PRO PUBLICO BONO – Magyar Közigazgatás, 2017/2, 120–137.

Kollár Csaba – Vinogradov Szergej

A MAGYARORSZÁGI KÖZSÉGI ÉS VÁROSI ÖNKORMÁNYZATOK VEZETŐ TISZTSÉGVISELŐINEK INFORMÁCIÓBIZTONSÁG-TUDATOSSÁGA[1]

Information Security Awareness of Senior Local Government Officers in Hungarian Villages and Towns

Dr. Kollár Csaba PhD, oktató, NKE Katonai Műszaki Doktori Iskola, kollar.csaba@uni-nke.hu

Dr. Vinogradov Szergej PhD, tanszékvezető egyetemi docens, SZIE Gazdaságelemzési Módszertani Tanszék, vinogradov.szergej@gtk.szie.hu

Tanulmányunkban először az információbiztonság teoretikus vonatkozásait ismertetjük, nevezetesen a jogalkotói szándék törvényi lenyomatait, az önkormányzati vezetők munkáját segítő fontosabb szakirodalmakat, illetve a Nemzeti Közszolgálati Egyetem tankönyveit. Az írásunkban feldolgozott forrásokon keresztül azt vizsgáljuk, hogy az információbiztonság-tudatosság fejlesztése mennyire hangsúlyosan jelenik meg ezekben a könyvekben, melyeknek célcsoportjai többek között az önkormányzati vezető tisztségviselők. A KSH országos településadatainak rövid elemzése után saját, nagy mintás online kutatásunk lebonyolításának bemutatásával foglalkozunk, majd a városok és a községek vezető önkormányzati tisztségviselőinek információbiztonság-tudatosságában esetleges eltérések kimutatására irányuló empirikus kutatásunk eredményeit mutatjuk be, három hipotézis mentén. Tanulmányunk záró részében rámutatunk az információbiztonság-tudatosság fejlesztésének fontosságára, illetve javaslatot teszünk néhány, a gyakorlatban is megvalósítható szakmai szolgáltatási módszerre.

[1] A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálatfejlesztés" elnevezésű kiemelt projekt keretében működtetett Zrínyi Miklós Habilitációs Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak:
információbiztonság, információbiztonság-tudatosság, képviselő-testület, önkormányzat, polgármester

The study first of all discusses the theoretical aspects of information security, namely the legal imprints of legislative intentions, the main references of specialised literature used by heads of local governments for their work and the textbooks of the National University of Public Service. With the help of references reviewed in the present paper, we examine the importance of the development of information security awareness in these books and their targets. These targets are mostly the senior officers of local governments. Following the short analysis of national settlement data provided by KSH (Hungarian Statistical Office), our large-sample online research is discussed, then we introduce the results of our empirical research exploring the possible deviations in the information security awareness of senior local government officers in cities and villages. The research results are drafted around three hypotheses. The closing chapter of our study highlights the importance of developing information security awareness and includes recommendations for several professional service methods which can be implemented in practice.

Keywords:
information security awareness, information security, local government, mayor, members of local government

1. BEVEZETÉS

A digitális kor gazdasági hatásai és társadalmi vetületei a korábbi korokhoz képest másfajta elméletek, modellek, módszerek, technikák megjelenését és elterjedését eredményezték, illetve ezekkel párhuzamosan másfajta értékrend kialakítását kívánják meg a jelen társadalmunk valamennyi szereplőjétől. Az információk felértékelődnek, egyre inkább vagyonként tekintünk rájuk, melynek védelme az információbiztonság komplex tevékenységében realizálódik. A törvények, rendeletek, illetve a szervezeti szabályzatok egyfajta keretrendszerként szolgálnak valamennyi vezető és beosztott számára az elvárt információbiztonsági magatartással kapcsolatban, azonban hosszú távú eredmény csak akkor érhető el, ha az információbiztonság-tudatosság fejlesztése a szervezetek nagyságától és tevékenységétől függetlenül valamennyi érintett esetében hatékony módszerekkel biztosítható.

A kormány 2014–2020 közötti időszakra vonatkozó Közigazgatás- és Közszolgáltatás-fejlesztési Stratégiájának célja a szolgáltatásokat igénybe vevő ember és az emberek bizalmát élvező szolgáltató állam kapcsolatának kialakítása és hatékony működtetése. Mivel a digitális korban a kapcsolatok egyre nagyobb része digitális platformokon keresztül valósul meg (értve ezalatt az állampolgár és a kormányzat/önkormányzat kapcsolatát is), így ezeknek a platformoknak a biztonságos használata, a használatukból eredő félelmek csökkentése, s általánosságban a digitális kompetenciák fejlesztése kiemelt jelentőséggel bír. A Stratégia 7.2.2.5 alpontja a közigazgatásban tevékenykedők továbbképzésével kapcsolatban a 77. oldalon úgy fogalmaz, hogy „a feladatellátáshoz kapcsolódó ismereteken túl lényeges feladat az IT-biztonság és az ezzel kapcsolatos tudatosság fejlesztése is".

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban Ibtv.) kiterjed a helyi önkormányzatok képviselő-testületének hivatalaira, s ezzel összhangban a polgármesterekre, az önkormányzatok vezető tisztségviselőire (alpolgármester, jegyző, titkárságvezető, osztályvezető stb.), a képviselő-testület tagjaira, valamint a hivatalban dolgozókra is. A személyhez kötött fontosabb feladatokkal és kötelezettségekkel kapcsolatban Bodó (2014) úgy fogalmaz, hogy *„az Ibtv. … rendelkezik a szervezet vezetőjének szerepvállalásáról, aki munkáltatói jogkörében eljárva kinevezi vagy megbízza az elektronikus információs rendszer biztonságáért felelős személyt, továbbá köteles gondoskodni az oktatásról és az információbiztonsági ismeretek szinten tartásáról".*

Saját – primer – kutatásunkat megelőzően az önkormányzati vezetők munkáját segítő irodalmat elemeztük, s a megjelent műveket öt nagy kategóriába soroltuk a biztonság fogalmának értelmezése és használata szempontjából.

