**NEMZETI KÖZSZOLGÁLATI EGYETEM**
**Közigazgatás-tudományi Doktori Iskola**

Som Zoltán

# Az információbiztonsági tudatosság kérdései a közigazgatásban

Doktori (PhD) értekezés

## TÉZISFÜZET

Témavezető:
Dr. Szádeczky Tamás, egyetemi docens

Budapest, 2021

# 1 AZ ÉRTEKEZÉS TÉMÁJA, CÉLJA

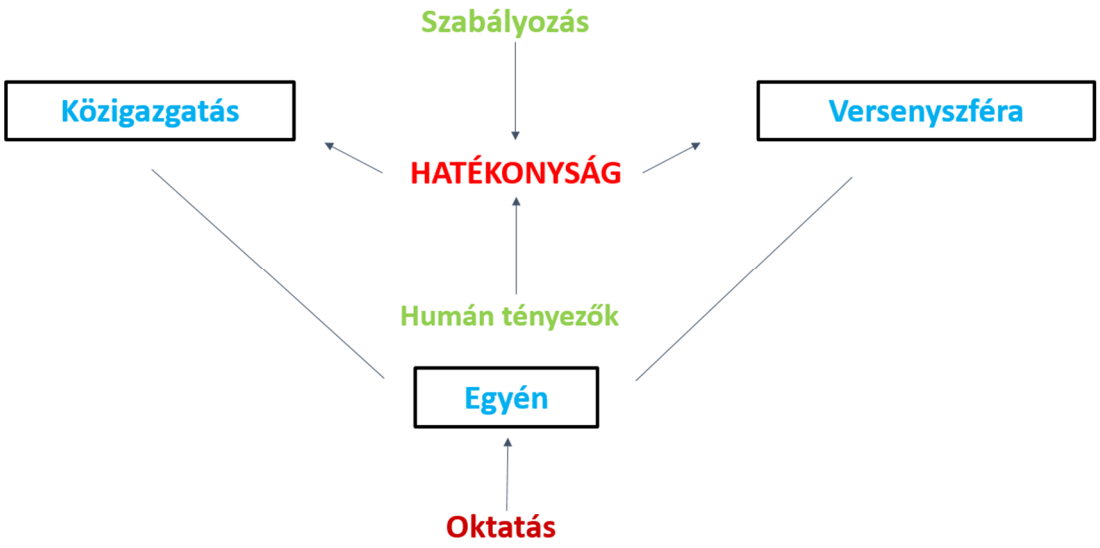
Felgyorsult világunkban a tudás mennyisége folyamatosan növekszik, egyre komplexebb, összetettebb tudás szükséges az informatikai rendszerek működtetéséhez, használatához és mindezek biztonságához. Az egész életen át tartó tanulás (ún. LLL, a lifelong learning) alapkövetelmény. A lexikális, elméleti tudás helyett a tudásalapú gazdaság és társadalom, a munkakörnyezet túlzott dinamizmusa miatt inkább az egyén adaptív és innovatív készségei fejlesztendők. Az önálló tanulni tudás és akarás képessége teszi lehetővé az állandóan változó környezethez való sikeres alkalmazkodást és a személyes megújulást. A jól teljesítő szervezetek sikerének egyik oka, hogy a vezető- és szervezetfejlesztés a szervezeti stratégia része. Olyan befektetés, amely a szervezet hosszú távú eredményes és hatékony működését biztosítja. A tanulási-oktatási kihívás komplexszé vált (folyamatos időhiány, stressz, multitasking, folyamatos változás stb.), ami hagyományos képzési formák segítségével nem kezelhető hatékonyan. A munkaszervezeteknek és munkavállalóknak olyan támogatásra van szüksége, amely a lehetőségekhez képest egyénileg róluk szól, időalap-kímélő, praktikus, mégis folyamatos, önállóan is elvégezhető önfejlesztést tesz lehetővé. Ehhez újszerű oktatási módszerek kombinációja szükséges. A formális oktatások mellett további csatornákat is szükséges bevonni a tudás átadás és tudatosság növelés érdekében. Az információbiztonsági kihívások megkövetelik, - ezzel párhuzamosan - hogy az aktuális, gyorsan változó kockázatokra, támadási vektorra egy emberként tudjon reagálni a munkaszervezet. Disszertációmban bemutatom az információbiztonsági szempontból releváns szabályozási környezet Magyarországi fejlődését 1994-től a közelmúltig. A 2013. évi L. (az állami és önkormányzati szervek elektronikus információbiztonságáról szóló) törvényt az Országgyűlés a 2013. április 15-i ülésnapján fogadta el, a kihirdetés napja 2013. április 25. Még ebben az évben megkezdődött a Nemzeti Közszolgálati Egyetemen (NKE) az Elektronikus információbiztonsági vezető (EIV) szakirányú továbbképzési szak oktatása, mellyel elindult a magyarországi információbiztonsági vezetők egyetemi képzése. Voltaképpen a törvény ezen mozzanata, a szakemberképzés elindítása rendkívül fontos lépés és szimbolikus jelentőségű: az oktatás fontosságára hívja fel a figyelmet. A megfelelő információbiztonsági szint belátható, hogy nemcsak egyéni vagy munkaszervezeti érdek, hanem nemzeti és nemzetgazdasági szinten is fontos. Ez azonban nem érhető el megfelelően felkészült szakemberek képzése nélkül. Az információbiztonsági tudatosság, felkészültség fontos egyrészt a magánérdekek mentén, másrészt állami szempontból az ügyfélbizalom, valamint az információs rendszerekbe és elektronikus állami szolgáltatásokba vetett bizalom szempontjából is. A közigazgatás mellett

