Óbudai Egyetem

Doktori (PhD-) értekezés tézisfüzete

Önkormányzatok kiberbiztonsági és online képességének vizsgálata, figyelemmel az emberi tényező fejlesztésének kérdéseire

Számadó Róza

Témavezető

Prof. Dr. Rajnai Zoltán

Dr. Belényesi Emese

Biztonságtudományi Doktori Iskola

Budapest, 2018

Tartalomjegyzék

Summary

Nowadays ICT tools, the internet are intertwined with the modern world and all aspects of life. This change has taken place abruptly, almost unnoticed. Security studies, in general information security as a discipline has undergone dynamic progress. Organisations of the public sphere - especially local governments - are slow to react to technological and citizens' expectations; organisational operation and organisational culture are slow to react by nature. The vulnerability of central and local governments to information security events and incidents has increased significantly in the past decades.

The research focus of my doctoral dissertation is the analysis of online presence and cybersecurity capabilities of local governments, taking into special consideration the significance of the human factor. In information society, changes in citizens' expectations and meeting information security challenges pose a significant challenge to local governments - in addition to accomplishing their extensive tasks. The complex security approach of information society originates from the interpretation of the people-technology-environment system as a whole. From these three elements, in my paper, I put the emphasis on the human factor. In my research I investigated whether a system of awareness-raising, education and cooperation can be formed that could help local governments meet citizens' and cyber security expectations.

In order to fulfil desired research ambitions, beyond cybersecurity questions, I also examined issues related to regulation, and consequently the character of municipal operation and the structure of local governance. In my research I aimed at achieving the complexity of theoretical correlations and practical application. The main purpose of reviewing literature and documents describing regulatory practices was to support empirical research and to place the results in the system. The attitudes, capabilities and practices of local governments regarding cyber security - based on the known theoretical and regulatory framework - were assessed through an online survey, whose results were also subjected to mathematical statistical analysis. I used factor and cluster analysis to explore the characteristics of online capabilities of local governments using data from the Ministry of Interior's nation-wide municipal data collection. Interpretation of the results and explanation of the main issues took place in a focus group interview.

Research results indicate that information security awareness of local governments is very low, which carries great risk considering cybersecurity trends, directions and this technological progress. The quick development of technology constantly increases vulnerability, making complete security impossible. As a result, prevention and improving resilience should be in focus, in which the individual is a key element. Critical attention should be given to the training, awareness-raising and motivation of officials, especially of executives by using a wide range of supporting toolsets. In order to use resources optimally, the possible benefits of horizontal and vertical cooperation and coordination between stakeholders should be reaped. Moreover, government organisations in cybersecurity need to regularly prepare short, comprehensible, online accessible guides for local

governments about cyber threat incidents; learning materials improving cyber defence, cybersecurity awareness that can be processed through the method of e-learning and self-learning.

I. A kutatás előzményei

Doktori értekezésem kutatási fókuszában a helyi önkormányzatok kiberbiztonságának és online megjelenési képességének a vizsgálata áll az emberi tényező jelenőségének fokozott figyelembevételével. Az információstársadalomban a helyi kormányzat elé – kiterjedt feladatai teljesítése mellett – jelentős kihívást állít az állampolgári elvárások változása és az információbiztonsági kérdések teljesítése. Az információs társadalom komplex biztonsági megközelítése az az ember–technika–környezet közös rendszerként történő értelmezéséből indul ki. E hármasból a dolgozatomban a fókuszt az emberi tényezőre helyeztem.

Tapasztalataim, a dokumentumelemzés és kutatásom alapján megállapítom, hogy a technológiai, szabályozási kérdések alapos figyelmet kapnak, ám az emberi tényező fejlesztése, kezelése nem kap kellő hangsúlyt, miközben az emberi erőforrások fejlesztése csak komplexen, a rendszer elvárásaihoz illesztve valósítható meg. A különböző felmérések évek óta hangsúlyozzák, hogy a „leggyengébb láncszem" a kiberbiztonsági kérdések kapcsán az emberi tényező. Az Institute of Information Security Professionals (IISP) IT biztonsági felmérése alapján a vezető kockázati tényező 2017-ben is a humán erőforrás (81%), míg a technológiai és a folyamatokból adódó kockázatok jóval kevésbé mérvadóak. [13] További fontos megállapítás, hogy a központi és helyi kormányzat – a szakértői vélemények szerint – minden más szektornál jobban kitett a kibertámadásoknak. Jelentős számú érzékeny adatot tárol és erőforrásai (emberi és technológiai) sokszor nem felkészültek, tudatosak vagy korszerűek. Növeli a veszélyeztetettség mértékét a kiberfenyegettség egyre komplexebbé válása, miközben általános a szakemberhiány, továbbá az (ön)kormányzati terület nem képes versenyezni a forprofit szféra kereseti kínálatával. A kutatási eredmények alapján az állami és helyi önkormányzati hivatalok világszerte hatalmas nyomás alatt vannak az adataik, infrastruktúrájuk és szolgáltatásaik biztonságossá tételét tekintve.

