Nagyné Takács Veronika – Kovács László

AZ INFORMÁCIÓBIZTONSÁGI VEZETŐ SZAKIRÁNYÚ TOVÁBBKÉPZÉS TAPASZTALATAI

Az információ biztonsága napjaink egyik legfontosabb tényezője. Ennek megteremtése a közigazgatásban is kiemelt feladat. Ugyanakkor az információbiztonság megvalósítása és folyamatos fenntartása nem csak technikai kérdés. Ennek megfelelően az információért felelős közigazgatási vezetőktől kezdődően az információt kezelőkig a folyamatos oktatás és felkészítés ezen a területen is elengedhetetlen. A Nemzeti Közszolgálati Egyetemen 2014-ben indultak azok a képzések, amelyeket az információbiztonsági törvény a hatálya alá tartozó szervezetek esetében az elektronikus információs rendszer biztonságáért felelős személyek számára kötelezően előír. A képzéssel kapcsolatos tapasztalatok összegzését kiegészítheti az egyik végzett évfolyam nyilvános szakdolgozatainak értékelése, visszajelzést adva a képzést szervező és a jogalkotó számára is. Jelen dolgozat a 2015-ben készült és hozzáférhető, nyílt szakdolgozatok elemzésére épít.

Kulcsszavak:
információbiztonság, oktatás, képzés, Nemzeti Közszolgálati Egyetem – information security, education, training, National University of Public Service

1. BEVEZETÉS

Ma az élet minden területén számítógépek segítségével gyűjtjük, dolgozzuk fel és használjuk a mind nélkülözhetetlenebbé vált információinkat. Társadalmunk minden szegmensét áthatja az az igény, hogy az információ biztonsága azt az elvárt mértéket képviselje, amely alapján valóban kiegyensúlyozottan működik minden társadalmi funkciónk és ezek minden egyes folyamata.

Az információbiztonságra ma már mint valódi tudományra tekinthetünk, amelynek alapja kétségtelenül maga az információtudomány. Ugyanakkor az információtudományban meglévő elveket ki kell egészítenünk a biztonság különböző tudományos igénnyel feltárt

kérdéseivel. Mivel napjainkban az információs rendszerek megfeleltethetőek számítógép-hálózatoknak és számítógéprendszereknek, ezért nagyon sokszor egyszerű technikai, ebben az esetben informatikai kérdésnek tekintjük az információbiztonságot.

Ez azonban csak részben igaz, hiszen az információ kezelésében jelen van az ember is, ami azonnal magával hozza a kérdés humán összetevőinek a vizsgálatát is. Ennek megfelelően ma az információbiztonságot alapvetően komplex megközelítésben kell alkalmazni, az-az figyelmet kell fordítani a fizikai, a humán, az adminisztratív és az elektronikus biztonsági összetevőkre egyaránt.

Mindezek a közigazgatásra hatványozottan igazak. A közigazgatásban megjelenő információk esetében az ágazat funkcióiból eredően megkérdőjelezhetetlen módon jelentkezik az információk bizalmassága és sértetlensége, valamint azok rendelkezésre állása.[1] Van azonban egy komoly probléma az információbiztonság közigazgatásban történő mérésével, mivel itt az esetek igen nagy százalékában a biztonság hiánya miatt esetlegesen bekövetkező károk nem, vagy csak nagyon nehezen – akkor is csak közvetett módon – fejezhetők ki anyagi veszteségként. Természetesen, ha például az állampolgárok bizalomvesztését mint kárt tekintjük, máris bizonyos mértékben mérhetővé válik a biztonság minősége.

Minden fejlett ország természetszerűleg ma már szabályozza az információbiztonság megteremtését és fejlesztését a stratégiai szinttől egészen a konkrét technikai vagy akár a humán összetevők szabályozásáig. Ezek az információbiztonsági szabályozók kiemelten kezelik a felkészítés és az oktatás kérdését. Így van ez hazánkban is.

Ennek megfelelően épül fel jelen írás is, amely a hazai információbiztonsági képzések közül egyet, nevezetesen az információbiztonsági vezető szakirányú továbbképzést emeli ki és vizsgálja meg, korántsem a teljesség igényével.

Jelen tanulmány mottójául a következők szolgáltak: *A tanulás célja – túl a tanulás nyújtotta gyönyörűségen – az, hogy a jövőben hasznunk legyen belőle* (Jerome Seymour Bruner amerikai pszichológus).

2. AZ INFORMÁCIÓBIZTONSÁG JELENTŐSÉGE ÉS SZABÁLYOZÁSA

Mindennapi életünket átszövik a számítógépes rendszerek. Ma nagyon nehéz elképzelni bármilyen társadalmi funkciót számítógépekre alapozott információs folyamat nélkül. Ahogy korábban utaltunk rá, ez a közigazgatás esetében sincs másképp. Természetesen az egyes szereplők nem egyformán érintettek a folyamatokban, ennek megfelelően az informatikai rendszerek biztonsága sem érint mindenkit egyforma mértékben. Az azonban ma elvitathatatlan tény, hogy az egyszerű felhasználó, vagy az egyszerű ügykezelő is fontos szereplője és aktív részese a biztonságnak. Ennek oka elsősorban az, hogy az információtechnikai és -technológiai biztonsági kérdéseket leszámítva (és még azok közül sem mindegyiket lehet a felhasználók felelősségi köréből kivonni) a felhasználó felkészültsége, képzettsége és ezzel (akár) egye-

1 Az információbiztonság szakmai terminológiájában az angolul confidentiality, integrity, availability, azaz bizalmasság, sértetlenség, rendelkezésre állás a legfontosabb alapelvek közé tartoznak. Az angol szavak kezdőbetűiből alkotott CIA elvként is ismert ez a fogalomhármas.

nes arányban álló biztonságtudatossága kulcskérdés, mert az ember az, aki a legtöbbet tudja tenni az információk biztonságának megteremtéséért.

