HADMÉRNÖK

XIII. Évfolyam 1. szám – 2018. március

A FELHASZNÁLÓK BIZTONSÁGÁNAK NÖVELÉSE INTERNETES SEGÉLYHÍVÓ RENDSZER ALKALMAZÁSÁVAL

INTERNET EMERGENCY CALL SYSTEM FOR INCREASING THE USERS SAFETY

NYIKES Zoltán;

(ORCID: 0000-0001-5654-5120)

nyikes.zoltan@hm.gov.hu

Absztrakt

Jelen korunkban az internet által nyújtott szolgáltatások és az elérhető lehetőségek teljesen átalakították az életünket. Felmérések alapján kimondható, hogy a lakosság jelentős többsége naponta használja az internetet kortól és lakhelytől függetlenül. Meglehet a felhasználói digitális kompetencia nincs magas szinten és ezzel együtt a biztonságtudatosság sem. [1] A felhasználók, valamint a kis és középvállalatok védelméről jelenleg szervezetten, valós idejű, azonnali megoldással senki sem gondoskodik. A meglévő szolgáltatások és lehetőségek, mind csak az incidenst követően, manuális és statikus bejelentési, valamint segítségnyújtási lehetőséget biztosítanak, ha biztosítanak. Jelen cikkemben bemutatom azt az általam kidolgozott valós idejű, dinamikus segítségnyújtási lehetőséget, melynek alkalmazásával biztosítható lenne mind az általános felhasználó, mind azok a szervezetek informatikai védelme, amelyek nem tartoznak a törvényi hatály alá. Úgy, mint az internetes zaklatás, a vírustámadás és a rendszerösszeomlás.

Kulcsszavak: *internetes segélyhívó rendszer, vírustámadás, internetes zaklatás, rendszerösszeomlás*

Abstract

Nowadays the internet supported applications and the available possibilities reformed our life. It can declare on base of surveys that the society use daily the internet independently of age or locality. Beside this practise the digital competency and the safety awareness are low level. The organized real time digital defence solution of the civil users and the small and middle enterprises are not available yet. Currently the available service supports means help after the incident by manual and static way. In this article I introduce own invented system that means real time and dynamic defence solution possibility for the public users and for the undefended users whom are not defended by laws obligation. The purposed incidents are cyberbullying, virus attacks and system disaster.

Keywords: *internet emergency call system, virus attack, cyberbullying; system disaster*

A kézirat benyújtásának dátuma (Date of the submission): 2018.01.20.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.03.18.

BEVEZETÉS

Amikor minden rendben van az életünkben, nincs szükségünk a segítségre. Egy ideális világban nem is lenne szükség semmilyen olyan szervezetre, ami megvédi az embereket, vagy segítséget nyújt a bajban, mert nem lenne baj. A tevőleges segítségnyújtásnál egy-egy adott szituációban életet is menthet, pláne, amikor vészhelyzetről van szó. A polgárosodás kezdetétől működnek különböző segítséget nyújtó szervezetek intézményesített formában, szinte minden országban. Ilyen a rendőrség, a tűzoltóság és a mentők. Ezek a szervezetek adott esetben, amikor olyan esemény történik, ami váratlan és elhárítására jogilag, fizikailag, vagy a tudás hiányában nem vagyunk képesek, riasztjuk őket. Ekkor vagy a helyszínre vonulva nyújtanak segítséget, hajtanak végre mentést, vagy védelmet nyújtanak, esetleg csak távolról próbálnak segítséget nyújtani, telefonon keresztül. A kommunikációs csatornák fejlődésével, annak lehetőségével a segélykérés és az arra történő reakció az adott szervek részéről gyorsabbá és pontosabbá vált.