A témaválasztást több tényező is indokolta. Egyrészt személyes ambíciók a szervezeti működés, szervezetfejlesztés kérdéskörében és az infokommunikáció rohamos fejlődése által generált változás okozta szervezeti átalakulás vizsgálatában. Másrészt az ezredforduló óta foglalkozom különböző szerepekben az önkormányzatokkal. Szervezetfejlesztőként, változásmenedzsment tanácsadóként és az elmúlt években mint a szakmai támogatást és felügyeletet biztosító minisztérium szakmai területének aktív részese. Szakmailag és személyesen is különösen érdekes, fontos téma számomra az önkormányzati kötelezettségek teljesítése, teljesíthetősége, az önkormányzatok dolgozóinak információbiztonsági tudatossága, valamint ezen belül a kiberbiztonsági kérdések által felvetett felelősség és annak teljesítésére való képesség. Harmadrészt lenyűgöz az infokommunikáció (IKT) által kínált lehetőségek széles tárháza, és elgondolkodtat a benne rejlő veszély.

Az értekezés megközelítése, nézőpontja a szervezeti hozzáállás, tudatos működés, az emberi tényező, a humán erőforrás vizsgálata, és nem célja a technikai kérdések, a kiberfenyegetések kezelésének részletes kifejtése.

II. Célkitűzések, hipotézisek

Kutatásomban arra kerestem a választ, hogy kialakítható-e olyan tudatosítási, képzési és együttműködési rendszer, ami hozzásegíti az önkormányzatokat a velük szemben támasztott állampolgári és kiberbiztonsági elvárások teljesítéséhez.

Célkitűzéseim:

- javaslat a kiberbiztonság területén a központi és a helyi kormányzati feladatmegosztás és együttműködés kereteire (mindezt a hatékonyság javítása érdekében, differenciáltan az önkormányzati rendszer sajátosságaihoz igazítva);
- javaslat előterjesztése a képzési / továbbképzési rendszerre, érintettjeire és módszereire, az önkormányzatok kiberbiztonsági tudatosságának és a reziliencia javításának érdekében;
- általános és napi működési ajánlások megfogalmazása az önkormányzatok részére az információbiztonság növelése érdekében;
- önkormányzatokat online képességének vizsgálata, csoportosítása és jellemzése

Megfogalmazott kutatási hipotézisek:

1. Gyakorlati tapasztalataim azt mutatják, hogy a kormányzat és az önkormányzatok között nem alkalmazzák a kooperációból és koordinációból származó előnyöket. Feltételezem, hogy ennek az együttműködésnek a keretei csak hatósági szempontból kimunkáltak.
2. Feltételezem, hogy az önkormányzatok online képességének szintje alacsony és, hogy az online képesség pedig összefüggést mutat gazdasági helyzetükkel, lakosságszámukkal és hivatali struktúrájukkal.
3. Tapasztalom, hogy az önkormányzatok vezetői, munkatársai nem, vagy csak részlegesen ismerik az IT-biztonsági kockázatokat, a biztonságtudatosság az önkormányzati hivatalokban jellemzően alacsony szintű. Feltételezem, hogy az önkormányzat vezetői és tisztségviselői nincsenek a megfelelő tudás birtokában és a megfelelő tudatosítási és képzési rendszer jelentősen csökkentené a kiberbiztonsági incidensek előfordulását.
4. Az önkormányzatokkal végzett munkám tapasztalatai alapján feltételezem, hogy az önkormányzatok nem rendelkeznek megfelelő gyakorlati tervekkel, protokollokkal az esetleges események, incidensek kezelésére.

5. Feltételezem, hogy az online képesség mellett a kiberbiztonság megvalósítása területén fennálló problémák a szakember- és kapacitáshiányra vezethetők vissza.

III. Vizsgálati módszerek

Kutatásom során a kiberbiztonsági kérdéseken túl vizsgáltam a szabályozottság kérdését és szükségszerűen az önkormányzati működés sajátosságait, az önkormányzati rendszer felépítését. Kutatómunkám során törekedtem az elméleti összefüggések és a gyakorlati alkalmazás komplex vizsgálatára. A szakirodalom-elemzés és a szabályozási gyakorlatot bemutató dokumentumok elemzésének fő feladata a kutatás megalapozása és az eredmények rendszerbe illesztése volt. A dokumentumelemzés az információbiztonság, a kiberbiztonság fogalmi meghatározásától a gyakorlati kérdések áttekintéséig terjedt, különös tekintettel a kormányzati és az önkormányzati tapasztalatokra. Az európai és hazai szabályozást és a szervezeti keretek kialakításának és változásának áttekintését jelentős számú állásfoglalás, stratégiai dokumentum és jogszabály segítette. Az egyes nemzeti kiberbiztonsági stratégiák összehasonlítása lehetőséget teremtett jó gyakorlatok megismerésére.