említést kell tenni az e-közigazgatásról is, amely évek óta folyamatosan fejlődik és egyre nagyobb területet hódít meg, azaz egyre elterjedtebb a használata mind a közigazgatásban, mind pedig a felhasználói oldalon, az állampolgároknál. Budai (2016) így fogalmaz: "Az e-közigazgatás kialakítása olyan kényszer, amelyet az információs társadalom egymást feltételező (társadalmi, technológiai, szociális, politológiai, jogi stb.) összetevői diktálnak." Így érinti tehát mind a közigazgatásban dolgozókat, mind pedig nemzeti, közigazgatási szinten az összes olyan állampolgárt, aki ügyeket kíván intézni; később pedig lehetséges európai uniós folyamatokkal történő összekapcsolása is megjelenhet, vagy gondolhatunk egyéb nemzetközi közigazgatási kapcsolatokra, állami és nemzetközi tevékenységekre. Ez viszont nemcsak szigorúan véve vett közigazgatási fejlesztéseket kíván, hanem a kompetenciák, tudás fejlesztése is szükséges. Budai (2016) így fogalmaz: "Bármilyen meglepő, a közigazgatás modernizációjának felhasználói oldala a nélkülözhetetlen kompetenciák fejlesztésénél: az írástudás oktatásánál kezdődik, mely egyre inkább a digitális írástudás dimenziói felé mozdul el. A járulékos kompetenciák pedig biztosítják az önálló továbbfejlődés, élethosszig tartó tanulás lehetőségét. A felhasználókat tehát képezni kell, így az erre irányuló programokat (…) a közigazgatási megújítás ütemtervéhez kell igazítani. Egyúttal erősíteni kell azokat a támogató programokat, melyek a közigazgatási szolgáltatások hatékonyabb állampolgári igénybevételét támogatják: ügysegédlet, IT-mentorálás." Az (információbiztonsági) oktatáshoz szükséges lehet a meglévő és a szükséges informatikai kompetenciák felmérése és kialakítása. (Bujdosó, 2014) Továbbá figyelembe kell venni, hogy az átviteli közeg használatában való jártasság szintén jelentősen képes befolyásolni az átvinni kívánt tudás, információ hasznosulását. (Bujdosó, 2015)