Az információbiztonság korábban jelzett komplex megvalósítása, azaz a fizikai, adminisztratív, humán és elektronikus információbiztonság szükségessé teszi mind nemzetközi, mind nemzeti szabályozás kialakítását. Mindezen területek a nemzetközi szervezetek – pl. NATO vagy az Európai Unió –, de akár egy adott ország esetében is a kibertér biztonságának megteremtésével kezdődik, mivel az információbiztonság egyik legfontosabb dimenziója a kibertér.

A NATO a 2007-es észt incidens[2] óta kiemelt kérdésként kezeli a kibertérben zajló tevékenységeket. A NATO 2010-es lisszaboni csúcstalálkozója után a szövetség stratégiai koncepciójában szerepelteti, hogy az egyre szofisztikáltabb számítógépes támadások miatt a szövetség információs és kommunikációs rendszereinek védelme az egyik legsürgősebb feladat.[3]

Az Európai Unióban 2013 év elején jelent meg az Unió új kiberbiztonsági stratégiája, amelyet az EU külügyi és biztonságpolitikai főképviselője és az Európai Bizottság közösen dolgozott ki. Az Európai Unióban ez az első olyan átfogó stratégia kibertérre, amelyet az EU a kiberbiztonság területén megalkotott.[4] A stratégia nagyon egyértelmű célokat és prioritásokat tűz ki az EU nemzetközi kibertér-politikája terén, amelyek között a szabadság és nyitottság, a jogkövetés, a kiberbiztonsági kapacitások kiépítése, valamint a kibertérrel kapcsolatos nemzetközi együttműködés ösztönzése is megjelenik.[5] Ezt követően 2014 novemberében született meg az EU kibervédelmi politikai keretrendszere, amely már több mint 40 jól megfogalmazott akciót fogalmaz meg a kibervédelem megvalósítása és növelése érdekében.[6] Ezek közül az egyik legfontosabbnak tekinthető a kibervédelmi képzések, oktatások és gyakorlatok megvalósítását szorgalmazza.

Magyarországon a biztonsági stratégiai dokumentumokban először 2012-ben jelent meg markáns módon a kibertér, mint olyan tényező, amelyre különös figyelmet kell fordítani. A 2012-ben megjelent új Nemzeti Biztonsági Stratégiában kiemelt helyen találhatjuk a kiberkihívások jelentette veszélyeket.[7] Ez a stratégia rendkívül előremutató, hiszen államilag elfogadott, a nemzet biztonságát meghatározó stratégiai elvek először tartalmazzák e terület fontosságát és védelmének szükségességét.[8] A stratégia természetszerűleg felméri a terület veszélyforrásait: „*Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szinte mindenki számára elérhetővé vált eredményeit egyes államok, vagy nem*

2 2007 tavaszán feltehetően orosz elkövetők komoly kibertámadásokat intéztek a fejlett észt internetes infrastruktúra ellen.

3 A NATO 2010-es új stratégiai koncepciója: Aktív Szerepvállalás, Modern Védelem. Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságáról.

4 Kovács László: *Biztonságpolitika = E-közszolgálatfejlesztés: Elméleti alapok és tudományos kutatási módszerek,* szerk. Nemeslaki András, Nemzeti Közszolgálati Egyetem, Budapest, 2014, 227–248, 245. (ISBN 978-615-5491-04-7)

5 EC Cybersecurity Strategy, 2013.

6 EU Cyber Defence Policy Framework, 2014.

7 Nemzeti Biztonsági Stratégia, 2012.

8 Kovács: *i. m.,* 241.

állami – akár terrorista – csoportok arra használhatják, hogy megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatok rendeltetésszerű működését."[9]

2013 elején a Kormány elfogadta a nemzeti kiberbiztonsági stratégiát.[10] A stratégia összhangban az EU-s ágazati stratégiával, az oktatás és képzés kérdését szintén kiemelt helyen kezeli, hiszen előirányozza annak szükségességét, hogy „*a kiberbiztonsági oktatás, képzés, valamint a kutatás és fejlesztés színvonala megfeleljen a legjobb nemzetközi gyakorlatoknak, hozzájárulva egy világszínvonalú hazai tudásbázis kialakításához.*"[11]

A nemzeti kiberbiztonsági stratégia alapelveire épülve született meg *Az állami és önkormányzati szervek elektronikus információbiztonságáról* szóló 2013. évi L. törvény, azaz a szakma által csak információbiztonsági törvénynek (Ibtv.) nevezett jogszabály. Ez a törvény alapvető változásokat hozott a hazai információbiztonság szervezeti kereteiben, valamint nagyon egyértelmű szabályozást ad a hazai információbiztonsági képzés és oktatás területére.

3. HAZAI INFORMÁCIÓBIZTONSÁGI KÉPZÉS

Az Ibtv. a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon és az ezt kezelő információs rendszerek védelme érdekében kiemelt figyelmet fordít arra, hogy a törvény hatálya alá tartozó szervezetek információbiztonsággal foglalkozó munkatársai megfelelő ismeretek birtokában lássák el feladataikat.[12]

Az Ibtv. és *a 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* (képzési rendelet) az érintett munkatársak számára egyrészt a munkakör betöltéséhez szükséges végzettségre, illetve szakmai tapasztalatra vonatkozó előírásokat rögzít, másrészt a Nemzeti Közszolgálati Egyetem (NKE) által szervezett képzéseken, továbbképzéseken történő részvétel kötelezettségét írja elő.[13]

A Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézete (VTKI) keretei között megvalósuló *Elektronikus információbiztonsági vezető szakirányú továbbképzési* szak második végzett évfolyamának eredményeit a szak minőségbiztosítási rendszerének megfelelően értékelik a szak vezetői és oktatói, valamint az egyetem érintett munkatársai, továbbá a hallgatók is.

Ugyanakkor jelen előzetes értékelés során, amely alapvetően a hallgatók szakdolgozatainak elemzésére épül, több olyan következtetés is levonható, amelyek mind a további képzések szervezése, mind az információbiztonsággal összefüggő jogalkotás során hasznosíthatóak lehetnek.