A SEGÉLYHÍVÓ RENDSZER

A telefon és a telefonközpontok megjelenésével már lehetőség volt a segélyhívásra telefonon keresztül. A kézibeszélő beemelésével a központ-kezelőt kellett kérni, hogy hívja, vagy kapcsolja a segítséget biztosító egységet. Az első segélyhívórendszert 1937. július 1-jén Londonban vezették be a 999 szám tárcsázásával, melyet rövid időn belül kiterjesztettek az egész országban. 1946-ban a Southern California Telephone Co. társaság a 116-os számot kezdte erre a célra használni Los Angelesben. A 999-et 1959-ben vette át Winnipeg, Manitoba és Kanada is Stephen Juba, Winnipeg polgármesterének a sürgetésére. A város 1972-ben váltott át a 911-re, hogy alkalmazkodjon az akkor már általános amerikai segélyhívószámhoz. Az 1960-as években - a 111-es új-zélandi segélyhívószám bevezetése előtt - Auckland városa, ahol 40 telefonközpont működött, mind más-más segélyhívó számokkal, és a helyi számokat a város 500 oldalas telefonkönyvéből kellett kikeresni. Ezt a problémát részben megoldották az Egyesült Államokban, Kanadában és az Egyesült Királyságban azzal, hogy a 0-t kellett tárcsázni veszély esetén. A modern időkben a mobiltelefonokon ezek a számok is gyorsan tárcsázhatók, még akkor is, ha nincs SIM kártya a készülékben. A szám országonként eltérő, általában egy könnyen megjegyezhető háromjegyű szám, amely gyorsan hívható. Egyes országokban több segélyhívószám is létezik különböző típusú vészhelyzetekre. Az Európai Unióban az 1990-es évek óta használatos segélyhívó szám a 112. A mobilkészülékek és a SIM kártyák tartalmaznak néhány előre beprogramozott telefonszámot. Amikor a felhasználó olyan segélyhívószámot tárcsáz, melyet egy mobilkészülék ismer, a hálózat automatikusan a helyi segélyhívószámra irányítja a hívást. A legtöbb GSM készüléken akkor is hívható ez a szám, ha a billentyűzet le van zárva, ha nincs a telefonban SIM kártya, vagy akár akkor is, ha a PIN kód megadása helyett tárcsázza ezt a hívó fél.

A segélyhívó Magyarországon

Hazánkban 2011. június 7.-én döntött a kormány az egységes, ingyenesen hívható segélyhívó rendszer kiépítéséről. Az ország két pontján – Szombathelyen és Miskolcon –, egy-egy rendőrségi központba futnak be a hívások, amelyeket rendvédelmi, tűzvédelmi és egészségügyi kérdésekben jártas operátorok fogadnak. A bejelentéseket, úgynevezett „intelligens adatlapra” rögzítik, amely azonnal megjelenik a rendőrség, tűzoltók vagy éppen a mentők megyei ügyeleti rendszerein, így a legrövidebb időn belül, a pontos információk alapján indulhat útnak a segítség. A rendőrség 107-es, tűzoltók 105-ös számára érkező hívásokat 170 helyen fogadják országosan. A mentők 104-es számának tárcsázásakor 26 központba érkeznek a hívások.

INTERNETES SEGÉLYHÍVÓ RENDSZER ALKALMAZÁSA

Az internet és főleg az okostelefonok megjelenésével már egyre több olyan funkció is megjelent, mint például az olyan komplex segélyhívó rendszerek, amit a telefonra telepítve, annak alkalmazásával a felhasználó egy gombnyomással segítséget tud hívni a geopozíciós adatok megadásával. Sok autógyár már az új fejlesztésekbe olyan fedélzeti egységet fejleszt, ami az autó esetleges közlekedési balesetekor, annak hirtelen sebességváltozása vagy az adott útelhagyása esetén azonnal, automatikusan riasztja a diszpécserközpontot. De más közlekedési formákban, mint például az 1900-as évek eleje óta a hajózásban is használnak vészhívó rendszereket. Az „SOS" morzekódot segítségével – amit rádiótávírón adtak le és a *„Save Our Souls, azaz mentsétek meg lelkeinket"* rövidítése – jelezték a vészhelyzetet. Ezt később több területen is alkalmazták. A rádiózás fejlődésével mind a hajózás, mind a légi közlekedésben a *„Mayday"* segélyhívó közlemény, vagy a *„Pan Pan"* sürgősségi közlemény, továbbá a *„Securite"* biztonsági közlemény, amit használnak. Léteznek már olyan alkalmazások és szolgáltatások, amelyek közúti baleset során, a geopozíciós adatok alapján aktiválják a segélyhívó rendszert automatikusan, de a felhasználó kapcsolatba léphet a szolgáltató központ operátorával, aki intézkedik a helyzetnek megfelelően.