1. A gazdálkodással (pl. Varga, 2010, Győrffi et al., 2011) foglalkozó könyvek szerzői a biztonság fogalmát és megközelítését rendszerint az állampolgárok élet- és vagyonbiztonságát veszélyeztető elemi csapás, illetve következményeinek elhárítása kontextusban értelmezik.
2. A napi működtetéssel, elsősorban a jogi és vezetési ismeretekkel foglalkozó szakirodalom (pl. Balás et al., 2015, Varga és Gergely, 2005) a biztonság fogalmának tárgyalásakor elsősorban a munkavédelemben megjelenő, az egészséget nem veszélyeztető és biztonságos munkavégzés követelményeit, illetve személyi feltételeit veszi alapul.

3. A polgármesterről szóló, illetve gondolatait tükröző könyvek (pl. Serényi, 2015, Szita, 2015) nem említik az információbiztonsággal kapcsolatos tevékenységeket, illetve a biztonságtudatosság fejlesztését.
4. Az elektronikus közigazgatásról szóló könyvek (pl. Budai és Szakolyi, 2005, Budai, 2013) a törvényi és a szakmai protokollok szerint használják a biztonság fogalmát, az információbiztonság-tudatosság, illetve a biztonságtudatosság fejlesztése azonban nem szerepel számottevő súllyal ezekben az írásművekben.
5. A Nemzeti Közszolgálati Egyetemen folyó oktató/nevelő munkához kapcsolódó, a közigazgatásban dolgozók képzését és továbbképzését segítő tankönyvek (pl. *Számadó,* 2015, Simon és Budai, 2015), illetve kiemelten a *Közigazgatási alapvizsga tankönyv*e (Almásy et al., 2016), az *Ügykezelői alapvizsga tankönyve* (Pócsi, 2016), a *Titkos ügykezelői képzés tankönyv*e (Tapa és Hegedűs, 2014) már kellő részletességgel, külön fejezet(ek)ben foglalkozik az információbiztonsággal, de még ezeknél a forrásoknál sem jelenik meg hangsúlyosan az információbiztonság-tudatosság fejlesztése.

A jelenleg érvényben lévő törvényi szabályozás szerint (pl. 2013. évi XXXVI. törvény, 1989. évi XXXIV. törvény, 2010. évi L. törvény) mindenki választható, aki választójoggal rendelkezik. A helyi önkormányzati képviselők és polgármesterek választásán nem választható, aki jogerős ítélet alapján szabadságvesztés büntetését vagy büntetőeljárásban elrendelt intézeti kényszergyógykezelését tölti. Ez – témánk vonatkozásában – azt jelenti, hogy a megfelelő vezetői képességek, illetve gyakorlat, valamint az informatikai tudás (beleértve a biztonságtudatosságot is) nem előfeltétele annak, hogy valaki polgármester legyen. Kutatásunk célja a fentiek alapján annak vizsgálata, hogy a magyarországi önkormányzatok vezető tisztségviselői jelenleg hogyan, mennyire tudatosan vélekednek az információbiztonságról.

2. ANYAG ÉS MÓDSZER

A KSH aktuális adatai alapján (Waffenschmidt, 2016) Magyarországon összesen 3155 település található a következők szerint: 1 főváros, 23 megyei jogú város, 322 város, 126 nagyközség és 2683 község. A települési önkormányzatok száma összesen 3178, melyből önálló polgármesteri hivatalt 545 település tart fenn, beleértve Budapestet, amelyhez 1 főpolgármesteri és 23 polgármesteri hivatal tartozik. Kutatásunkba azokat a polgármesteri hivatalokat vontuk be, amelyek szerepelnek az *Önkormányzati Tudástár – Önkormányzati Címtár 2015* című kiadványban, s az adatbázisban a hivatal, a polgármester és a jegyző e-mail-elérhetőségei közül legalább az egyik meg volt adva. Kutatásunkban két területet vizsgáltunk, a közszolgálati etikát és az információbiztonságot, s arra voltunk kíváncsiak, hogy mi a véleménye az önkormányzatok vezető tisztségviselőinek, a képviselő-testület tagjainak és az információbiztonságban érintett szakembereinek az etikáról és az információbiztonságról – jelen tanulmányunkban csak ez utóbbival foglalkozunk. Felkérő

levelünket 2016. június közepén küldtük ki a tárhelyünk terhelhetőségének figyelembevételével szakaszosan (naponta rendszerint egy vagy két megye polgármesteri hivatalának, polgármesterének, illetve jegyzőjének). A Limesurvey alkalmazással készített kérdőívünket a kutatasmodszertan.hu oldalon tettük elérhetővé, kitöltési határideje 2016. július 6-a volt. A címzetteknek küldött felkérő levelünkben lehetővé tettük, hogy javaslataikat, megjegyzéseiket, észrevételeiket, illetve kérdéseiket az adatkezelési elveinkkel kapcsolatban egy erre a célra létrehozott e-mail-címen is megtegyék. Biztosítottuk őket, hogy e-mail-címük a kutatás lezárását követően automatikusan törlődik minden időlegesen létrehozott adatbázisból (pl. levélküldő alkalmazás adatbázisa), s válaszaik anonimek lesznek a feldolgozás során, így semmilyen személyes adatot nem tudtunk és nem is akartunk a címzettek vagy kollégáik konkrét személyére visszavezetni.

A beérkezett válaszokat a Limesurvey alkalmazásból az IBM SPSS Statistics statisztikai programba exportáltuk, s az adatok statisztikai feldolgozását is ezzel a szoftverrel végeztük el.

Az adatok elemzése során abból a feltételezésünkből indultunk ki, hogy lesznek olyan kérdések, amelyekre a válaszadók – bár lehetőségük lenne – nem feltétlenül akarnak válaszolni. Ezért minden olyan kérdőívet bevontunk a vizsgálódásunkba, amelyik – ha nem is teljes egészében, de – használható adatokkal szolgált az elemzéshez. Ezért fordul elő eredményeink bemutatásakor, hogy rendszerint nem abszolút, hanem a könnyebb érthetőség miatt relatív gyakoriságokat adtunk meg.

A fent leírtak alapján összesen 397 darab kérdőívet dolgoztunk fel, ebből 334 tartalmazta a város/község településkategóriába való besoroláshoz szükséges választ. Az 1. táblázat a minta településkategóriák szerinti megoszlását mutatja Magyarország településszerkezetéhez viszonyítva. Bár a minta nem tekinthető reprezentatívnak a településszerkezet alapján, hiszen a városok felülreprezentáltak, ez nem veszélyezteti a községi és városi önkormányzatok vezető tisztségviselőinek információbiztonság-tudatossága összehasonlítására irányuló vizsgálatok eredményeit.