---

9 Nemzeti Biztonsági Stratégia, 2012.

10 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

11 *Uo.*

12 Krasznay Csaba, Szádeczky Tamás: *Az információbiztonság és állami szabályozása = E-közszolgálatfejlesztés: Elméleti alapok és tudományos kutatási módszerek,* szerk. Nemeslaki András Nemzeti Közszolgálati Egyetem, Budapest, 2014, 353, 249–264. (ISBN 978-615-5491-04-7)

13 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

4. AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI VEZETŐ SZAKIRÁNYÚ TOVÁBBKÉPZÉS TARTALMA

Az *Elektronikus információbiztonsági vezető szakirányú továbbképzés* az elektronikus információs rendszerek védelméért felelős vezető, az elektronikus információs rendszerek biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek szakirányú továbbképzése.[14] A képzés[15] fő célja – a Nemzeti Közszolgálati Egyetem honlapján közzétett információ szerint – „az Ibtv.-ben meghatározott elektronikus információs rendszer biztonságáért felelős személyek feladatellátáshoz szükséges szakmai kompetenciáinak átadása és a biztonságtudatos szemléletmód kialakítása".[16]

A képzés kialakítása során az Information Systems and Control Association (ISACA) nemzetközi szervezet Certified Information Security Manager (CISM) képzését vették alapul. Mindazonáltal „a nemzetközi trendek is alátámasztják, hogy az információbiztonság nemcsak technológiai, hanem elsősorban szervezetirányítási kérdés, erős jogi-közigazgatási fókusszal", ezért „a képzés – bár az információbiztonság műszaki, informatikai szakterületnek tűnik – egy speciális, információbiztonságra koncentráló menedzserképzés".[17]

A fenti állítást a magyar és nemzetközi közigazgatási,[18] valamint kutatási tapasztalatok[19] is alátámasztják. Az Ibtv. szerint a felelős vezető mellett (aki lehet a szervezet első számú vezetője vagy az általa kijelölt, megbízott „egyéb" vezető) kiemelt felelőssége van az információbiztonságért felelős személynek is. Az Ibtv. hatálya alá tartozó szervezetek esetében az ő feladatait jellemzően vagy a jogi-igazgatási szakterület vezetőjére/munkatársára telepítik (az adatvédelem hagyományosnak tekinthető feladatcsoportját bővítve ezzel), vagy az informatikai szakterület vezetőjére/munkatársára (mivel informatikai szakmai ismeretekkel végzettségéből fakadóan ő rendelkezik). A képzés tartalma összeállításának nehézsége ebből a kettősségből fakad. Az informatikai szakmai részt úgy kell összeállítani, hogy egy szakmabelinek is adhasson hasznosítható ismeretet, de az informatikától, mint konkrét szakmai feladatoktól kissé távolabb álló szakterület munkatársai számára is befogadható legyen, ugyanakkor a jogi-igazgatási szakmai rész címzettjei lehetnek jogászok, igazgatási szakon végzettek többéves jogi képzéssel

14 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 (Képzési rendelet)

15 A képzési rendelet ezt az oktatási formát nevezi *képzés*nek; ezen kívül rendelkezik az egyszer teljesítendő *továbbképzés*ről és az éves továbbképzésről.

16 vtki.uni-nke.hu/szakiranyu-tovabbkepzes/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto-szakiranyu-tovabbkepzesi-szak (2015. 10. 12.)

17 Illésy Miklós, Nemeslaki András, Som Zoltán: *Elektronikus információbiztonság-tudatosság a magyar közigazgatásban,* Információs Társadalom, 14(2014)/1, 52–73.
Forrás: www.infonia.hu/digitalis_folyoirat/2014/2014_1/i_tarsadalom_2014_1_illessy_nemeslaki_som.pdf

18 Nemeslaki András: *Vállalati internetstratégia*, Budapest, Akadémiai Kiadó, 2012, 271. (ISBN 978-963-05-9189-8)

19 Sasvári Péter, Nemeslaki András, Wolf Rauch: *Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises,* Academic and Applied Research in Public Management Science, 14(2015)/1, 63–78.

a hátuk mögött és olyan informatikusok is, akiknek jogi-igazgatási ismeretei szinte egyáltalán nincsenek, így számukra ezen a területen a legelemibb ismeretek átadása is szükséges.

A képzési idő a jogszabály alapján két félév (300 óra, ennek 80%-a elmélet, 20%-a gyakorlat), a képzés szakdolgozat megírásával és megvédésével, valamint záróvizsgával zárul. Ebben a képzésben alapképzésben vagy mesterképzésben szerzett oklevéllel rendelkezők vehetnek részt, amennyiben rendelkeznek angol nyelvű alapfokú komplex nyelvvizsgával vagy ezzel egyenértékű bizonyítvánnyal. Ez utóbbi feltétel indoka, hogy az információbiztonsági szakirodalom jelentős hányada angol nyelven érhető el, tanulmányozása ugyanakkor szükséges a naprakész ismeretek megszerzéséhez, következménye viszont, hogy az esetleg több nyelvből nyelvvizsgával rendelkező, esetenként még angol nyelvismerettel is bíró, de azt oklevéllel, bizonyítvánnyal igazolni nem tudó foglalkoztatottak, munkavállalók kiesnek a felvehető személyek köréből. Mindezek igazak úgy, hogy munkakörük betöltéséhez az angol nyelv említett dokumentumokkal igazolt ismerete nem is feltétlenül szükséges.

A képzés tárgykörei:[20]

– információbiztonsági szervezési ismeretek;
– kockázatértékelés és -menedzsment;
– stratégia és szervezeti támogatás;
– biztonsági események kezelése (incidenskezelés);
– jogi, vezetéselméleti és technológiai ismeretek az információbiztonságban.[21]

A képzés tananyaga 2014-ben, az ÁROP-*2.2.21 Tudásalapú közszolgálati előmenetel* projekt keretein belül készült és az alábbi témaköröket foglalja magában:

– A minőségirányítás alapjai;
– Biztonsági technológiák alkalmazása;
– Biztonsági tesztelés a gyakorlatban;
– Biztonságpolitika;
– Biztonság támogatása;
– Biztonságtechnika;
– Hálózatok biztonsága;
– Incidensmenedzsment, BCP, DRP integráció;
– Incidensmenedzsment gyakorlat;
– Információbiztonsági program;
– Információbiztonsági stratégia és vezetés;
– Információbiztonsági szabványok;
– Információbiztonság-tudatosság gyakorlat;
– Irányítási rendszerek;

20 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 (Képzési rendelet)

21 Az egyetem honlapja szerint a megszerezhető tudáselemek: Alapismeretek – jogi, vezetéselméleti és technológiai ismeretek, Stratégia és szervezettámogatás – Rendszerirányítási szakismeretek, Információbiztonsági szervezési szakismeretek, Információkockázatok kezelése és a megfelelőség, Információbiztonsági események kezelése (incidenskezelés) ismeretek. (2015. 10. 12.)