A megismert elméleti és szabályozási keretekre építve összeállítottam egy kérdőívet, amely kiküldésre került a teljes önkormányzati kör részére. Célja az egyes önkormányzatok kiberbiztonsággal kapcsolatos attitűdjének, képességéknek és gyakorlatának megismerése volt.

A Belügyminisztérium országos önkormányzati adatfelvételét felhasználva faktor- és klaszteranalízist végeztem annak érdekében, hogy feltárjam az önkormányzatok online képességének jellemzőit.

Fókuszcsoportos interjút folytattam le a kutatási fázis végén a kapott eredmények értelmezése és a kérdéskörök tisztázása céljából.

Különös figyelmet fordítottam a nemzetközi és a hazai gyakorlati tapasztalatok elemzésére, az adatelemzésre és az online felmérés eredményeinek vizsgálatára, továbbá az értékelhető következtetések megfogalmazására. A kutatás lezárásra került 2018. február 15-én.

IV. Új tudományos eredmények

1. A szabályozási környezet, a kiberkoordináció, a szervezeti működés és a fókuszcsoportos interjú területein végzett kutatásaim alapján – a hipotézisemben felvetett feltételezéseimet igazolva – be**bizonyítottam, hogy a kormányzat és az önkormányzatok között a kapcsolat csak adminisztratív és hatósági szempontból kimunkált, továbbá nem alkalmazzák a kooperációból, koordinációból és együttműködésből származó előnyöket. Kidolgoztam és javaslatot tettem a kiberoordináció szabályozási és szervezeti működésének módosítására** (1. függelék).
2. **Bebizonyítottam, hogy az önkormányzatok gazdasági helyzete, a lakosságszám és a hivatali struktúrájuk az online képességük jelentősen befolyásoló tényezői.** Hipotéziseimet faktor- és klaszteranalízis elemzésekkel igazoltam, **kimutattam az online képesség** (webability) **feltételeinek szoros, a működést befolyásoló összefüggéseit**. Kutatási eredményeim alapján **kidolgoztam az önkormányzatok online képesség szerinti besorolását** (2. függelék). Kimutattam, hogy egyértelmű összefüggés mutatkozik a jobb online képesség és az önkormányzatok magasabb lakosságszáma, továbbá az önálló vagy székhely-önkormányzati hivatal megléte és az adóerő-képesség nagysága között, azzal a kitétellel, hogy önmagában az adóerő-képesség nem hat pozitívan az online képességre.
3. **A nemzetközi tapasztalatok feldolgozása és saját kutatásaim alapján igazoltam**, **hogy az önkormányzatok vezetői, munkatársai nincsenek tisztában az információbiztonsági kockázatokkal és tudatosságuk nagyon alacsony szintű, a fenyegetettség mértékét alul becsülik.** Az információbiztonság kérdéskörének megfelelő szintű kezelésében az önkormányzatok esetében különösen kritikus szerepe van a vezetőknek. Az IT kockázatokat nem, vagy csak részlegesen ismerik, a biztonságtudatosság az önkormányzati hivatalokban jellemzően alacsony szintű. Az alacsony tudás és tudatossági szint emelésére **továbbfejlesztettem a jelenlegi képzési elemeket is tartalmazó tudatosítási és képzési rendszert**, **amelyek bevezetésére javaslatot dolgoztam ki** az önkormányzatok információbiztonságban érintett vezetői, felelősei és résztvevői számára (3. függelék).
4. Empirikus kutatási módszerekkel **igazoltam, hogy az önkormányzatok nem rendelkeznek** az információs rendszerük használatához szükséges, a biztonságos működést támogató **protokollokkal,** egyszerűbb ellenőrzési listákkal, útmutatókkal a napi információbiztonsági feladatok ellátáshoz. Segítségül **egyszerű ellenőrzési listát dolgoztam ki**, amit használatra javaslok az önkormányzatok számára (4. függelék).
5. A fókuszcsoportos kutatás igazolta, hogy kapacitás, a szakember- és az erőforráshiány miatt az 5000 fő lakosságszám alatti települések többnyire külső vállalkozásokkal oldják meg az IT és IT biztonsági feladataikat, így sem a folytonosság, sem a naprakészség nem valósul meg.