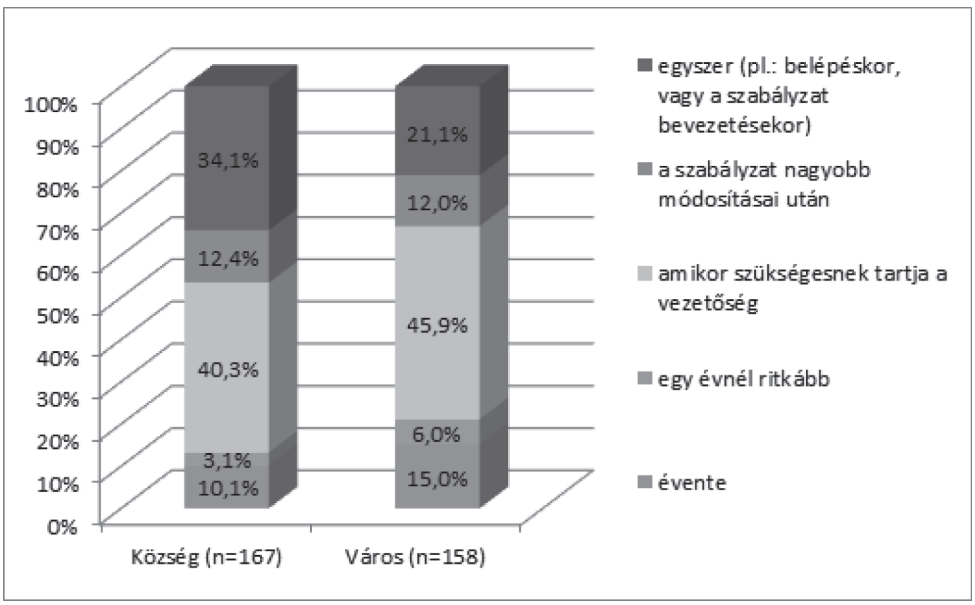
1. táblázat • *A minta településkategóriák szerinti megoszlása Magyarország településszerkezetéhez viszonyítva (Forrás: [1]KSH: Magyarország településhálózata [2016], [2]saját kutatás [2016])*

Településkategória	Magyarország[1]		Minta[2]	
	db	%	db	%
Város	346	10,97	163	48,80
Község	2809	89,03	171	51,20
Összesen	3155	100,00	334	100,00

A kérdőív kérdéseire adott válaszokat két lépésben elemeztük. Az első lépésben a gyakorisági eloszlásokat vizsgáltuk, a második lépésben pedig a mélyebb összefüggések feltárásával, a hipotézisek ellenőrzésével foglalkoztunk. Tanulmányunkban is ezt a felépítést követve előbb a fontosabb kérdésekre adott válaszokat mutatjuk be.

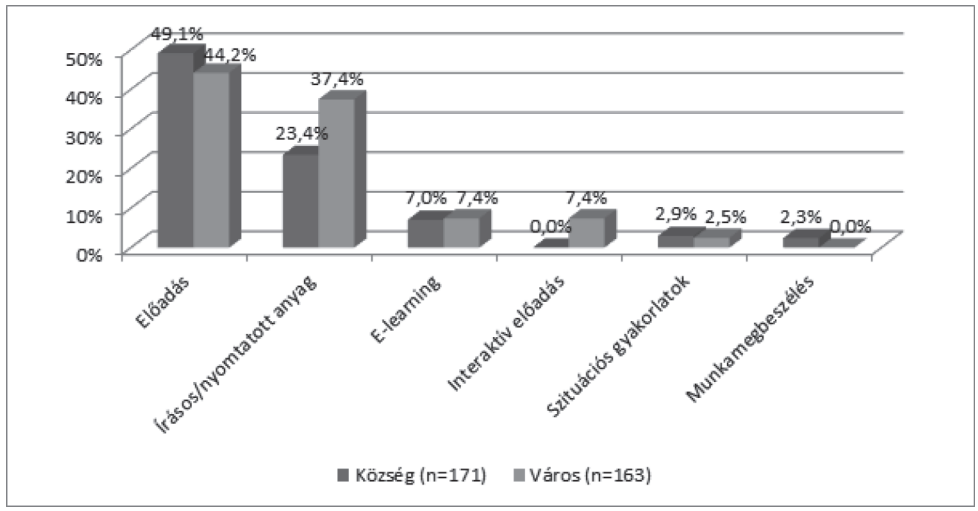
3. AZ INFORMÁCIÓBIZTONSÁGGAL KAPCSOLATOS KÉRDÉSEK GYAKORISÁGI VIZSGÁLATA

Az önkormányzatoknál leggyakrabban akkor tartanak az információbiztonsággal és az adatvédelemmel kapcsolatos képzéseket (1. ábra), amikor a vezetőség szükségesnek tartja, illetve egyszer, amikor az adott munkavállaló belép az önkormányzathoz, vagy az információbiztonsággal kapcsolatos szabályzatok bevezetésekor. Ezeket az évente, illetve a szabályzat nagyobb módosításaikor tartott képzések, valamint az egy évnél ritkábban megtartott képzések követik. A községi önkormányzatok a városi önkormányzatokhoz képest kisebb arányban évente és nagyobb arányban egyszer tartanak ilyen oktatást. A válaszok alapján az információbiztonsággal kapcsolatos oktatások gyakoriságát alapvetően elfogadhatónak ítéljük meg, hiszen országos átlagban a településtípustól függetlenül a válaszadók több mint kétharmada a környezeti változásokra reagálva, illetve legalább a munkavállalói munkaviszony megkezdésekor erősíti a dolgozók információbiztonság-tudatosságát.



1. ábra • *Az információ- és adatbiztonsággal kapcsolatos oktatások gyakorisága a községi és városi önkormányzatoknál (az önkormányzatok számának %-os megoszlása)*

A biztonságtudatosság fejlesztésének gyakoribb, akár egymással közösen is alkalmazható képzési formáit a 2. ábra szemlélteti.