– Jogi és közigazgatási ismeretek;
– Kockázatértékelés, kockázatmenedzsment;
– Kockázatmenedzsment gyakorlat.

A képzés tartalmának optimalizálásához figyelembe kell venni azt is, hogy a célközönség számára a képzési rendelet további rendszeres továbbképzést is előír. Évente továbbképzésen kell részt vennie 8 órában a vezetőnek, 25 órában az információbiztonság megvalósításában közreműködőnek és 50 órában az információbiztonságért felelős személynek. Ez utóbbi továbbképzés tárgykörei:
– információbiztonsági technológiai ismeretek;
– kockázatértékelés és biztonsági események kezelése (incidenskezelés);
– informatikai biztonságpolitikai, stratégiai és szabályozási ismeretek;
– jogi és szervezetirányítási ismeretek.[22]

Első ízben ezt a továbbképzést szintén a Nemzeti Közszolgálati Egyetem szervezte meg 2014-ben, amely képzés e-learning keretében történt és vizsgával zárult. A továbbképzés elvégzéséről a résztvevők tanúsítványt kaptak. A tananyag az alábbi részekből állt:
– Kriptográfia;
– Alkalmazásbiztonság;
– Sebezhetőségvizsgálatok a gyakorlatban;
– A személyes adatok védelmének szabályozási környezete és gyakorlati kérdései;
– Elektronikus dokumentumok kezelése, hitelesítése, megőrzése.

A 2015-ben sorra kerülő továbbképzésben – a hallgatóknak e-mailben megküldött tájékoztató szerint – a tananyag (értelemszerűen), az oktatás módja és a számonkérés is módosult. A tananyag jogi-közigazgatási ismereteket tartalmazó részét személyes jelenléti (tantermi) oktatás keretében kell elsajátítani (mivel a 2015 nyarán bekövetkezett jelentős jogszabályváltozásokról még nem áll rendelkezésre hatályos tananyag), a számonkérés formája házi dolgozat. A tananyag:
– Jogi és közigazgatási ismeretek;
– Kockázatmenedzsment;
– Biztonsági technológiák alkalmazása.

5. A KÉPZÉSEN VÉGZETT MÁSODIK ÉVFOLYAM MEGISMERHETŐ SZAKDOLGOZATAI

Az első évfolyamon 2014. február és 2015. január között 30 fő képzése történt meg, 29 hallgató zárta sikeresen a tanulmányait. A jelen tanulmányban szereplő szakdolgozatokat készítő hallgatók képzése a 2014–2015-ös tanulmányi évben zajlott, 25 fő részvételével. A tanulmányok zárásakor hozzájuk csatlakozott az előző évfolyamról további 1 hallgató, így eb-

22 Vezetői éves továbbképzés: jogi, közigazgatási, vezetéselméleti és szervezetirányítási ismeretek, információbiztonsági technológiai ismeretek, informatikai biztonságpolitikai, stratégiai és szabályozási ismeretek, közreműködői éves továbbképzés: információbiztonsági technológiai ismeretek, informatikai biztonságpolitikai, stratégiai, szabályozási ismeretek, jogi és szervezetirányítási ismeretek.

ben a tanévben 26 szakdolgozat sikeres védése történt meg. A szakdolgozatok közül 6 titkosításra került, jelenleg 20, korlátozás nélkül hozzáférhető szakdolgozat áll rendelkezésre az elemzéshez. A képzés harmadik évfolyama 2015 szeptemberében indult, 38 hallgatóval.

A szakdolgozatok szerzői a magyar közigazgatás (központi és területi államigazgatás, illetve önkormányzati igazgatás), valamint az Ibtv. által érintett piaci szféra különböző területeiről érkeztek, a dolgozatok tárgya is ennek megfelelő szóródást mutat.

A szakdolgozatok áttekintésének nem célja az egyes munkák tartalmának tételes értékelése, minősítése. A tanulmány – a hallgatók témaválasztása, a dolgozatokban megjelenő (régi vagy újonnan megszerzett) tudásanyag legfontosabb elemeinek hangsúlyozottsága, a téma feldolgozásának módja, mélysége, valamint a felvetett általános és sok esetben konkrét problémák, kérdések alapján – az oktatói és a jogalkotói tevékenység tervezéséhez, végrehajtásához kíván – néhány szempont felvetésével – támogatást nyújtani.

A szakdolgozatok fent említett szempontok szerinti áttekintése alapján az alábbi megállapítások tehetők.[23]

1. A szakdolgozatok – a hallgatók előképzettsége, munkaköre, érdeklődése alapján – részben informatikai-műszaki, részben jogi-igazgatási témákat tárgyalnak. A dolgozatok egy része a képzés során megismert tananyagokat, kapcsolódó szakirodalmat ismerteti, értékeli, másik része a megszerzett ismereteket és a saját, konkrét élményeket, problémákat, tervezett vagy már végrehajtott feladatokat írja le, veti össze. Mindkét típusban jelen vannak a „top témák", a közkedvelt ábrák, szófordulatok.

2. Az Ibtv. és a *77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményekről* (a továbbiakban: technológiai rendelet) előírásainak teljesítésével összefüggésben jelentős az adminisztratív, szabályozási kötelezettségekkel kapcsolatos tartalom, így különösen az informatikai biztonságpolitika, informatikai biztonsági stratégia és informatikai biztonsági szabályzat, valamint a kapcsolódó eljárásrendek kidolgozása.[24] A szabályozás szintjeivel, tartalmával hat szakdolgozat foglalkozik.