V. Az eredmények hasznosítási lehetősége

A kutatás eredményei alapján több a gyakorlatba hasznosítható eredményt és ajánlást fogalmaztam meg:

A) A kooperáció és koordináció területén

- A kutatás eredményei alapján javaslom, hogy a kormányzati kiberkoordináció kerüljön kibővítésre és az önkormányzati szektor kerüljön bevonásra.
  Ez jelenti egyrészt a Nemzeti Kibervédelmi tanács kibővítését az önkormányzatokért felelős miniszter képviselőjével, másrészt önkormányzati kiberbiztonsági munkacsoport létrehozását. Ehhez szükséges beavatkozás a 2013. évi L. törvény és a 484/2013. (XII. 17.) Korm. rendelet vonatkozó részeinek módosítása.
- A koordinációból származó előnyök kiaknázása érdekében javaslom a központi kormányzati szervezetek és az önkormányzatok közötti operatív koordinációs működés megvalósítását. Tekintettel a téma, a feladat komplexitására és a terület átalakulási sebességére javaslom a felelős miniszter irányítása alatt operatív munkaszervezet létrehozását, hogy biztosított legyen a nagyszámú érintett közötti horizontális és vertikális információáramlás, együttműködés. Kiemelt figyelemmel:
  - az aktuális helyzet feltérképezése, a felmerülő problémák, nehézségek összegyűjtése, becsatornázása a Tanács felé;
  - az önkormányzatokat érintő szabályozás véleményezése, javaslattétel;
  - közreműködés önkormányzati ellenőrző listák, útmutatók, módszertanok kidolgozásában és disszeminálásában;
  - az önkormányzati tudatosság rendszeres felmérése és a tudatosító akciók, rendezvények, versenyek szervezése;
  - együttműködés önkormányzati érdekképviseleti szervezetekkel az információbiztonság témakörében;
  - önkormányzati jó gyakorlatok gyűjtése és terjesztése;
  - önkormányzati információbiztonságban érintett szervezetek információmegosztási és partnertségi platformjának létrehozása és operatív munkaszervezeti feladatainak ellátása.

B) Önkormányzati információbiztonsági képzési rendszer átalakítása, bővítése.

A kutatási eredmények az mutatják, hogy az önkormányzatok információbiztonsági tudatossága nagyon alacsony, ami a kiberbiztonsági trendeket, irányokat és ez a technológiai fejlődést figyelembe véve hatalmas kockázatot hordoz. A technológia gyors fejlődése folyamatosan növeli a kitettséget, lehetetlenné vált a teljes biztonság megteremtése, ezért a megelőzésre és az ellenálló képesség növelésére kell koncentrálni, amelynek kritikus eleme az ember. Kiemelt figyelmet kell szentelni a tisztviselők, ezen belül is a vezetők felkészítésének, tudatosításának és motiválásának a támogató eszköztár széleskörű felhasználásával.

A hazai képzési palettát áttekintve sturkturált képzést és továbbképzést az NKE biztosít, azonban a gyakorlatiasság, a tudatosítás egyéb módszerei, az önkormányzati hivatalok felkészítése hiányos és hiányoznak az egyszerű, könnyen érthető és autodidakta módon feldolgozható képzési anyagok. A fentiek és a fókuszcsoportos kutatásban megfogalmazódott önkormányzati elvárásoknak való megfelelés érdekében a rendszer átalakítása, kiegészítése szükséges.

Javaslom, az általam felvázolt képzési, tudatosítási és rezilienciát növelő komplex rendszer részletes kidolgozását és bevezetését.

C) Önkormányzati információbiztonsági rutinjának kialakítása, folyamatos támogatása

Javaslom, hogy az önkormányzatok részére, hogy valósítsanak meg központi menedzsmentet, vezessenek be kétszintű azonosítást, vezessék be a napi biztonsági mentést, dolgozzanak ki és alkalmazzanak védekező és reagáló képességet támogató eljárásrendeket. Javaslom továbbá, hogy az általam kidolgozott ellenőrző listára építve dolgozzanak ki – az adott szervezet sajátosságaihoz illeszkedő egyszerű – saját információbiztonsági check listát.

Javaslom a kiberbiztonsági kormányzati szervezeteknek, hogy az önkormányzatok részére

- készüljön rendszeresen (havonta, háromhavonta) rövid, köznapi nyelven, online formában útmutató a kiberfenyegetettségi eseményekről;
- készüljön legalább évente rövid közérthető módszertani útmutató;
- készüljenek nem szakmai nyelvezettel, autodidakta módon feldolgozható e-learning módszerű kibervédekezési, kiberbiztonsági tudatosságot javító képzési anyagok.