2. ábra • *Az információbiztonsággal és adatvédelemmel kapcsolatos oktatási formák alkalmazása a községi és városi önkormányzatoknál (többfeleletes kérdés, az önkormányzatok %-a)*

A leggyakoribb, egymással együtt futó képzési lehetőség mind a városi, mind a községi önkormányzatoknál az előadás, illetve az írásos/nyomtatott (tan)anyag. Ez utóbbinál – az önkormányzatoknál szerzett személyes tapasztalatunk alapján – egy rendszerint a törvényből kimásolt, nem vagy csak kevés magyarázattal ellátott anyagot kapnak a munkavállalók azzal a megjegyzéssel, hogy olvassák el, majd írják alá ennek tényét egy erre a célra rendszeresített formanyomtatványon. Az így aláírt nyilatkozatok bekerülnek a dolgozók személyügyi aktáiba a dolgozó nevére kiírt informatikai eszközök nyomtatványa, a végzettségek másolatai és egyéb dokumentumok mellé, de a gyakorlatban sajnos nem tud realizálódni az információbiztonság-tudatos attitűd erősödése. Sajnos az előadásokról sem tudunk optimista képet bemutatni, mivel vagy az önkormányzat saját rendszergazdája, munkavédelmi felelőse, vagy kisebb önkormányzatoknál a jegyző vagy a polgármester ad tájékoztatást a dolgozóknak a biztonságos munkavégzésről, s ennek része (ha egyáltalán megemlítik) az információbiztonság. Hatékonyság szempontjából a legjobb módszernek az interaktív előadást, illetve a kiscsoportos esettanulmányokat és szituációs gyakorlatokat tartjuk, de sem kérdőívünk szabad válaszadásos részében, sem a saját tapasztalatunk alapján nem tudunk olyan esetről beszámolni, amikor a szituációs gyakorlatok az üzleti életben egyre gyakrabban jelen lévő információbiztonsági gyakorlati audittal (pl. social engineeringgel) is kiegészültek volna.

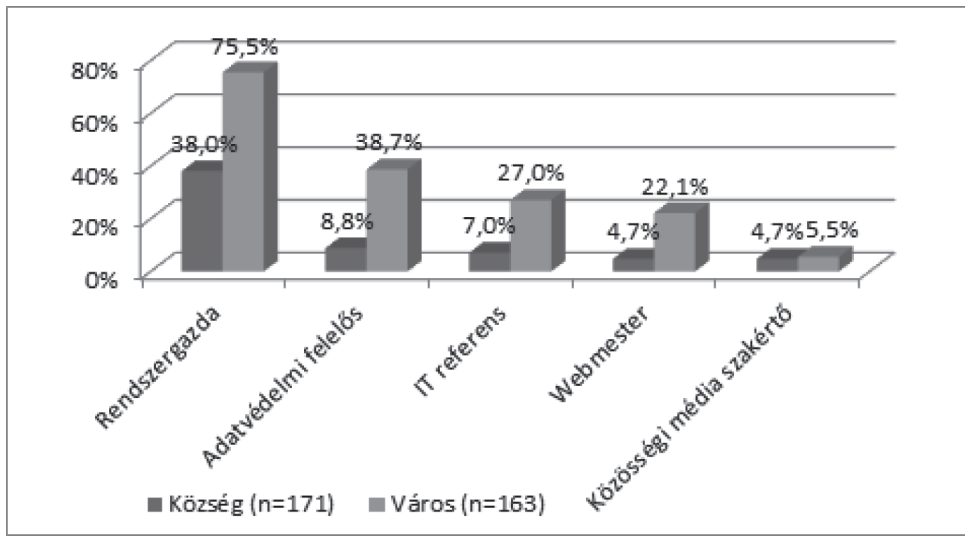
Részben a törvényi előírásoknak is köszönhető, hogy a felmérésben képviselt önkormányzatok közül minden második elkészítette az adatvédelmi és adatbiztonsági szabályzatot, harmaduknál pedig megtalálható a titoktartási nyilatkozat, az információbiztonsági szabályzat, az informatikai biztonsági szabályzat, az adminisztrátorok és a hozzáférési

jogosultságot engedélyező személyek listája (nyilvántartás), illetve a személyes és közérdekű adatok adatszolgáltatási nyilvántartása. Az önkormányzatok életében is megjelenő munkavégzéssel kapcsolatos változások (pl. a hordozható számítástechnikai eszközök megjelenése, s ezzel párhuzamosan az irodán kívül is végzett munkatevékenység) miatt úgy gondoljuk, hogy szükséges lenne a jelenleginél lényegesen nagyobb arányban elkészíteni az informatikai eszközök átadás/átvétele lapokat (15,5% községi vs 47,7% városi), az adathordozók és a számítógépek selejtezésére vonatkozó szabályzatokat (18,1% községi vs 29,7% városi), a szoftver- és hardvernyilvántartó lapokat (10,3% községi vs 33,5% városi), a felhasználói hozzáférések kiosztására/megszüntetésére/módosítására vonatkozó lapokat (3,2% községi vs 33,5% városi). További információbiztonsági kockázatot jelent az is, hogy csak minden nyolcadik önkormányzatnál vezettek be olyan nyomtatványt, amelyik az önkormányzat tulajdonában levő eszközök szállítására/tárolására vonatkozik. Az üzleti életben gyakori, hogy a kilépő munkavállaló a munkaviszony megszüntetésének a pillanatában már nem tud hozzáférni a szervezet informatikai erőforrásaihoz (az eszközöket le kell adnia, a jelszavait megváltoztatják, a hozzáférési jogosultságait megvonják). Az önkormányzatoknál csak néhány említésben szerepelt a kilépő dolgozó informatikai nyilatkozata, aminek az a célja, hogy a hozzáférések és engedélyek megszüntetése mellett a munkavállaló büntetőjogi felelőssége tudatában nyilatkozik a tudomására jutott, az önkormányzatok működésével összefüggő titkos és bizalmas adatok és információk további kezeléséről (pl. ha az adatok a privát számítógépén vannak, akkor azokat végérvényesen letörli).

