy realitás? In: Kőszegi, Irén Rita (szerk.) III. Gazdálkodás és Menedzsment Tudományos Konferencia : Versenyképesség és innováció Kecskemét, Magyarország : Neumann János Egyetem, pp. 29-35.
Kovács Tibor - Otti Csaba (2012): A biztonságtudomány biometriai aspektusai In: Hautzinger, Zoltán (szerk.) A biztonság rendészettudományi dimenziói : Változások és hatások Pécs, Magyarország : Magyar Rendészettudományi Társaság, pp. 1-10.
Kovács Tibor -Viplak Armand Máté (2017) Drónok a biztonságtechnikában HADMÉRNÖK XII : 2 pp. 7-13.

Szabó Anikó – Rajnai Zoltán (2017) The review of the external risk factors during the operation training plan of the security guards In: Szakál, Anikó (szerk.) IEEE 15th International Symposium on Intelligent Systems and Informatics : SISY 2017
New York, Amerikai Egyesült Államok : IEEE, (2017) pp. 359-364.

Tokody Dániel - Rajnai Zoltán – Albini Attila - Ady László - Temesvári Zsolt Marcell (2018): Kiberbiztonság az autóiparban BÁNKI KÖZLEMÉNYEK 1 : 3 pp. 71-77.
Tokody Dániel - Schuster György (2016):Driving Forces Behind Smart City Implementations-The Next Smart Revolution., Journal of Emerging Research and Solutions in ICT 1.2, pp. 1-16., http://eprints.fikt.edu.mk/171/, (letöltés ideje: 2019.02.23.)
Tóth Levente (2018): A komplex objektumvédelem kihívásai napjainkban BOLYAI SZEMLE 27 : 1 p. 35
Nyikes Zoltán (2017): A Közép-Kelet Európai Generációk Digitális Kompetencia és Biztonságtudatosság Vizsgálatának Eredményei = Results of Digital Competency and Safety Awareness Assesement in Middle East Europe HADMÉRNÖK XII : 4 pp. 159-172.
Vass Attila – Berek Lajos (2015): Napenergia és az elektronikai jelzőrendszer, villamos energia hálózattól távol lévő objektumok védelmének lehetőségei Hadmérnök 24:(2) pp. 41-57. http://www.hadmernok.hu/152_04_vassa_bl.pdf