Hangsúlyosan szerepelnek az informatikai rendszerekkel kapcsolatos besorolási, kockázatelemzési feladatok. Elméleti kérdéseket négy dolgozat tárgyal, három dolgozat saját módszertant ismertet, ugyanazon kockázatelemzési képletet két dolgozat idézi.

Külön kört képeznek az önkormányzatok, kis szervezetek esetében felmerülő problémák, különösen

– a saját információbiztonsági kapacitás, szaktudás hiánya;
– a biztonsági és üzemeltetési feladatok egy személy általi ellátása;

23 A közölt adatok arányokat, tendenciákat jelölnek, nem cél a teljes körű, tételes tartalomelemzés, felmérés.

24 2015. július 16-ai hatállyal a 77/2013. NFM rendelet helyébe lépett a *41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről*. Az új jogszabály már nem tartalmazza az informatikai biztonságpolitika, informatikai biztonsági stratégia elkészítésére vonatkozó követelményt.

– az információbiztonsági feladatok ellátása kiszervezésének (outsourcing) szükségessége, terhei és kockázatai (kitettség, magas szakértői költségek stb.);
– a szolgáltatók által előkészített szerződések felelősséget korlátozó rendelkezéseinek diktátum jellege.

Figyelemre méltó a jogszabály végrehajtása során tapasztalt – a jogi szabályozás hiányosságaiból vagy éppen a túl szigorú szabályozásból fakadó – problémák köre. Ilyen például

– a más szervezet által fejlesztett és üzemeltetett informatikai („idegen") rendszer használata következtében felmerülő információvédelmi feladatok (pl. besorolás, kockázatértékelés szükségessége vagy a tulajdonos, szolgáltató általi értékelés átvételének lehetősége) és felelősségek tisztázatlansága;
– a központi és területi szervek, integrált és integrálódó szervezetek feladatellátása során felmerülő szabályozási, üzemeltetési és felelősségi kérdések, figyelemmel a többes és többszintű irányítási, felügyeleti jogkörökre, az elődszervezetek továbbélő eltérő gyakorlatára;
– a nagyszámú, eltérő infrastruktúrán működő, eltérő informatikai támogatással rendelkező alkalmazással összefüggő adminisztratív feladatok teljesíthetősége, ár-érték aránya;
– az országos rendszerek, adatbázisok, hálózatok és ezek helyi részhalmazaira vonatkozó biztonsági elvárások teljesíthetősége központi, jelentősebb erőforrások és szűkös helyi erőforrások esetében.

Az előírt információvédelmi kötelezettségek és a forráshiány ellentéte szervezeti mérettől függetlenül megjelenik.

3. A felhasználók információbiztonsági közömbössége, az információbiztonsági tudatosság hiánya nyolc dolgozatban szerepel, a biztonságtudatosság növelését célzó oktatásról (tematika, tananyag, célcsoportok stb.) pedig hét dolgozat szól. Ezzel összefüggésben a kártékony kódok elleni védekezés szükségességével öt hallgató foglalkozott, a jelszóhasználattal összefüggő hibákra (nem megfelelő hosszúságú, bonyolultságú jelszó használata, a jelszó felírása mások számára elérhető módon, közös jelszavak használata, jelszavak átadása stb.) hat dolgozatíró tért ki, a jogosultságkezeléssel és a felhasználói tevékenység naplózásával összefüggő problémákat három dolgozat tárgyalta.

4. A szakdolgozatok szakmai mélysége is változó. Egyes, erre egyébként is hajlamosító témáknál (biztonságtudatosság, kártékony kódok elleni védelem, jelszóhasználat, szabályozás) vélhetően az ismeretösszegzés, ismeretterjesztés volt a szerzők célja. Az ITB 12. ajánlásában szereplő adatbiztonsági ábrát öt, a PDCA[25] modellt két, a CIA[26] információbiztonsági elvet négy munka tartalmazza. Az esettanulmányok, a feladat-tervezések és -végrehajtások leírásai értelemszerűen egyénibb látásmódot tükröznek, problémafelvetéseik konkrétabbak, életszerűbbek. A megkülönböztetés értékítéletet nem tartalmaz, mindkét típus szükséges és visszacsatolásként hasznosítható.

5. A jogi-igazgatási fogalomhasználat több dolgozatban pontatlan, hibás, elavult; előfordul már nem hatályos törvényre történő hivatkozás is.

6. Erős szóródást mutat a dolgozatok terjedelme.

25 PDCA: Plan, Do, Check, Act – Tervezés, Végrehajtás, Ellenőrzés, Beavatkozás
26 CIA: Confidentiality, Integrity, Availability – Bizalmasság, Sértetlenség, Rendelkezésre állás

7. A dolgozatok formai jellemzői kapcsán megjegyzendő, hogy több ízben előfordul szerkesztési következetlenség (mondatok, bekezdések ismétlése), központozási hiba, a hivatkozások jelölése nem egységes.

6. A KÉPZÉSSEL ÖSSZEFÜGGŐ ÉSZREVÉTELEK

A mottóban jelzett haszon több szempont szerint, több viszonylatban is értelmezhető. A hallgató új ismereteket szerez, új készségekre tesz szert, ezeket remélhetőleg hasznosítani tudja a napi feladatellátása kapcsán (a szakdolgozatok témaválasztásai utalnak arra, hogy a hallgatók és az oktatók is a gyakorlatban hasznosítható tudás megszerzését-átadását részesítik előnyben). A képzésen részt vett személyek a tudást továbbsugározzák munkahelyi környezetükben, így az Ibtv. hatálya alá tartozó szervezetek és munkatársaik másodlagos haszonélvezőivé válhatnak a képzésen átadott ismereteknek. Amennyiben az ilyen „haszonélvező" szervezetek száma növekszik, a jogalkotói cél – információbiztonsági szempontból megbízhatóbban működő információs rendszerek, tudatosabb felhasználók, biztonságosabb adatkezelés – is teljesülhet.[27]

Ahhoz azonban, hogy ez az ismeretátadási rendszer folyamatosan biztosítsa a korszerű tudás terjesztését – részben az elvárások, részben a tapasztalatok alapján – a képzés folyamatos korrekciója, optimalizálása is szükséges.