Több részkérdésen keresztül vizsgáltuk azt, hogy az önkormányzatok a feladataik ellátására milyen szoftvereket, alkalmazásokat, adatbázisokat használnak. Meglehetősen heterogén képet kaptunk. Az általános használatnál a leggyakoribb említéssel az E-iktat, a Microsoft Office, illetve az Adobe Reader szerepelt, de a válaszok között megtalálható volt az ASZA, a KCR, az ÁNYT, az ÁNYK, a Takarnet, a MÜKENG, a DOQUIS, a Poszeidon, a TERKA, az OptiJUS. Az ezt követő kérdésnél a használt szoftverek és alkalmazások körét leszűkítettük az irodai alkalmazásokra (pl. e-mail, webböngésző, szövegszerkesztő). Itt is a Microsoft termékei domináltak, úgymint a Word, az Excel, a PowerPoint. Sokkal kisebb arányban szerepelt a válaszokban a szabadon használható LibreOffice. Az e-mail használata természetes az önkormányzatoknál, de a többség nem nevezett meg konkrét alkalmazást (elvétve találkoztunk a Zimbra, a Thunderbird, a Windows Live Mail és az Outlook nevével). A webböngészőknél a válaszadók a gyakoribb böngészők nevét adták meg, úgymint Firefox, Chrome, Internet Explorer. Meglepő volt a számunkra, hogy a Windows 10-nél megjelenő Edge böngészőt senki nem nevezte meg, s általánosságban a Windows XP-t említették. Az önkormányzatoknál a többség a KIRA rendszert használja a munkaügy területén, illetve néhány válaszadó a saját munkaügyi rendszerét részesíti előnyben, vagy azt sem tudja, hogy milyen szoftvert/alkalmazást használnak. A szociális igazgatásban a kérdőív válaszadói a leggyakrabban a PTR-t, a Win-mankót, a KENYSZI-t, a Winszoc-t használják. A műszaki igazgatásban a leggyakoribb említés a Takarnet volt, a pénzügyi területen pedig az EPER, az Önkadó, a Forrás-SQL/KGR és a CGR volt. Az adatbázisok közül a válaszadók többnyire az ÁNYK-t, az E-adatot, a Govsyst, az IQtatót

nevezték meg, de a többség inkább csak adatbázis-területeket adott meg: népesség-nyilvántartó rendszert, térinformatikai rendszert, települési képviselők adatbázisát.

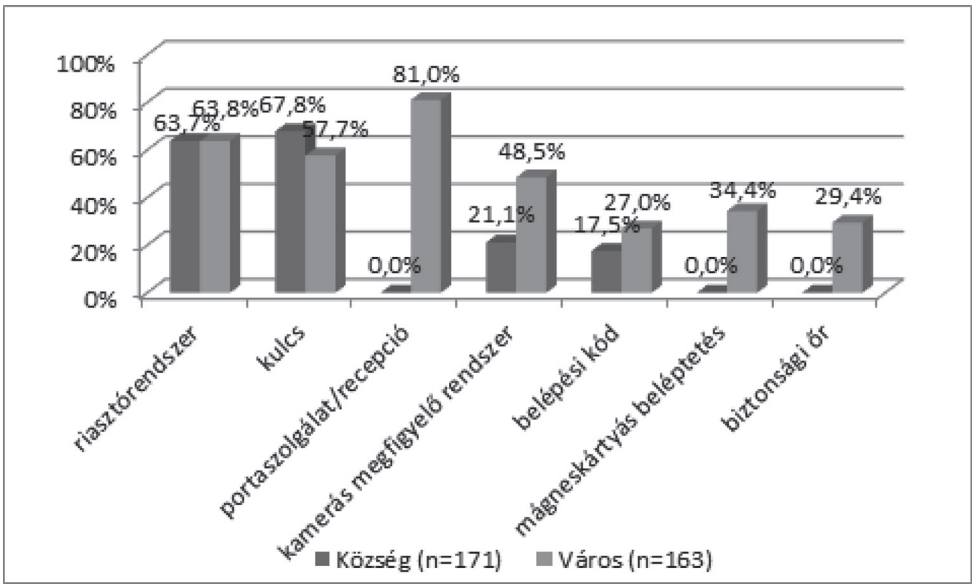
Kérdőívünkben azt is megkérdeztük, hogy az informatikával kapcsolatban milyen konkrét munkakörök vannak (3. ábra).



3. ábra • *Az informatikával összefüggő munkakörök betöltése a községi és városi önkormányzatoknál (többfeleletes kérdés, az önkormányzatok %-a)*

A 3. ábrán látható, hogy a leggyakoribb előfordulás a rendszergazda, majd az adatvédelmi felelős. A webmester és a közösségi média szakértő (elsősorban Facebook és YouTube oldalak/csatornák gondozása) inkább csak a nagyobb településeken található meg. Ennek okait többek között abban látjuk, hogy a városokhoz képest lényegesen kisebb költségvetési keretből gazdálkodó községi önkormányzatoknál ha lenne is igény az informatikával és adatvédelemmel, illetve az online kommunikációval kapcsolatos feladatok elvégzésére, a keret nincs meg rá, hogy külön-külön szakembert alkalmazzanak. Megállapítható továbbá, hogy valamennyi informatikával összefüggő munkakör sokkal nagyobb arányban jelenik meg a városi önkormányzatoknál, mint a községinél.

Az adatok és az információk komplex védelmének egyik területe a fizikai biztonság. Kérdőívünknek ebben a kérdésében arra kerestük a választ, hogy az önkormányzatok fizikai védelme milyen módon valósul meg (4. ábra).



4. ábra • *Az önkormányzatok fizikai védelme a községi és városi önkormányzatoknál (többfeleletes kérdés, az önkormányzatok %-a)*

A kérdés elemzése során megállapítható, hogy általánosságban a riasztórendszer, a kulcs, illetve a portaszolgálat/recepció jellemzi az önkormányzatok fizikai védelmét. A riasztórendszer közel azonos arányban található meg a községeknél és a városoknál, s a kulcsok használatánál sem látható markáns különbség. A többi fizikai védelem kivétel nélkül a városokban gyakoribb. A vizsgált mintában csak a városi önkormányzatoknál találunk portaszolgálatot, mágneskártyás beléptetést, illetve biztonsági őrt.

Kérdéseink következő nagy csoportja a válaszadó személy információbiztonságával és adatvédelmével kapcsolatos véleményét, attitűdjét vizsgálta. A válaszok közlése előtt megjegyezzük, hogy a válaszadó önkormányzati vezető tisztségviselők többsége 40 év feletti volt (74,7% községi vs 62,4% városi), az életkori átlaguk pedig 47,8 év a községi, illetve 45,4 év a városi önkormányzatok esetében. Nemi arányuk közelítőleg azonos, a községi önkormányzatok vezető tisztségviselői 70,8%-ának van főiskolai vagy egyetemi végzettsége, a városi önkormányzatoknál ez az arány 95,4%.