Belátható továbbá, hogy nem nélkülözhető az információbiztonsági kompetenciák fejlesztése sem, ahol a felhasználói oldal túlnyúlik a közigazgatásban dolgozókon; s a közigazgatási szolgáltatásokat igénybe vevőkre (például: az állampolgárokra) is gondolni szükséges. Mindezeken az államhoz köthető e-közigazgatási és közigazgatási aspektusokon kívül meg kell említeni a GDP arányosan szignifikánsan jelenlévő IKT szektort, e-kereskedelmi fejlesztéseket és befektetéseket (Som, Papp 2015).

A 2013-as L. törvény, majd az azt követő 41/2015 BM végrehajtási rendelet, illetve az ágazatspecifikus [17/2019. (VIII. 15.) BM utasítása; a Belügyminisztérium és a belügyminiszter által irányított szervek elektronikus információbiztonsággal összefüggő biztonságtudatos viselkedési kódexe kiadásáról] rendelet kapcsán látható, hogy törvényi szinten megjelent az igény, hogy a fejlődés érdekében szervezett információbiztonsági oktatások valósuljanak meg. Ezen folyamatok már 1994-ban megkezdődtek, az Informatikai Tárcaközi

Bizottság 8. sz. ajánlásával, címe: Informatikai biztonsági módszertani kézikönyv. Majd ezt követte időben az Informatikai Tárcaközi Bizottság ajánlásai közül 1996-ban a 12. sz. ajánlás, melynek címe: Informatikai rendszerek biztonsági követelményei. 2008-ban pedig a Közigazgatási Informatikai Bizottság 25. számú ajánlása Magyar Informatikai Biztonsági Ajánlások (MIBA) címmel, amely voltaképpen egy ajánlás gyűjtemény. Valamint egyéb ágazatspecifikus, de mégis információbiztonságot érintő fontos jogszabályok a zártsági tanúsítás előírása a 2008. évi XL. tv. 100. § (1b) bekezdés, (törvény a földgázellátásról) valamint a 2011. évi CCIX. tv. 63. § (törvény a víziközmű-szolgáltatásról). Továbbá a Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájával [1838/2018. (XII. 28.) Korm. határozata], vonatkozásában kiberbiztonsági oktatás, képzés, valamint a kutatási és fejlesztési lehetőségek, versenyképes hazai tudásbázis létrehozásához kapcsolható a jogalkotói szándék. A szabályozás tekintetében a magyar közigazgatást a 2013 éves L. tv. az élvonalba emelte, jó alapot teremtett az információbiztonsági törekvéseknek, ugyanakkor szakirodalom feldolgozás során, arra a következtetésre jutottam, hogy számos szerző különböző HUMÁN szempontokat is bevont kutatásaiba. A SZABÁLYOZÁS (a szabály-alkotás) mint KEMÉNY követelmény van jelen az általam vizsgált tényezők közt, míg az újonnan megjelent HUMÁN tényezőket, PUHA tényezőként vettem figyelembe, amellyel az információbiztonság hatékonyságát lehet emelni. Ezen összefüggésrendszert, azaz a kutatásom fő vonulatát mutatom be az 1. ábrán.




1. ábra: A kutatás összefüggésrendszere

Az ábráról leolvasható, hogy az információbiztonsági hatékonyság úgy növelhető, ha egy-egy szféra hatékonyságát az egyén tudatosságán keresztül növeljük, amely az oktatáson keresztül valósítható meg. Az oktatás azt a célt szolgálja, hogy ha az egyén effektívebben megérti, akkor

jobban el is fogadja, sőt hathatósabban is követi a szabályzatot, vagyis még hatékonyabb lesz általa az információbiztonság. A KÖZIGAZGATÁS e tekintetben kiemelkedően jelentős szereppel (és felelősséggel) bír, hiszen a közigazgatás azon szervezetek összessége, amelyek közfeladatokat látnak el és országos jelentőségű ügyekben járnak el, szolgáltatásokat nyújtanak. Ha pedig Magyarország egyik legnagyobb munkáltatójaként tekintünk a közigazgatási szervezetek összességére, akkor az ott dolgozók tudásának fejlesztése révén nemzeti szintű változások indukálhatóak.