Informatikai rendszerek kártékony kódok elleni védelme

Az internet és az okostelefon ma már nem csak életet menthet, hanem annak meghibásodása, vagy működésének zavara olyan problémát is okozhat, amely a legrosszabb esetben akár emberi életet is követelhet. Sajnos, az informatikai eszközök védelmére, azok üzemszerű működésének biztosítása érdekében sokan nem fordítanak megfelelő figyelmet. [2] Ez eredhet a felhasználói gondatlanságból, vagy a felhasználói digitális kompetencia hiányából. [3] Azonban naponta jelennek meg az újabbnál újabb kártékony kódok, amelyek már nem csak a felhasználót, hanem sok esetben előfordul, hogy komplett rendszereket, például kórházak, repülőterek, bankok információs rendszereit támadják célzottan. Minden esetben probléma ez, de mint láthatjuk, akár emberi életek is veszélybe kerülhetnek egy-egy ilyen jellegű támadás miatt. [4]

Internetes zaklatás elleni védelem

A rosszindulatú kódok mellett, beszélhetünk a rosszindulatú emberekről, az internetes zaklatókról is. Ezek az emberek az internetet használják fel, hogy azon keresztül, annak védettsége mögé bújva zaklassák áldozatukat. [5] Ilyen esetben ezek az áldozatok védtelenek, kiszolgáltatottak és egyedül vannak a bajban. Sok esetben azt se tudják, hogy mit is csináljanak, kihez forduljanak a bajukkal. Sokszor rendőrségi feljelentés követ egy-egy ilyen zaklatást, de mire az áldozat a rendőrséghez eljut addigra a „forró nyom" már „kihűl".

Informatikai rendszerek üzemeltetésének biztonsága

Az is előfordulhat, hogy nem rosszindulatú kód, vagy zaklató okozza a gondot, hanem egyszerűen egy rosszul működő alkalmazás, vagy maga az operációs rendszerben keletkezik olyan üzemzavar, amit a felhasználó egyedül nem tud elhárítani. [6]

Az ilyen jellegű problémák orvoslására a megoldást egy olyan rendszer nyújthat, ami a vész-, vagy segélyhívó rendszerekhez hasonlóan működik. Annak mintájára, a felhasználó vagy a rendszer üzemeltetője részére rendelkezésre állna egy olyan internetes szolgáltatás, amely a fent felsorolt vész-, vagy veszélyhelyzet esetén olyan azonnali segítséget nyújtana, ami megakadályozza a rosszindulatú kód eszkalálódását, a zaklató ténykedését, vagy megoldást nyújt a rendszerhibára. A felsorolt első két esetben a technikai segítségnyújtás mellett nyomozati tevékenység is indíthatóvá válna az elkövető(k) kilétének megállapítására és a további rendőrségi eljárás alá vonására. Míg a harmadik esetben egyszerűen technikai segítségnyújtás történhet.