A vezető tisztségviselők munkahelyi számítógépén 87,2%-os (község) vs 87,9%-os (város) arányban található vírusirtó. Esetünkben ez két dolgot jelenthet:

1. a fennmaradó számítógépek ki vannak téve a hackerek és vírusok támadásának,
2. nem minden vezető van tudatában annak, hogy a gépe a vírusok ellen védve van.

Csak minden második tisztségviselő gépét védi jelszó a belépéskor. Ez azt jelenti, hogy az önkormányzatok ellen indított social engineering akciók a vállalati támadásokhoz képest

arányait tekintve sokkal nagyobb mértékben tudnak/tudnának realizálódni. Ez véleményünk szerint hatalmas biztonsági kockázatot jelent nem csak a helyi önkormányzatoknak, hanem a hálózatba kötött önkormányzati számítógépeken keresztül a kormányzati informatikai infrastruktúrának is. A községi önkormányzatok vezető tisztségviselői 41,3%-ának, a városiakéi pedig 51,3%-ának a munkára (is) használt egyéb eszközein (pl. tablet, otthoni számítógép) van vírusvédelme. Itt is a pesszimista forgatókönyv szerint értelmezzük a választ: még nagyobb esélye van a vezetők laptopján, tabletjén, otthoni számítógépén lévő önkormányzati adatokhoz hozzáférni a támadónak, illetve az említett eszközökön keresztül még nagyobb eséllyel lehet megtámadni a kormányzati informatikai infrastruktúrát. A pesszimista forgatókönyvet erősítik meg a következő állításunkra kapott válaszok: az önkormányzati vezetők munkára (is) használt egyéb eszközeinek a községi önkormányzatoknál 22,0%-át, a városiaknál 41,0%-át védi belépéskor jelszavas vagy egyéb megoldás. A községi válaszadók 28%-ára vs a városiak egyharmadára jellemző, hogy az önkormányzat által adott és/vagy munkára használt okostelefonon van jelszavas, vagy egyéb védelem. Az üzleti élet (felső)vezetőinek információbiztonság-tudatossága kapcsán viszonylag kevés szó esik arról, hogy a többségük a hatékonyság és a gyorsaság érdekében (mondván, a készülék úgyis állandóan a kezében van) nem használja, illetve tudatosan kikapcsolja az okostelefonok jelszavas, illetve képernyővédelmét. Ez az arány a községi önkormányzati vezetők körében 94,9%, a városiaknál pedig 71,8%. Tehát ha az önkormányzat vezetőinek a sérelmére követnek el telefonlopást, akkor az elkövető szinte biztos lehet abban, hogy a telefonon lévő adatok komolyabb informatikai tudás hiányában is megszerezhetők.

A megkérdezett vezetők az önkormányzati munkájukhoz kapcsolódó adatokat, információkat, dokumentumokat rendszerint az önkormányzati számítógépen, laptopon tárolják (80,6% község vs 77,9% város), ezt követi gyakoriságban az önkormányzat szervere, illetve zárt felhője (24,0% község vs 74,4% város), majd a saját számítógép/laptop (20,5% község vs 18,7% város). Bár a válaszadók úgy nyilatkoztak, hogy a telefonon szinte alig tárolnak ilyen adatokat, arra vélhetőleg kevesen gondoltak, hogy pl. egy polgármester vagy egy jegyző telefonos névregisztere mekkora értéket jelenthet azoknak a hackereknek, social engineereknek, akik a társadalmi hálóra épülő támadási módszereket részesítik előnyben. A CD-n/DVD-n tárolt adatok gyakorlatilag elenyészőben vannak (15,4% község vs 2,6% város), ugyanakkor csak bízni lehet abban, hogy nem a publikus felhő ismeretlensége, hanem a tudatos döntés eredménye az, hogy a nyilvános felhő által nyújtott szolgáltatásokkal csak a városi önkormányzatok vezető tisztségviselőinek 4,6%-a él az önkormányzati adatok, információk, dokumentumok tárolása során. A községi önkormányzatoknál nem jellemző a nyilvános felhő használata.

A községi válaszadók 56,3%-a vs a városiak kétharmada használja a közösségi médiát, azon belül is elsősorban a Facebookot és a Youtube-ot, a Linkedin használata elenyészőnek tekinthető. A kapott arány alapján nagymértékű hasonlóságról beszélhetünk a közösségi média használati szokásait tekintve a diplomás, negyvenévesnél idősebb felhasználók körében. Akik aktívan tevékenykednek a közösségi médiában, azoknál a leggyakoribb tevékenységek a következők: lájkolás (27,7% község vs 26,6% város), az önkormányzattal kapcsolatos információk megosztása (22,9% község vs 29,1% város), mások által írt/megosztott

tartalmak megosztása (25,1% község vs 21,4% város), a válaszadóval kapcsolatos információk megosztása (18,3% község vs 23,7% város), a válaszadó családjával kapcsolatos információk megosztása (12,8% község vs 18,1% város), valamint 12,6%-uk a község, illetve 16,8%-uk a város esetében más posztjaihoz, megosztásaihoz fűz megjegyzést.

Egy korábbi kérdésünkben az önkormányzati munkához kapcsolódó adatok, információk, dokumentumok tárolásáról érdeklődtünk (lásd fentebb), s a községi megkérdezettek 12,8%-a a városiak 19,1%-ával szemben azt válaszolta, hogy ezeket az anyagokat pendrive-on, valamint 15,4%-uk a községi, illetve 2,6%-uk a városi önkormányzatoknál CD-n/DVD-n is tárolja. A községi önkormányzatok tisztségviselőinek 23,1%-a, míg a városiakéinak 41,0%-a kapott már idegen forrásból hordozható adattárolót. A kérdőívben nem kérdeztünk rá külön arra, hogy kitől kapta az adattárolót, de azt meglepőnek tartjuk, hogy senki nem jelöltbe be azt a válaszlehetőséget, hogy „megtekintés nélkül kidobtam". A kíváncsiság tehát itt is legyőzte a biztonságot, 7,7%-uk a községi, illetve 15,4%-uk a városi önkormányzatoknál azonnal betette a számítógépébe, míg további 7,7%-uk (a városi és községi önkormányzatoknál egyaránt) ugyan gyanakvó volt, de miután elolvasta a CD-hez, pendrive-hoz mellékelt leírást, betette az adathordozót a számítógépébe.