A szakdolgozatok fent említett szempontok szerinti áttekintése alapján az alábbi megfontolások érdemelhetnek figyelmet.

1. Pontosítandó a képzés célja és ennek alapján a tartalma. Amennyiben a cél az információbiztonsági felvilágosítás, egységes szemlélet és gyakorlat elterjesztése, a „mindenből egy kicsit, rendszerezetten" elv – a korábbi képzések során teljesített tantárgyak alóli mentesítésekkel – érvényesülhet. Egy jogász számára a 10-20 órás, jogi ismeretek átadását célzó tárgy időpazarlás lehet, egy informatikus számára az információtechnológiai alapfogalmak „megismertetése" lehet felesleges. Ilyen tartalmú képzés elsősorban a biztonságtudatos szemléletmód kialakítását szolgálhatja; első körben a hallgatókét, ezt követően – amennyiben megszerzett ismereteiket továbbadják és ennek a tudástranszfernek kedvező a fogadtatása – a környezetükét. Amennyiben a cél a képzési rendeletben is megjelenített, piaci képzéssel egyenértékű szakmai kompetenciák átadása, a különböző előképzettséggel rendelkező hallgatók tananyagát differenciálni és mélyíteni kell műszaki-informatikai és jogi-igazgatási irányok szerint.

2. A fenti célok alapján célszerű az éves továbbképzést is újragondolni. Alapismeretek évenkénti átadása nem túlságosan vonzó oktatási forma, magasabb szintű kurzusok biztosítása 3-5 évente rangot adó tapasztalatszerzés lehet.

3. A hallgatók előképzettségének különbözősége miatt a homogén oktatási csoportok és tananyag kialakítása nem feltétlenül célravezető (lásd előbb).

4. Az 1. és 2. pontban foglaltakkal összefüggésben kerülendő olyan ismeretek átadása személyes jelenléti képzésben, amelyek az arra feljogosított hatóság által kiadott ajánlásokban,

27 Szádeczky Tamás: *Information Security – Strategy, Codification and Awareness = ICT Driven Public Service Innovation: Comparative Approach Focusing on Hungary*, szerk. Nemeslaki, Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., Budapest, 2014, 208, 109–122. (ISBN:978-615-5305-89-4)

útmutatókban is közzétehetők, vagy kampányokkal közvetíthetők (ez utóbbira példa lehet az Alkotmányvédelmi Hivatal Awareness programja).[28] A közigazgatásban ezek alapján egyes információvédelmi szakmai evidenciák az irányító, felügyelő szervek által kötelező normaként előírhatók, így a képzési időkeret mélyebb ismeretek átadására vagy az ismeretek elmélyültebb feldolgozására fordítható.

5. Az előző ponthoz is kapcsolódva célszerű lehet az egyénre szabottabb tanári támogatás (szükség esetén korrekció) biztosítása az előadásokon elhangzott tananyag feldolgozása és a szakdolgozat elkészítése során. A képzés akkor lehet sikeres, ha a közös „információvédelmi műveltségi minimum" biztosításán túl a hallgatóknak egyéni igényeiknek megfelelő szakmai felkészítést is nyújt, hiszen a végső cél olyan szakemberek képzése, akik a jogszabályokban előírt feladatokat végre tudják hajtani vagy hajtatni. Ehhez stabil, a mindennapokban alkalmazott tudás szükséges.

6. A mindennapokban alkalmazható tudás átadásának elvéhez kapcsolódva kifejezetten ajánlott konkrét segédletek, módszertanok megismertetése, kipróbáltatása. Így például hangsúlyos a jogszabályok által elvárt dokumentumok elkészítésének támogatása, de a feladatkipipálás helyett a jogalkotói célnak megfelelő, valóban érdemi szabályozás és dokumentálás kialakításának támogatása szükséges.

7. Az oktatói felelősség érzékeny pontja a szakmai igényesség és az önkorlátozás egyensúlya megteremtésének megtanítása. A szakmai toposzok, közhelyek mechanikus ismétlése, a túlbuzgó lelkesedés (a dolgozatokban ezekre is akad példa) a várttal ellentétes hatást válthat ki. Az információbiztonsági szabályozás és felügyelet felhasználói élményt korlátozó tevékenységként jelenik meg a mindennapokban, nem kell a képviselőit még meg is utáltatni.

A megismert szakdolgozatok tartalmától független, de a megismerhetőséggel összefüggő javaslat a szakdolgozatok titkosításának mellőzése. Valóban érzékeny adatok felhasználásához a képzést finanszírozó szervek, szervezetek jellemzően nem járulnak hozzá (üzleti titkok, minősített adatok stb. felhasználása további védelmi garanciákat igényelne a képzést lebonyolító részéről). Ugyanakkor az általában kijelenthető, hogy a közigazgatási szervek foglalkoztatottjainak közpénzből finanszírozott képzésének eredménye legyen mindenki által hasznosítható tudás.

7. AZ IBTV. ÉS A KAPCSOLÓDÓ RENDELETEK VÉGREHAJTÁSÁNAK TÁMOGATÁSÁRA VONATKOZÓ JAVASLATOK

A szakdolgozatok témaválasztása, a kiemelten tárgyalt kérdéskörök, valamint a konkrét kérdésfelvetések, javaslatok egyértelműen utalnak azokra a problémákra, amelyek megoldásához a végrehajtásban érintettek további segítséget várnak.