AZ INTERNETES SEGÉLYHÍVÓ RENDSZER MEGVALÓSÍTÁSÁNAK ÉS ALKALMAZHATÓSÁGÁNAK ELGONDOLÁSA

A rendszer kialakításához szükség van egy diszpécser központra, amely a technikai segítségnyújtás mellett a hatósági funkciót is ellátja. Ezt gyakorlatilag a meglévő 112-es Egységes Európai Segélyhívó számot üzemeltető diszpécser központokba lehetne integrálni, vagy a Nemzeti Kibervédelmi Intézet is üzemeltetheti. A Nemzeti Kibervédelmi Intézet a 2013. évi L. tv. [7] értelmében, a magyarországi kormányzati eseménykezelő központ, az úgynevezett GovCERT funkciót is ellátó hatósági jogkörrel rendelkező szervezet. Ezen kívül léteznek még olyan szervezetek, amelyek működtetnek jelenleg is olyan szolgáltatást, amely akár a rendszerszintű hiba, akár a zaklatás bejelentésére szolgálnak, valamint segítséget tudnak nyújtani. Vizsgálat tárgyát képezheti az a megoldási lehetőség is, hogy a jelenleg a telefonszolgáltatók, vagy a műsorszolgáltatók által üzemeltett telefonos ügyfélszolgálatok kínálatában jelenne meg ez a segítségnyújtó rendszer. Jelenleg azonban nincs olyan elérhető szolgáltatás a polgári felhasználók számára az informatikai piac kínálatában mely az általam megfogalmazott követelményeket teljesíteni tudja. A Hun-CERT által elérhető olyan szolgáltatás, amely egy statikus felületen történő bejelentéssel – az esemény leírásával – egy vizsgálat indítható. Azonban ez már az incidenst követően tudja megtenni a bejelentő, amivel értékes idő veszíthető. A Hun-CERT küldetése a Magyar Internet Társadalom segítése, ezen belül különösen a Magyar Internet Szolgáltatók segítése abban, hogy megfelelő eljárásokat alkalmazzanak a számítógépes hálózati incidensek kockázatainak kezelésére és az ilyen incidensek előfordulásakor az azokra adandó válaszokra. [8] Azonban egy statikus űrlap kitöltésén és egy 7/24-ben elérhető telefonszámon kívül más segítséget nem tudnak nyújtani. Továbbá léteznek különböző megoldások az internetes zaklatásra is, amely egy, az interneten kereséssel fellelhető oldalon adnak tanácsokat, jó esetben még egy telefonszám is meg van adva. Tehát ezek is statikus és nem valós idejű szolgáltatások. Az általam felvázoltak működhetnek önálló szervezetként is, hogy ezzel ne terheljék a fenti rendszerek működését. Ez a lehetőség funkcióját tekintve egy akkora területet fed le, amely fejlődése és használata folyamatosan nő. Ennek a rendszernek az „Internetes Segélyhívó Rendszer” (ISR) azaz az „Internet Emergency Call System” (IECS) elnevezést gondoltam adni.

Az Internetes Segélyhívó Rendszer megvalósítása

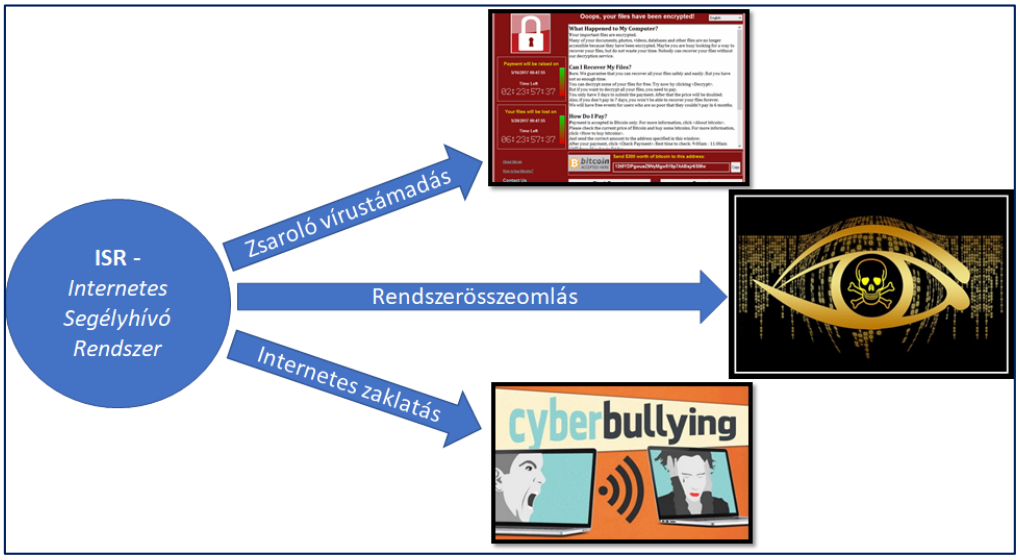
Működését tekintve, vészhelyzet esetén egy gombnyomásra, olyan dedikált virtuális magán hálózat (virtual privat network - VPN) kerül alkalmazásra, amely előre definiált és elkülönített porton és csatornán lép kapcsolatban a diszpécserközponttal, amely távsegítség lehetőségével nyújt segítséget a bajbajutottnak. Amennyiben szükséges, azonnal, „forrónyomon” is el tud indulni a nyomozás az elkövető(k) felkutatására.