A baseline mérés és kiértékelés utáni oktatások és azok kiértékelése révén meghatározhatóvá válnak az információbiztonsági fejlesztés kritikus területei. Voltaképpen a jelenlegi szint mérése (As-Is állapot) azért fontos, hogy azt követően mérhetőek, nyomon követhetőek legyenek a változások. Az elmúlt évek során látható, hogy nem tartunk még ott, hogy a közigazgatási információbiztonsági felelősök szervezett módon eszközt kapjanak, vagy önszerveződő módon egy ilyen folyamat elinduljon. Több kezdeményezés is létezik, hogy ezen információbiztonsági felelősök szakmai kapcsolatokat tudjanak egymással vagy piaci szereplőkkel építeni, ám ennek célja és funkciója más. Kijelenthető tehát, hogy az információk (a fentebb bemutatott információbiztonsági ajánlások) és törvényi feltételek adottak. Ezért is tűztem ki célul ennek vizsgálatát, hogy objektív módon lehessen vizsgálni a tényeket, feloldani azt a látszólagos ellentmondást, ami egy-egy munkaszervezetben vett egy-egy kiscsoportos mintából, vagy az oktatás során kapott visszajelzések során megjelentek. Az eltérések azonban már ott is jelentkeztek, hogy hogyan tudták ezt a szervezetek alkalmazni, hogyan értelmezték az ajánlásokat és a jogszabályokat, mit értettek oktatás alatt, hogy milyen hatékonyságú szabálykövetés valósult meg általa. Disszertációmban kizárólag az információbiztonsági oktatással kapcsolatos, meghatározott kérdéseket vizsgáltam. Ezen, egyes szervezetekre jellemző tényező nem került vizsgálatra, hogyan értelmezték az ajánlásokat, jogszabályokat, hogyan építették be azt a folyamatokba.

A magyar közigazgatás szempontjából az értekezés az alábbi célokhoz kapcsolható:

- Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájával [1838/2018. (XII. 28.) Korm. határozata], vonatkozásában kiberbiztonsági oktatás, képzés, valamint a kutatási és fejlesztési lehetőségek, versenyképes hazai tudásbázis létrehozásához kapcsolható.
- Magyarország Digitális Oktatási Stratégiája a fentiekkel azonos indíttatásból fogalmaz meg célokat és intézkedéseket a digitális kompetenciák, tudatosság és tájékozottság, illetve az információbiztonságot elősegítő oktatási és szakképzési szakterületek fejlesztésére vonatkozásában.

- Ezen kívül a 2013. évi L. törvényben megfogalmazott I. fejezet 1. § adminisztratív védelmi intézkedések közé sorolja, a IV. fejezet, oktatás-képzés résznél az NKE képzési tevékenység ellátásával kapcsolatosan;
- valamint a 41/2015 BM végrehajtási rendelet 3.1.7. Tudatosság és képzés c. fejezetben, valamint már 1-es biztonsági osztálytól kötelezővé teszi.