1. A biztonsági besorolás (információs rendszer biztonsági osztályának, szervezet biztonsági szintjének a meghatározása) és a kockázatelemzés – előzmények híján – (túl) nagy feladatot jelent az Ibtv. hatálya alá tartozó közigazgatási szervek érintett munkatársainak. A kockázatelemzés megkönnyítéséhez célszerű lenne konkrét módszertani útmutató rendelkezésre bo-

28 Forrás: ah.gov.hu/html/awareness.html (2015. 10. 12.)

csátása, amely a képzésen oktatott elméleti alapokon túl tartalmazhatná az előírt feladatok teljesítése során született eredményeket (amelyeket a jogszabály rendelkezése szerint a Nemzeti Elektronikus Információbiztonsági Hatóság számára meg kellett küldeni).[29] Az elektronikus információs rendszerek esetében felmerülő összes kockázat számbavétele, értékelése egységes gyakorlati útmutató nélkül aránytalanul nagy feladatot jelent az egyébként is kapacitáshiányos kis szervezeteknél (jellemzően önkormányzatoknál), ráadásul az eredmény szubjektív lesz, hiszen egyéni döntéseken múlik az egyes tényezők figyelembevétele.

2. A kis szervezetek már említett erőforráshiánya ismét többelemű probléma. Ha nincs információvédelmi szakember, külső szaktudást kell igénybe venni (a dolgozatok utalnak a 3–15 millió Ft-os áron ilyen jellegű szolgáltatásokat kínáló cégekre, illetve a kiszervezés információbiztonsági kockázataira is). Az outsourcing költségeire azonban nincs fedezet (ahogyan sok esetben az előírt információvédelmi eszközökre, megoldásokra sincs).

3. A jogszabályban meghatározott jelenlegi információbiztonsági elvárásrendszer – éppen a számonkérhetőség érdekében – nagyon kötött, szigorú; nem ad módot a szervezetek és információs rendszereik mérete, munkaszervezési sajátosságai szerinti differenciálásra, nem veszi figyelembe a különböző szervezetek által közösen használt, illetve a szervezetek együttműködő rendszereinek szabályozási és felügyeleti igényeit. A továbbiakban célszerű lenne megteremteni ennek lehetőségét.

4. Pénzügyi többletforrások biztosítása nélkül a jogszabályokban előírt feltételek teljesítésének lehetősége – még a két-két éves felkészülési időszakokkal is – erősen kérdéses.

5. Az információbiztonsági tudatosságra nevelés feladatának és felelősségének az információbiztonságért felelős személyre telepítése figyelmen kívül hagyja az előző pontokban jelzett erőforrásbeli problémákon túl azt a tényt is, hogy ennek a tevékenységnek a fogadtatása az érintettek részéről – részben a felhasználók hamis biztonságtudata miatt – az esetek túlnyomó többségében nem kedvező (az oktatás a szükséges rossz).

6. Ugyanez a helyzet az információbiztonságért felelős személy általános információbiztonsági feladatkörei tekintetében is. Nem elhanyagolható körülmény, hogy az információbiztonságért felelős személy csak egy a különböző szerveknél kijelölt számtalan felelős (adatvédelmi felelős, biztonsági vezető, integritás tanácsadó stb.) közül; nem mindenható, szervezeti presztízse és tevékenységének eredményessége másoktól, ez utóbbi nagymértékben a rendelkezésre álló pénzügyi erőforrásoktól is függ. Nem lehet cél sem a jogszabályi követelmények teljesítésének „lepapírozása", sem az információbiztonságért magányosan küzdő „mártírok" kitermelése.

7. Szükséges lehet – a jelenlegi kinevezési és megbízási gyakorlatra tekintettel – az információbiztonságért felelős személy feladatellátáshoz szükséges végzettségére és szakképzettségére vonatkozó rendelkezések korrekciója és ennek alapján a képzések, továbbképzések tartalmának finomhangolása.

29 Az Ibtv. módosítása eredményeként 2015. október 1-jén a Nemzeti Elektronikus Információbiztonsági Hatóság, a Kormányzati Eseménykezelő Központ (GovCERT) és a Nemzeti Biztonsági Felügyelet szervezeti keretein belül működő Cyber Defence Management Authority összeolvadásával megalakult a Nemzeti Kibervédelmi Intézet. Forrás: www.kormany.hu/hu/belugyminiszterium/rendeszeti-allamtitkarsag/hirek/megalakul-a-nemzeti-kibervedelmi-intezet

1. táblázat • *A szakdolgozatok alapadatai*

Cím	Tartalom
Hatásköri kérdések az Ibtv. szabályozásában	Az Ibtv.-ben meghatározott információvédelmi elvárások teljesítésével összefüggő kérdések a kormányhivatalok esetében, figyelemmel a kormányhivatalok és a központi hivatalok speciális kapcsolatára.
Ágazati hitelesítés-szolgáltatás kialakítás IT biztonsági kérdései, különös tekintettel a fizikai biztonságra	Az elektronikus aláírással kapcsolatos szolgáltatások létrehozásának feltételei, tervezésének folyamata, elvárt fizikai biztonsági környezete.
Információbiztonsági kockázatok felmérése a Ceglédi Közös Önkormányzati Hivatalnál	Kockázatelemzés elmélete és lehetséges módszertana egy konkrét önkormányzati szerv esetében.
Biztonságtudatosságot fokozó oktatási program létrehozása a KÖTIVIZIG-nél	Egy konkrét vízügyi szerv dokumentumkezelő rendszerének alkalmazása, alkalmassá tétele az információvédelmi dokumentumok kezelésére és hozzáférhetővé tételére, valamint a felhasználók információbiztonsági tudatosságát növelő audiovizuális oktatási anyagok készítése.
Kormányzati célú elkülönült hírközlő hálózat információbiztonságának szabályozása	A honvédelmi tárca információvédelmi szabályozásának bemutatása.
Felhasználók biztonságtudatosságának kezelése	Az informatikai biztonság fogalma, különös tekintettel az emberi kockázatokra (felhasználók, külső személyek tevékenysége). Az informatikai rendszerek felhasználóinak informatikai biztonsági tájékoztatása, képzése, biztonságtudatosságának növelése.
Az Ibtv. implementálása kis szervezeteknél	Az Ibtv. és végrehajtási rendeletei által meghatározott elvárások és feladatok az 1. és 2. biztonsági szintbe sorolt kisméretű szervezetek vonatkozásában.
Biztonság fokozását szolgáló technikai eszközök kiválasztása	Jogszabályok, stratégiák, szakmai ajánlások, módszertanok átfogó bemutatása az információbiztonsági tervezéssel összefüggésben.
Ibtv. követelmények az egyszerű és összetett közigazgatási rendszerekben	Az információvédelem szabályozási előzményei, az Ibtv.-ben meghatározott feladatok, felelősségek értelmezése, megvalósíthatóságának értékelése, az információbiztonsági tudatosság mérése.
„Tudáscsöppek" – biztonság-tudatosító e-learning oktatás a XVIII. kerületi Polgármesteri Hivatalban	Egy konkrét önkormányzati szervnél megvalósított információbiztonsági oktatás tartalma és tapasztalatai.