A vészhelyzet típusát tekintve különböző funkciók lépnek működésbe. Úgy mint, a rosszindulatú támadás esetén a nyílt internet azonnali megszakítása, hogy az eszközön megjelenő kártékony alkalmazás ne tudjon a hálózaton tovább eszkalálódni, viszont a VPN segítségével a diszpécser központ átveszi az irányítást az eszköz felett és megindítja annak mentesítését. Továbbá bizonyítékokat gyűjt az ezt követő nyomozáshoz. Ebben az esetben a diszpécser központ ezen bejelentés esetén alkalmazhat akár mesterséges intelligenciát is, amely adott esetben sokkal gyorsabb és pontosabb beavatkozást tud kezdeményezni. Ezt követően egy operátor is felügyelheti a beavatkozást vagy át is veheti a műveletet.

A zaklatás esetén a felhasználó internet kapcsolata nem szakad meg, de a diszpécser központ távsegítséget, instrukciókat ad az áldozat számára, úgy, hogy látja az elkövetővel folytatott üzenetváltást, vagy internet-telefon hívást a dedikált VPN segítségével. Mindemellett egy olyan funkció is alkalmazható, amely a diszpécser központ az áldozat profiljában, az áldozat személyének kiadva magát, a zaklatóval direktben kommunikál szakértő módon. Ebben az

esetben, mód van az elkövető(k) elleni bizonyítékok azonnali gyűjtésére is. Itt indokoltnak tartom a diszpécser alkalmazását, az empátia szükségessége miatt.

A technikai meghibásodás esetén szintén egy dedikált VPN használatával biztosítható a diszpécser központ számára a távsegítség nyújtás és a rendszer helyreállítására történő kísérlet. Ebben az esetben is megoldás lehet a mesterséges intelligencia alkalmazása és az operátor felügyelete. Ezek a megoldások a humánerőforrás hatékony alkalmazását tehetik lehetővé.



1. ábra Az Internetes Segélyhívó Rendszer (ISR) alkalmazásának lehetőségei

Az Internetes Segélyhívó Rendszer alkalmazhatósága

Az Internetes Segélyhívó Rendszer alkalmazhatóságát tekintve, egy olyan űrt tölthet ki, ami jelenleg nem áll rendelkezésre. Figyelembe véve, hogy az informatika milyen szintű fejlődésen ment keresztül az elmúlt évtizedekben és jelenleg is napról napra rohamosan fejlődik, továbbá a jövőbeni alkalmazhatósága manapság még csak körvonalazódik, ezért azt merész vállalkozás lenne megjósolni, hogy az informatika hova és milyen formában fog betörni, vagy a jelenlegi területeken milyen irányba fog tovább fejlődni. [9] Ebből adódóan, valamint az eddigi tapasztalatok alapján az megállapítható, hogy az informatikai rendszereket újabbnál újabb támadások fogják érni, aminek megelőzésére és a kialakult helyzet azonnali felszámolására megoldásokat kell találni. [10] Továbbá az is várható, hogy a felhasználókat tekintve a már most is jelenlévő IoT eszközök alkalmazása tovább fog terjedni, ezáltal sokkal jobban ki leszünk szolgáltatva, sokkal több és veszélyesebb támadásokra kell felkészülniük a felhasználóknak és az üzemeltetőknek az internet okán. [11] Ennek érdekében egy, az általam elgondolt segélyhívó rendszer alkalmazásának létfontosságú jelentősége van. A kutatásaim során, hasonló megoldással működő rendszer alkalmazására utaló információkat nem találtam.

A konkrét alkalmazhatóságot tekintve olyan, jelenleg „szürke zónában” lévő területet lehetne kiszolgálni egy ilyen rendszerrel, amit most se a törvényi kötelezettség, se a piaci pozíció okán nincs védve hasonló megoldással. [12] Ilyen terület a kis- és középvállalkozások (KKV) informatikai rendszerei, amelyek önmagukban ugyan nem nagy számú munkaállomást, felhasználót és adatvagyont szolgál ki, de az előfordulásának számosságát tekintve jelentős akár csak Magyarországot tekintve. Ezeknek a kis- és középvállalkozásoknak jelentős szerepe van a hazai termelés és szolgáltatások területén, ezért a kormányzat jelenlegi programját tekintve, amely az Irinyi-program nevet viseli, az a szándéka, hogy a jelenleg zajló Ipar 4.0, azaz az ipar digitális transzformációjaként aposztrofált 4. ipari forradalom keretében a hazai kis- és középvállalkozások informatikai fejlesztését támogassa.