D) Önkormányzatok online képességének

Az önkormányzatok számára – az eredmények alapján - az Infotv. teljesíthetősége, az állampolgárok bizalmának megerősítése, a település népességmegtartó képességének növelése és a versenyképesség javítása érdekében javaslom,

- hogy alkalmazásra kerüljenek települési online képesség javítását támogató integrált módszertanok (web és közösségi média alkalmazása települési környezetben);
- hogy erőforráshiányos környezetben mérjék fel az önkormányzatok a lakosaik online fogyasztási szokásait - az erőforrások optimális felhasználása érdekében -, hogy megfelelő irányba kezdjék meg a fejlesztéseket.

VI. Irodalmi hivatkozások jegyzéke

[1] BUKOVICS, I.: Létfontosságú infrastruktúrák; KDI előadás, 2016

[2] BEREK, L.: Biztonságtechnika, NKE, Budapest, 2014.

[3] MUNK, T. H.: Cyber-security in the European Region: Anticipatory Governance and Practices; The University of Warwick 2015. https://www.research.manchester.ac.uk/portal/files/54570851/FULL_TEXT.PDF (letöltve: 2018. 01. 22.)

[4] BUKOVICS, I.: A kritikus infrastruktúrák rendszerkoncepciója - Egy kérdőív módszertani kritikája; In: HORVÁTH, A. /szerk./: Fejezetek a kritikus infrastruktúra védelemből Tanulmánykötet, Budapest, Magyar hadtudományi Társaság, 2013. pp.58–75.

[5] Országos Katasztrófavédelmi Főigazgatóság (OKF): A kritikus infrastruktúra. http://www.katasztrofavedelem.hu/index2.php?pageid=lrl_index (letöltve: 2018. 03. 07.)

[6] RAJNAI Z. – FREGAN B.: Kritikus infrastruktúrák védelme (jogi szabályozás). In: BITAY E. /szerk./:XXI. Fiatal Műszakiak Tudományos Ülésszaka. Kolozsvár: Erdélyi Múzeum-Egyesület, 2016. pp. 349–352. http://hdl.handle.net/10598/29102 (letöltve: 2018. 03. 15)

[7] BONNYAI T.: A kritikusinfrastruktúra-védelem elemzése a lakosságfelkészítés tükrében (doktori értekezés tervezet) Budapest: NKE, 2014. DOI azonosító: 10.17625/NKE.2015.001

[8] ERDŐSI P. M. – CISA: ECDL / ICDL, IT biztonság; Budapest, Neumann János Számítógép-tudományi Társaság. 2013.

[9] HORVÁTH G. K.: Közérthetően (nem csak) az IT biztonságról; Budapest, KIFÜ 2013. http://www.kifu.gov.hu/kifu/sites/default/files/IT_brosura_v7.pdf (letöltve: 2018. 03. 05.)

[10] RAJNAI Z.: Információbiztonság tudatosság, In: BITAY E. /szerk./: XXI. Fiatal Műszakiak Tudományos Ülésszak Előadásai. Kolozsvár: Erdélyi Múzeum-Egyesület, 2017. pp.37–42. http://hdl.handle.net/10598/29758 (letöltve: 2018. 03. 15.)

[11] BELÁZ A. – BERZSENYI D.: Kiberbiztonsági Stratégia 2.0 – A kiberbiztonság stratégiai irányításának kérdései. Elemzések. Budapest, Stratégiai Védelmi Kutatóközpont 2017. http://netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-3-kiberbiztonsagi-strategia-2-0-belaz-a-berzsenyi-d.original.pdf (letöltve: 2017. 08. 23.)

[12] JUNCKER, Jean-Claude, az Európai Bizottság elnökének beszéde: Az Unió helyzete 2017. szeptember 13.; Strasbourg 2017. https://ec.europa.eu/commission/sites/beta-political/files/state-union-2017-brochure_hu.pdf (letöltve: 2018. 03. 15.)

[13] MUNCASTER, P.: Security Pros: People Are the Biggest Problem, Infosecurity Magazine, UK 2017. https://www.infosecurity-magazine.com/news/security-pros-people-are-the/ (letöltve:2018. 02. 20.)

[14] European Commission: Resilience, Deterrence and Defence: Building strong cybersecurity in Europe; https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe (letöltve: 2018. 02. 21.)

[15] European Union Agency for Network and Information Security: ENISA Threat Landscape Report 2017. Top 15 Cyber-Threats and Trends; https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017 (letöltve: 2018. 02. 24.)

[16] Panda Security: 2017 Cybersecurity Trends; 2017. https://www.pandasecurity.com/mediacenter/pandalabs/annual-report-cybersecurity-predictions-2018/ (letöltve: 2018. 03. 18.)