4. HIPOTÉZISEK

Tanulmányunkban a kutatási eredményeinket a községi és a városi önkormányzati vezetők információbiztonságról alkotott válaszai alapján négy hipotézis köré rendeztük, úgymint:

1. A városi és a községi önkormányzatok között jelentős különbségek állnak fenn az információvédelemmel kapcsolatos szabályozási gyakorlatban.
2. A városi és a községi önkormányzatok információvédelmi infrastruktúrája eltérő.
3. A városi és a községi önkormányzatok tisztségviselőinek eltérő információbiztonság-tudatosságuk van.

Hipotéziseink ellenőrzéséhez a statisztikai módszerek közül a khi-négyzet próbát választottuk.

5. AZ EMPIRIKUS KUTATÁS EREDMÉNYEI

A városi és a községi önkormányzatok között jelentős különbségek állnak fenn az információvédelemmel kapcsolatos szabályozási gyakorlatban. A khi-négyzet próba eredménye ($p = 0{,}003$) statisztikailag igazolja, hogy a városi önkormányzatok a községi önkormányzatokhoz képest jelentősen nagyobb arányban rendelkeznek az adatvédelmi és adatbiztonsági szabályzattal. A minta esetében a városi önkormányzatok 71,6%-a rendelkezett az adatvédelmi és adatbiztonsági szabályzattal, míg a községi önkormányzatoknál ez az arány csak 55,5%.

A khi-négyzet próba eredménye ($p = 0{,}029$) alapján statisztikailag igazolható, hogy a városi önkormányzatok a községi önkormányzatokhoz képest jelentősen nagyobb

arányban rendelkeznek az információbiztonsági szabályzattal. A minta esetében a városi önkormányzatok 48,4%-a rendelkezett az információbiztonsági szabályzattal, míg a községi önkormányzatoknál ez az arány csak 36,1%.

A khi-négyzet próba eredménye ($p < 0,01$) alapján megállapítható, hogy a városi önkormányzatok a községi önkormányzatokhoz képest jelentősen nagyobb arányban rendelkeznek az informatikai biztonsági szabályzattal. A minta esetében a városi önkormányzatok 51,3%-a rendelkezett az informatikai biztonsági szabályzattal, míg a községi önkormányzatoknál ez az arány csak 25,8%. Az első hipotézisünket elfogadottnak tekintjük.

A városi és a községi önkormányzatok információvédelmi infrastruktúrája eltérő. A khi-négyzet próba eredménye ($p < 0,01$) igazolja, hogy a városi önkormányzatok jelentősen nagyobb arányban rendelkeznek adatvédelmi felelőssel. A minta esetében a városi önkormányzatok 40,6%-a rendelkezett adatvédelmi felelőssel, míg a községi önkormányzatoknál ez az arány csak 9,7%. A második hipotézisünket elfogadottnak tekintjük.

A városi és a községi önkormányzatok tisztségviselőinek eltérő információbiztonság-tudatosságuk van. Az alábbi – információbiztonság-tudatosság mérésére használható – kérdésekre adott válaszokban vizsgáltuk az esetleges eltéréseket a városi és a községi önkormányzatok tisztségviselői között:

- az önkormányzat által adott és/vagy munkára használt okostelefonon van jelszavas vagy egyéb védelem: nem állapítható meg jelentős eltérés ($p = 0,284$);
- az önkormányzat által adott és/vagy munkára használt okostelefonon van jelszavas vagy egyéb képernyővédő: jelentős eltérés ($p < 0,001$) állapítható meg, a minta esetében a városi önkormányzatok tisztségviselőinek 28,4%-a használta a képernyővédőt, míg a községi önkormányzatoknál ez az arány csak 5,5%;
- az önkormányzat által adott és/vagy munkára használt okostelefonon van vírusirtó: nem állapítható meg jelentős eltérés ($p = 0,052$);
- a munkára (is) használt egyéb eszközeimen (pl. tablet, otthoni számítógép) belépéskor van jelszavas vagy egyéb védelem: jelentős eltérés ($p = 0,001$) állapítható meg, a minta esetében a városi önkormányzatok tisztségviselőinek 43,2%-a használta a jelszavas vagy egyéb védelmet, míg a községi önkormányzatoknál ez az arány csak 24,5%.

A harmadik hipotézisünket részben elfogadottnak tekintjük.

6. AZ EREDMÉNYEK ÉRTÉKELÉSE

Kutatásunk egyik legnagyobb eredményének azt tekintjük, hogy lehetőségünk volt egy országos, online kutatás révén felmérni az önkormányzatok vezető tisztségviselőinek információbiztonsággal kapcsolatos véleményét egy olyan magyarországi kutatási környezetben, ahol tudomásunk szerint az utóbbi időben ilyen nagy mintán senki nem vizsgálta a témát.

Eredménynek tekintjük, hogy a kérdőív nagy terjedelme ellenére is összességében 397 darab kérdőívet tudtunk feldolgozni, igaz, minden olyan kérdőívet feldolgozásra alkalmasnak ítéltünk meg, amelyiknél érdemi válaszokat is adtak a megkérdezettek.

A válaszok gyakorisági elemzése során egy átfogó képet rajzoltunk meg a magyarországi önkormányzatok vezető tisztségviselőinek információbiztonság-tudatosságáról, beazonosítottuk azokat a fontosabb veszélyforrásokat, amelyek egyrészt a (lokális) informatikai rendszerek használatából, másrészt a nem kellő információbiztonsági felkészültségből erednek. Rámutattunk arra is, hogy a helyi szinten jelen lévő informatikai és információbiztonsági kockázatok komoly veszélyt jelenthetnek a kormányzati informatikai infrastruktúra vonatkozásában is.

A kapott adatok robusztussága lehetővé tette a számunkra, hogy számos dimenzió mentén vizsgálódjunk. Jelen tanulmányunk hipotézisfókusza elsősorban a város-község párhuzamba állításához kötődött, s jelentős különbségeket tudtunk igazolni a statisztikai vizsgálatok során.