Továbbá az egyéni felhasználók tekintetében is nagy jelentőséggel bírna egy, az általam javasolt rendszer megvalósítása. Annak figyelembe vételével, hogy a felhasználó egymagában nem jelent kritikus mennyiséget, azonban, ha a felhasználók számosságát vesszük alapul, akkor akár beszélhetünk majdnem a teljes lakosságról, ami már önmagában jelentős számú mennyiséget jelent. 0

Meg kell említeni azokat az oktatási intézményeket is, amelyek nem állami fenntartásúak, ezáltal nem vonatkozik rájuk a már korábban említett 2013 évi L. törvény. Az iskolák digitalizációja és a diákok, hallgatók digitális kompetenciájának fejlesztése esetében kulcskérdés az iskolák korszerű informatikai infrastruktúrája és annak megfelelő szintű védelme. Ezért ezen intézmények informatikai védelme is jelentős fontossággal bír, ahol alkalmazható lehetne az általam javasolt rendszer.

Azon szervezetek, vagy vállalkozások esetében is lehetséges lenne az általam elgondolt rendszer alkalmazása, amelyek önkormányzatokkal vagy állami tulajdonú vállalatokkal állnak kapcsolatban, de rájuk szintén nem vonatkozik az információbiztonsági törvény, azonban részeit képezik az „ellátási láncnak", ezáltal kockázatos elemei egy-egy, a törvény által védett szervezetnek.

KÖVETKEZTETÉSEK

A fenti részben az általam elgondolt vészhelyzeti segélyhívó rendszert és annak megvalósítási és alkalmazási lehetőségeit mutattam be. Az előzményekben bemutattam a telefonos segélyhívó rendszert, mint az általam elgondoltak alapját képező megoldás kialakulását és a magyarországi helyzetét. Ezt követően bemutattam a vészhelyzeti online segélyhívó alkalmazást, ezen belül annak az informatikai rendszerek kártékony kódok elleni-, valamint az internetes zaklatás elleni védelmét és az informatikai rendszerek üzemeltetésének biztonságát, mint lehetőségeket. Bemutattam a vészhelyzeti online segélyhívó rendszer megvalósításának és alkalmazhatóságának elgondolását. Ennek keretében részleteztem az Internetes Vészhelyzeti Segélyhívó Rendszer megvalósításának lehetőségeit, és az Internetes Vészhelyzeti Segélyhívó Rendszer alkalmazhatóságát.

Az elgondolásom, annak megvalósítása esetén a felhasználók és az üzemeltetők biztonságát szolgálja. Az általam bemutatottakban olyan új megoldás biztosíthatja a biztonságot a kibertérben, amely egyedülálló módon szolgálná a felhasználók és a különböző, a jogszabály által védelmet nem élvező informatikai rendszerek biztonságát, amely forradalmasíthatja a biztonsági megoldásokat és védelmi lehetőségeket. Továbbá megállíthatja és visszaszoríthatja a jelenlegi kiberbűnözési módszereket.

Az Internetes Segélyhívó Rendszer szükségességét a korábbi vizsgálataim is alátámasztják. Az általam lefolytatott kérdőíves felmérés eredményei alapján elvégzett korrelációk bizonyítják [1], hogy a felhasználók, vagy üzemeltetők esetében egy-egy informatikai biztonsági esemény, vagy internetes zaklatás esetén nincs olyan alternatíva biztosítva a megoldásra, amely megnyugtató módon nyújtana védelmi lehetőséget ezen felhasználók és üzemeltetők számára. A jövőben várható fejlődési irányokat tekintve, amely érinteni fogja az otthonainkat (intelligens otthonok – smart home), valamint a közúti- és más közlekedéseinket (önvezető autók, intelligens vasút stb.), szükséges olyan védelmi megoldások kidolgozása és alkalmazása, ami azonnali, hatósági, valós beavatkozást biztosít az általam említett felhasználók és rendszerek számára. [14] Az Internetes Segélyhívó Rendszer alkalmazása jól illeszkedik az Európai Unió Európai Digitális Menetrend programjába és a Magyar Kormányzat Digitális Jólét Programjába, valamint az Irinyi Programba. Továbbá segítené a megvalósítását és nagyobb számú elterjedését a Smart City – azaz az okos város projekteknek, melyeknek a közeljövőben Magyarországon, Európában, és az egész világon a kialakítása, fejlesztése várható.