[17] OLAJOS M.: Az IoT eszközök térnyerése az adatvédelem tükrében In: BOGÁRDI D. – KOCSIS G. /szerk./: Jog és innováció tanulmánykötet. Stádium Intézet Alapítvány Budapest, 2017. pp. 17–28. http://arsboni.hu/wp-content/uploads/2018/03/Arsboni-Tanulm%C3%A1nyk%C3%B6tet_20180305_uj_borit%C3%B3.pdf (letöltve: 2018. 03. 27.)

[18] EGGERS, W. D.: Government's cyber challenge. Protecting sensitive data for the public good; Deloitte Review 19. (2016) pp. 138–155. https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/risk/DR19-governments-cyber-challenge.pdf (letöltve: 2018. 02. 23.)

[19] LIPMAN P.: 4 Critical challenges to State and Local Government Cybersecurity Efforts (Industry Perspective); http://www.govtech.com/opinion/4-Critical-Challenges-to-State-and-Local-Government-Cybersecurity-Efforts.html (letöltve: 2018. 02. 22.)

[20] ROMERO L.: Eye-Opening Findings About Local Government Cyber Security; https://www.pivotpointsecurity.com/blog/local-government-cyber-security-issues/ (letöltve: 2018. 02. 22.)

[21] Socitm Insight Briefing: Push for local cyber security and resilience; Socitm Insight Briefing 83. (2015). http://www.socitm.net/insight (letöltve: 2018. 02. 21.)

[22] European Commission: Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity in Europe; http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450 (letöltve: 2018. 02. 22.)

[23] Európai Digitális Egységes Piaci Stratégia; http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM:3102_3 (letöltve: 2018. 03. 18.)

[24] Az európai digitális menetrend: http://www.europarl.europa.eu/atyourservice/hu/displayFtu.html?ftuId=FTU_2.4.3.html (letöltve: 2018. 03. 19.)

[25] Európai Digitális Egységes Piaci Stratégia; http://eu.kormany.hu/europai-digitalis-egyseges-piaci-strategia (letöltve: 2018. 03. 18.)

[26] Európai Bizottság tájékoztatója: Hogyan érinti az adatvédelmi reform a közösségi hálózatokat? 2016; file:///C:/Users/DrIsk/Downloads/PP-2016-00621-00-00-HU-TRA-00.pdf (letöltve: 2018. 01. 25.)

[27] BERZSENYI D.: Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése; Nemzet és Biztonság VII. 6. (2014) pp. 110–136. file:///C:/Users/DrIsk/Downloads/_cikkek_nb_2014_6_10_berzsenyi%20(2).pdf (letöltve: 2018. 02. 04.)

[28] MOLNÁR D.: Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia; Hadmérnök XII. „KÖFOP" (2017) pp. 149–162.

[29] Digitális Jólét Program 2.0; Budapest 2017. http://www.kormany.hu/download/6/6d/21000/DJP20%20Strat%C3%A9giai%20Tanulm%C3%A1ny.pdf (letöltve: 2018. 03. 17.)

[30] RAJNAI Z. – FREGAN B.: Új alapokon a Magyarországi kibervédelmi stratégia. In: BITAY E. /szerk./: XXI. Fiatal Műszakiak Tudományos Ülésszak Előadásai. Kolozsvár: Erdélyi Múzeum-Egyesület, 2017. pp. 351–354. http://eda.eme.ro/bitstream/handle/10598/29842/XXII_FMTU_Rajnai.pdf?sequence=3 (letöltve: 2018. 02. 28.)

[31] ILLÉSSY M. – NEMESLAKI A. – SOM Z.: Elektronikus információbiztonság – tudatosság a magyar közigazgatásban; Információs Társadalom XIV. 1. (2014) pp. 52–73. http://real.mtak.hu/41849/1/i_tarsadalom_2014_1_illessy_nemeslaki_som.pdf (letöltve: 2018. 03. 17.)

[32] VERECZKEI Béla *Elektronikus információbiztonsági ellenőrzések tapasztalatai* című előadása az Önkormányzati Road Show keretében, 2017. október 04.

[33] KOVÁCS É.: Koordinációs mechanizmusok és fejlődésük az államigazgatásban (1990–2014). Phd-értekezés. Budapest, Budapesti Corvinus Egyetem Politikatudományi Doktori Iskola 2014. pp. 20–21. http://phd.lib.uni-corvinus.hu/788/1/Kovacs_Eva.pdf (letöltve: 2017. 12. 12.)

[34] RAJNAI Z.: Kibervédelem és kiberkoordináció. Vállalti aspektusok – vízió 2016. Budapest, 2016. njszt.hu/sites/default/files/rajnai.pptx (letöltve: 2018. 04. 08.)

[35] A Nemzeti Infokommunikációs Stratégia 2014–2020. Az infokommunikációs szektor fejlesztési stratégiája (2014–2020) v9.0; 2014. ttp://www.kormany.hu/download/a/f7/30000/NIS_v%C3%A9gleges.pdf (letöltve: 2018. 03. 10.)