7. KÖVETKEZTETÉSEK

Ahogy az üzleti életben a fenntarthatóság és a biztonságos működés már elképzelhetetlen a megfelelő információbiztonság, illetve biztonságtudatosság nélkül, úgy ez az elvárás – összhangban a kormány 2014–2020 közötti időszakra vonatkozó Közigazgatás- és Közszolgáltatás-fejlesztési Stratégiájának céljaival – szintén egyre nagyobb hangsúlyt kap a helyi közigazgatás területén, az önkormányzatoknál. A Nemzeti Közszolgálati Egyetem tudományos potenciálja (akár együttműködésben az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának felkészült oktatóival) lehetővé teszi a tartalmában megfelelő és korszerű tananyagok kidolgozását, illetve tanítását valamennyi önkormányzati vezető tisztségviselő számára. Ez ugyan kellő alapot jelent valamennyi, oktatásban részt vevő vezető számára, ami révén a biztonságot fókuszba helyezve biztonságtudatosabban tudnak példát mutatni az informatikai eszközök, alkalmazások, adatbázisok használata területén, de a folyamatos technikai/technológiai fejlődés megkívánja, hogy

1. megismerkedjenek az információbiztonsággal és adatvédelemmel kapcsolatos támadásokkal és az ellenük fejlesztett védelmi módszerekkel (nem programozói szinten), illetve
2. megfelelő szinten tartsák információbiztonság-tudatosságukat, illetve biztonságfókuszukat.

A hagyományosnak tekinthető képzési formák, mint pl. a tantermi oktatás mellett, célszerű több – az üzleti életben már sikeresen alkalmazott – módszert (szakmai szolgáltatást) is igénybe venni, értve ezalatt az önkormányzati vezetők információbiztonság-tudatosság coacholását a kiterjesztett PDCA-modell alapján, vagy olyan tanácsadói/szakértői segítség felajánlását, ahol a helyi viszonyok, korlátok és lehetőségek ismeretében nem általános, hanem konkrét és egyedi projektek, javaslatok, megoldások születhetnek.

Három igazolt hipotézisünk alapján az a következtetés vonható le, hogy komoly hátrányban vannak a kisebb önkormányzatok (községek) a nagyobb, városi önkormányzatokhoz képest. Esetükben indokolt lehet olyan kormányzati támogatási programok kidolgozása és megvalósítása, amelyek segítenek csökkenteni, mérsékelni ezt a hátrányt.

Az empirikus kutatásunk kiterjesztését tervezzük a regionális dimenzióra: a magyarországi nagy régiók között is vizsgáljuk az esetleges eltéréseket az önkormányzati tisztségviselők információbiztonság-tudatosságában.

FELHASZNÁLT IRODALOM

1. Almásy Gyula et al: *Közigazgatási alapvizsga,* Dialóg Campus Kiadó, Budapest, 2016, 240.
2. Balás Endre – Schmidt Anikó – Szmetana György et al.: *Polgármesterek és jegyzők jó gyakorlat kézikönyve – korszerű településmenedzsment és igazgatás,* Menedzser Praxis, Budapest, 2015.
3. Bodó Attila Pál: *Jogi és közigazgatási ismeretek,* Nemzeti Közszolgálati Egyetem, Budapest, 2014, 74.
4. Budai Balázs Benjámin – Szakolyi András: *Interaktív önkormányzat,* Magyar Mediprint Szakkiadó, Budapest, 2005, 208.
5. Budai Balázs Benjámin: *Az e-közigazgatás elmélete,* Akadémiai Kiadó, Budapest, 2013, 474.
6. Győrffi Dezső – Győrffi György – Fülöp Judit – Farkas Sándor – Printz János: *Az önkormányzatok pénzügyei,* Perfekt, Budapest, 2011, 424.
7. Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia – 2014–2020.
8. Önkormányzati Tudástár – Önkormányzati Címtár 2015. Forrás: hirlevel.egov.hu/2015/06/27/megjelent-az-onkormanyzati-tudastar-onkormanyzati-cimtar-2015/ (A letöltés időpontja: 2016. május 2.)
9. Szerk. Pócsi Anikó: *Ügykezelői alapvizsga,* Dialóg Campus Kiadó, Budapest, 2016, 223.
10. Serényi Péter: *Dr. Gémesi György Amiben hiszel, az van,* Gödöllő Városáért Alapítvány, Gödöllő, 2015, 191.
11. Simon Barbara – Budai Balázs: *Elektronikus-közigazgatási modernizáció,* NKE, Budapest, 2015, 132.
12. Számadó Róza: *Inkluzív önkormányzat,* NKE, Budapest, 2015, 145.
13. Szita Károly: *Egy kaposvári,* Kaposvár Polgáraiért Egyesület, Kaposvár, 2015, 236.
14. Tapa Barnabás – Hegedűs Tamás: *Titkos ügykezelői ismeretek,* NKE, Budapest, 2014, 130.
15. Szerk. Varga Árpád: *Központi és önkormányzati költségvetési szervek számviteli politikája, számlarendje,* Saldo Pénzügyi Tanácsadó és Informatikai Zrt., Budapest, 2010, 487.
16. Varga Katalin – Gergely János: *Polgármesterek könyve,* Pénzügyi Tájékoztató Iroda, Budapest, 2005, 280.
17. Szerk. Waffenschmidt Jánosné: *Magyarország közigazgatási helynévkönyve,* KSH, Budapest, 2016.

Jogszabályok

1989. évi XXXIV. törvény az országgyűlési képviselők választásáról

2010. évi L. törvény a helyi önkormányzati képviselők és polgármesterek választásáról

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

2013. évi XXXVI. törvény a választási eljárásról

Dr. Kollár Csaba (kollar.csaba@uni-nke.hu) kommunikációtechnikai mérnök, okleveles kommunikációs szakember, a közgazdaság-tudomány doktora (PhD), tanácsadó, coach, mediátor. A Szent István Egyetem Gazdaság- és Társadalomtudományi Kar Vezetéstudományi Tanszék, illetve a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola oktatója, az Igazságügyi Minisztérium regisztrált közvetítője (mediátora), országos szakmai vizsgaelnök, a PREMA Consulting vezető tanácsadója, mediátora, coacha. Kutatási területe a digitális kor társadalmi vetületei és gazdasági hatásai, kiemelten az információbiztonság humán aspektusa és az információbiztonság-tudatosság fejlesztése.

Dr. Vinogradov Szergej (vinogradov.szergej@gtk.szie.hu) a gazdálkodás- és szervezéstudományok doktora (PhD), a Szent István Egyetem Gazdaság- és Társadalomtudományi Kar Közgazdaságtudományi, Jogi és Módszertani Intézetének tanszékvezető docense. Kutatási területe a statisztikai módszerek és alkalmazásuk a gazdasági és társadalmi elemzésekben, különös tekintettel a területi egyenlőtlenségek vizsgálatára.