FELHASZNÁLT IRODALOM

[1] NYIKES, Z.: *A Közép-Kelet európai generációk digitális kompetencia és biztonságtudatosság vizsgálatának eredményei*, Hadmérnök, XII. Évfolyam 4. szám, 2017, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, pp. 159-173, ISSN 1788-1919

[2] RAJNAI, Z.; KERTI, A.: *A kormányzati IT rendszerek technológia-upgrade lehetősége*, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2011., 132 p.

[3] ŐSZI, A.; KOVÁCS T.: *A Jelen Kor Titkosítási Módszerei az Informatikában*, A Magyar Tudomány Ünnepe 2012 Konferencia Az Óbudai Egyetemen: Biztonságtechnikai Szekció., Budapest, Óbudai Egyetem, 2012., pp. 1-10., ISBN:978-615-5018-46-6

[4] HOLTAI, A.; MAGYAR, S.; PUSKÁS, B.: *Az informatikai fejlesztés és üzemeltetés határvonalai,* Felderítő Szemle, 2016, (1), pp. 191-203., 2016

[5] NYIKES, Z: *Creation Proposal for the Digital Competency Framework of the Middle-East European Region*, Key Engineering Materials, Vol. 755, pp. 106-111, 2017

[6] RAJNAI, Z.; FREGAN, B.: *Kritikus infrastrukturák védelme*, Kolozsvár, Erdélyi Múzeum-Egyesület (EME), 2016., pp. 349-352., Műszaki Tudományos Közlemények 5.

[7] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[8] RAJNAI, Z.: *Információtechnológiai kutatások a védelmi szektorban,* Az 5. Báthory-Brassai Konferencia tanulmánykötetei., 709 p., Budapest, Óbudai Egyetem Biztonságtudományi Doktori Iskola, 2014., pp. 1-12., 1-2. köt., ISBN:978-615-5460-38-8

[9] RAJNAI, Z.: *Planification of a Transmission Network*, Proceedings of the International Scientific Conference: New Trends in Signal Processing. 213 p., Liptovsky Mikulas: Armed Forces Academy of General Milan Rastislav Štefánik, 2012., pp. 134-141., ISBN:978-80-8040-447-5

[10] RAJNAI, Z.: *A Kritikus Információs Infrastruktúrák Összetétele, Biztonsági Kérdései,* Nemzetközi Gépész és Biztonságtechnikai Szimpózium: a Magyar Tudomány Ünnepe tiszteletére, Budapest, 2012., Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2012., pp. 15-22., [8]ISBN:978-615-5018-35-0

[11] KOVÁCS, T.; NYIKES, Z.; TOKODY, D.: *Komplex monitoring-rendszer használata vasúti felépítmény vizsgálatában az Ipar 4.0-hoz*, XVII. Műszaki Tudományos Ülésszak előadásai. ISSN 2393–1280, EME, MTK 6. szám, Kolozsvár, 2017, http://eda.eme.ro/handle/10598/30075?show=full, (letöltve: 2017.09.20.)

[12] TOKODY, D.; FLAMMINI, F.: *Smart Systems for the Protection of Individuals*, Key Engineering Materials, Vol. 755, pp. 190-197, 2017, DOI: 10.4028/www.scientific.net/KEM.755.190, https://www.scientific.net/Paper/Preview/525154 (letöltve: 2017.08.21.)

[13] TOKODY D.; SCHUSTER Gy.: *Driving Forces Behind Smart City Implementations-The Next Smart Revolutio*n., Journal of Emerging Research and Solutions in ICT 1.2, 2016, pp. 1-16., http://eprints.fikt.edu.mk/171/, (letöltve: 2017.03.18)

[14] SCHUSTER, Gy.; TOKODY, D.; MEZEI, I. J.: *Software reliability of complex systems focus for intelligent vehicles*, Vehicle and Automotive Engineering. Lecture Notes in Mechanical Engineering, 2017. ISSN: 2195-4356, pp. 309–321., Springer, Cham, DOI 10.1007/978-3-319-51189-4_28, https://link.springer.com/chapter/10.1007/978-3-319-51189-4_28, (letöltve: 2017.09.21.)