[36] E-közigazgatási keretrendszer koncepció; Budapest, Belügyminisztérium 2015. http://www.kormany.hu/download/0/05/50000/E-k%C3%B6zigazgat%C3%A1si_keretrendszer_koncepci%C3%B3.pdf (letöltve: 2018. 02. 28.)

[37] MOLNÁR D.: Egységes Európai kibertér? Az Európai Unió kiberbiztonsági stratégiájának fejlődése; Hadmérnök XII. 1. (2017) pp. 255–267.

[38] KÓNYA L. – FARKAS ZS. – PUSZTAI A. – TÓZSA I. – SIMON B. – TÓTH F.: Önkormányzatok jogállása és döntési kompetenciája; Budapest, NKE 2014. p. 12.

[39] Önkormányzatiság Magyarországon; Kormányportál. http://2010-2014.kormany.hu/hu/mo/onkormanyzatisag-magyarorszagon (letöltve: 2017. 03. 10.)

[40] BEKÉNYI J. /szerk./: Szabályozási segédlet a helyi önkormányzati feladatok ellátásához; Budapest, Belügyminisztérium 2017.

[41] Érdemi nyilvánosság az önkormányzati döntéshozatalban. Útmutató helyi önkormányzatoknak; Budapest, NVSZ 2016. http://korrupciomegelozes.kormany.hu/download/6/42/a1000/%C3%9ATMUTAT%C3%93.pdf (letöltve: 2018. 03. 10.)

[42] Információszabadság állásfoglalások, jelentések; Budapest, NAIH. https://www.naih.hu/informacioszabadsag-allasfoglalasok,-jelentesek.html (letöltve: 2018. 03. 11.)

[43] BUDAI B. B. – HERMAN Sz.: Az Infotv. közzétételi kötelezettségének gyakorlata. Önkormányzati tanácsadó 3. Budapest, Menedzser praxis. 2018.

[44] NEWMAN D.: Top 6 Digital Transformation Trends In Government; 2017. https://www.forbes.com/sites/danielnewman/2017/06/29/top-6-digital-transformation-trends-in-government/#2e4e52dc7efc (letöltve: 2018. 01. 02.)

[45] ITBUSINESS: DJP 2.0: jött, látott, győzött; 2017. http://www.itbusiness.hu/Fooldal/rss_3/DJP_20_jott_latott_gyozott.html (letöltve: 2018. 03. 17.)

[46] Digitális Jólét Program: Magyarország Digitális Oktatási Stratégiája (DOS); 2016. http://www.kormany.hu/download/0/cc/d0000/MDO.pdf (letöltve: 2018. 03. 17.)

[47] (n. n.) Rosszul elköltött pénz; Biztosítási szemle 2017. http://www.biztositasiszemle.hu/cikk/elemzesek/NULL/rosszul_elkoltott_penz.6865.html (letöltve: 2018. 02. 03.)

[48] GAJDUSCHEK Gy.: Miben áll, és mérhető-e a kormányzati teljesítmény? Politikatudományi Szemle 2014. 23. évf. 3. szám pp. 97–118. http://www.poltudszemle.hu/szamok/2014_3szam/gajduschek.pdf (letöltés: 2017. 12. 21.)

[49] ENDRŐDI I.: Polgári védelmi ismeret. Budapest, Magyar Polgári Védelmi Szövetség 2015. www.mpvsz.hu/letoltes/document/download.php?id=125-polgari-vedelemi-ismeret2015.pdf (letöltve: 2018. 04. 05.)

[50] 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

[51] A Bizottság közleménye a Tanács és az Európai Parlament részére – A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben

[52] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

[53] 2016. évi CXVI. törvény az egyes belügyi tárgyú törvények módosításáról

[54] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról;

[55] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

[56] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

[57] 2012/2015. (XII. 29.) Korm. határozat az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (InternetKon) eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról

[58] 38/2012. (III. 12.) Kormányrendelet a kormányzati stratégiai irányításáról

[59] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[60] 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

[61] 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól

[62] 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről

[63] A TANÁCS 98/83/EK IRÁNYELVE (1998. november 3.) az emberi fogyasztásra szánt víz minőségéről

[64] 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól

[65] 2016. évi CL. törvény az általános közigazgatási rendtartásról

[66] 2013. évi CCXX. törvény az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól

[67] Magyarország Alaptörvénye (2011. április 25.)