A kiberbiztonság szerepének felértékelődése, mint napjaink fő biztonsági kihívása	Elméleti összefoglaló, kiberincidensek, szereplők összegző bemutatása.
A felhasználók biztonságtudatosságának kezelése és fejlesztése az önkormányzatoknál	Az információvédelem személyi aspektusai; helyzetértékelés és képzésre vonatkozó javaslatok egy konkrét önkormányzati szervnél szerzett tapasztalatok alapján.
Adatvédelmi szempontból kiemelten veszélyeztetett objektumok biztonságtechnikai védelme	Az információvédelem egyik részterülete: objektumvédelmi megoldások egy képzeletbeli nagykövetségi épület esetében.
Felhasználók biztonságtudatosságának fejlesztése	Az információvédelem különböző területeinek bemutatása. Kérdőíves felmérés a biztonságtudatosság növelését szolgáló oktatás előtt.
A Celldömölki Közös Önkormányzati Hivatal információbiztonsági helyzete az Ibtv. tükrében	Az Ibtv.-ből fakadó információvédelmi feladatok egy konkrét önkormányzati szerv esetében, különös tekintettel az elvárt alapdokumentumok elkészítésére.
Az európai uniós pályázatkezelő rendszerek vizsgálata az elektronikus információbiztonsági vezető szemével	Szoftverfejlesztés elméleti alapjai és biztonsági kérdései a Magyarországon alkalmazott pályázatkezelő rendszerekkel összefüggésben.
Informatikai biztonságtudatosság-növelő oktatási anyag	Biztonságtudatossággal kapcsolatos alapismeretek rendszerezése, példákkal, fogalommagyarázatokkal.
A bírósági épületek komplex védelme napjaink biztonsági kihívásainak tükrében	Egy elképzelt bírósági épület védelmi rendszerei (környezetbiztonság, vagyonvédelem, informatikai védelmi rendszer, személyalapú fenyegetések, adatközponttal szembeni elvárások).
IBIR bevezetése a Zalavíz Zrt.-nél	Információbiztonsági irányítási rendszer kiépítése a már működő és tanúsított minőségirányítási és környezetirányítási rendszerekhez történő illesztéssel.
Humán kockázatok azonosítása és kezelése a közigazgatásban	Az információbiztonsági felelősséget hordozó munkakörök szabályozási, oktatási kérdései, különös tekintettel a jogszabályok jelenlegi tartalmára és az elektronikus információbiztonsági vezető szakirányú továbbképzésre.

8. ÖSSZEGZÉS

Több, fent ismertetett dolgozat, számos előadás és tanulmány szögezi le, hogy az Ibtv. és végrehajtási rendeletei – beleértve a képzési rendeletet is – legnagyobb erénye, hogy megszülettek.

Egy-másfél évvel a hatálybalépésük után – figyelemmel az elmúlt időszak részben ismertetett történéseire – megállapítható, hogy jelentőségük ennél jóval összetettebb. Célokat tűztek ki és ezek megvalósításához támogató szervezeteket, folyamatokat rendeltek. Az első ered-

mények már megismerhetők. Annak érdekében, hogy a kitűzött célok és a megvalósítás érdekében megteendő lépések összhangja egyre nagyobb legyen, ahogyan az a képzés során is elhangzott, a visszacsatolások értékelése és a szükséges korrekciók sem maradhatnak el. Ehhez kívánt jelen tanulmány néhány felvetéssel hozzájárulni, remélhetőleg sikerrel.

SUMMARY IN ENGLISH: Information safety is a key factor today. Creating information security is a priority in public service. However, implementing and maintaining information security is not only a technical issue. The preparation and continuing education of administrative leaders as well as information managers are essential.

In 2014 the National University of Public Service lunched a further training programme for information security experts. These trainings are required by the Act on Information Security of Hungary. This study summarizes the first experiences of the trainings, which is based on the students' final theses. The findings of this paper may serve as valuable feedback for the training organizers as well as for the legislator. This paper is based on the freely accessible final theses submitted in 2015.

Prof. Dr. Kovács László ezredes (kovacs.laszlo@uni-nke.hu): a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Karának egyetemi tanára. Több mint húsz éve foglalkozik elektronikai hadviseléssel, valamint információs műveletekkel. Az egyetemen oktatóként részt vesz az alap-, mester- és doktori képzésben. Az oktatás mellett tudományos kutatásokat folytat, amelyek a kiberhadviselés, az információs terrorizmus, a kritikus információs infrastruktúrák védelme, valamint az információs hadviselés különböző kérdéseit vizsgálják. 2005-ben, illetve 2009-ben információs terrorizmus kutatási témával elnyerte a Magyar Tudományos Akadémia Bolyai János Kutatói Ösztöndíját. Több olyan PhD-hallgató tudományos témavezetője, akiknek kutatásai az információbiztonság, az információs támadások, illetve az ellenük való védekezés nemzetbiztonsági kérdéseit vizsgálják.

Nagyné dr. Takács Veronika (takacs.veronika@freemail.hu): szakokleveles külügyi szakértő, jogász. A Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola hallgatója 2011 óta. Kutatási témája az adatvagyon-gazdálkodás a közigazgatásban: stratégiaalkotás és szabályozás a Nemzeti Adó- és Vámhivatal adatvagyon-gazdálkodási tapasztalatai alapján. Doktori kutatásai alatt közel 15 tudományos és szakcikke jelent meg a témában.