[68] 2011. évi CLXXXIX. törvény Magyarország helyi önkormányzatairól

[69] 273/2012. (IX. 28.) Korm. rendelet a közszolgálati tisztviselők továbbképzéséről

[70] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[71] 2015. évi XCVI. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény és a közadatok újrahasznosításáról szóló 2012. évi LXIII. törvény módosításáról

[729] 61/2012. (XII. 11.) BM rendelet a települések katasztrófavédelmi besorolásáról, valamint a katasztrófák elleni védekezés egyes szabályairól szóló 62/2011. (XII. 29.) BM rendelet módosításáról

[73] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről;

[74] 2015. évi CXXX. törvény az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról

[75] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

[76] 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

[77] Önkormányzati rendeletek – Nemzeti Jogszabálytár. http://njt.hu/njt.php?onkormanyzati_rendeletek (letöltve: 2018. 03. 21.)

[78] Magyar Államkincstár Általános Információk: http://www.allamkincstar.gov.hu/hu/koltsegvetesi-informaciok/torzskonyv_altalanos (letöltve: 2018. 03. 21.)

VII. A tézispontokhoz kapcsolódó tudományos közlemények jegyzéke

1. Számadó Róza

Önkormányzatok helye a kormányzati kiberkoordinációban

JEGYZŐ ÉS KÖZIGAZGATÁS XX:(2) p.27. 29 p. (2018)

2. Számadó Róza

Önkormányzatok kiberbiztonsági helyzete a nemzetközi és hazai tapasztalatok tükrében

ÚJ MAGYAR KÖZIGAZGATÁS 11:(2) p. 1. 5 p. (2018)

3. Számadó Róza

Analysing online capabilities of local governments

ACTA TECHNICA CORVINIENSIS – BULLETIN OF ENGINEERING 2018:(3) p. 1. 12 p. (2018)

4. Számadó Róza

ÖNKORMÁNYZATOK MEGFELELÉSI KÉPESSÉGE A KIBERBIZTONSÁGI KIHÍVÁSOKNAK: Online felmérés eredményei

ÚJ MAGYAR KÖZIGAZGATÁS 2018:(3) pp. 1-12. (2018)

5. Számadó Róza

Impact of Leaders: The Impact of the Engagement of Local Government Leaders' on the Effectiveness of Participatory Planning as Found in the Local Community Academy Program1 (2014–2015)

ACADEMIC AND APPLIED RESEARCH IN MILITARY AND PUBLIC MANAGEMENT SCIENCE 16:(1) pp. 63-76. (2017)

VIII. További tudományos közlemények

6. Számadó Róza

Inkluzív önkormányzat építés: Az Önkormányzati szaktanácsadó szakirányú továbbképzési szak Inkluzív önkormányzat és fejlesztéspolitika I. c. tantárgyának egyetemi tankönyve

Budapest: Dialóg Campus Kiadó, 2018. 97 p.

(Önkormányzati szaktanácsadó szakirányú továbbképzési szak)

(ISBN:978-615-5889-06-6)

7. Számadó Róza (szerk.)

Inkluzív önkormányzat tervezés: Önkormányzati szaktanácsadó szakirányú továbbképzési szak Inkluzív önkormányzat és fejlesztéspolitika II. c. tantárgyának egyetemi tankönyve

Budapest: Dialóg Campus Kiadó, 2018. 126 p.

(ISBN:978-615-5889-04-2)

8. Belényesi Emese , Számadó Róza

Önkormányzatok tervezési gyakorlata – tervek és a valóság.

ÚJ MAGYAR KÖZIGAZGATÁS 3:(3) pp. 28-40. (2015)

9. Farkasné Gasparics Emese , Számadó Róza

A településmenedzsment átalakulása a működési keretek tükrében

POLGÁRI SZEMLE: GAZDASÁGI ÉS TÁRSADALMI FOLYÓIRAT 11:(1--3) pp. 1-15. (2015)

10. Holcreiter Marianna , Számadó Róza , Szilágyi Ildikó , Treszkán Hováth Viktória

Pályázatmenedzsment

Budapest: Nemzeti Közszolgálati Egyetem, 2015. 149 p.

(ISBN:978-615-5057-41-0)

11. Számadó Róza , Gáspár Mátyás , Göndör András , Belényesi Emese , Brecsok Anna , Jenei Ágnes , Dömötör Ildikó

Csóka Gabriella (szerk.)

Fejlesztő közösségek: A helyi közösségi akadémiák hálózata

Budapest: Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, 2015. 62 p.

12. Számadó Róza

Inkluzív önkormányzat

Budapest: Nemzeti Közszolgálati Egyetem, 2015. 130 p.

(ISBN:ISBN 978 615 5057 35 9)

13. Számadó Róza (szerk.)

Módszertani kézikönyv: Szociális szövetkezetek az alakulástól a fenntartható működésig

Budapest: Országos Foglalkoztatási Közalapítvány (OFA), 2011.