## 2 A KUTATÁS CÉLJAI, HIPOTÉZISEI, MÓDSZEREI

Értekezésem célja, hogy objektív kutatási adatokat vizsgáljak a felmért időintervallumban. Célom, hogy ezek azonosítása révén lendületet vehessen, és kidolgozott megoldási javaslataim révén feloldható legyen az esetlegesen vagy egyes munkaszervezetekben jelentkező fejlesztések és fejlődés gátja. Ezáltal a közigazgatási információbiztonsági szintet követően, mint egyik jelentős összetevőn keresztül, a nemzeti kibertudatossági szint is számottevő és mérhető növekedésnek indulhasson. Ezen kívül bár már az 1996-ban kiadott ajánlás, majd azt követő ajánlás gyűjtemény is foglalkozik az oktatások megszervezésének felelősségével, később ez a 2013. évi L. törvényben és annak 41/2015-ös végrehajtási rendeletében, ez ajánlásból törvényi szintre emelkedik. Azonban ennek megvalósítása munkaszervezetenként eltérő lehet. Az oktatás előtti, (baseline, jelenállapot) és oktatás utáni (megértési, tudatosság, szabálykövetési hajlandóságra vonatkozó, annak változására vonatkozó) mérések elvégzésére nincs előírás, arról nemzeti vagy közigazgatási szintű információkkal nem rendelkezünk. Az egyes közigazgatási szervezetekben elvégzett mérések így szigetszerűek maradnak és nem összehasonlíthatóak. Ugyanakkor, mivel az ajánlásgyűjtemény már 1996 óta a teljes közigazgatás rendelkezésére állt és 2013 óta kötelező érvényű, így feltételezhető, hogy nincs lemaradás információbiztonsági tudatosság, szabályozottság szempontjából. Mindezen előzmények és a nemzetközi szakirodalmi feldolgozás után a humán (soft) tényezők viselkedést befolyásoló tényezőit és a kemény (hard) tényezőként a szabályozást vizsgáltam és mutatom be disszertációmban, megfogalmazott hipotéziseimmel összefüggésben.

A kutatási célok elérése érdekében a kutatásom alapjául szolgáló hipotéziseimet a következőképpen fogalmaztam meg:

H1: Az információbiztonsági tudatossági szintjének tekintetében a magyar közigazgatás területén nem tapasztalható lemaradás a magyar üzleti szférával összehasonlítva

H2: Az információbiztonsági szabályalkalmazás gyakorlata jelenléti oktatás keretében hatékonyabban fejleszthető az írásbeli szabályozáshoz képest

H3: Az információbiztonsági szabályalkalmazás gyakorlata e-learning oktatás keretében fejleszthető.

Disszertációmban kizárólag a Magyarországon elérhető információbiztonsági képzések és minősítések bemutatására szorítkoztam és a magyar közigazgatást és magyar üzleti szférát vizsgáltam. Ennek okai a terjedelmi korlátok, a külföldi mintavétel és felmérés idő és költség korlátai, valamint eddigi oktatási tapasztalataim is a magyarországi szervezetekhez kötődnek. Továbbá a 2013. évi L. tv. által a szakembereknek előírt minősítések is innen származhatnak, így nem releváns más nemzetközi minősítés vagy oktatás mélyebb vizsgálata. A disszertációmban bemutatott összesen 7 darab kutatás értelmezési tartománya kutatásonként eltérő, az viszont kiemelendő, hogy minden esetben kizárólag az adott szervezetekben dolgozó válaszokat adó munkavállalók válaszait tartalmazza, nem pedig minden egyes munkavállaló válaszát. Azaz akár közigazgatáson belül, egyes szervezeteken belül, vagy azok között is lehetnek eltérések, de a minta nagysága révén mégis következtetéseket vonhatunk le, szem előtt tartva természetesen, hogy ettől eltérő, kiugró értékek is lehetnek.

Kutatásom során a jelszókezelést, valamint annak gyakorlatát az információbiztonsági tudatosság, a szabályalkalmazási képesség egyik indikátorának tekintettem. A 3 fő kérdésblokkon belül 72 kérdésre kért a kérdőív különböző válaszokat. A kiértékelés során indexet készítettem a skálás válaszadási lehetőségek egyik csoportjából. Nyolc változót azonos súllyal szerepeltettem a jelszókezelés-információbiztonsági tudatossági indexben, egy esetben pedig transzponáltam a kapott válaszok értékeit, mivel az állítás (*Ritkán változtatok jelszót*) tagadó logikai minőségű volt, illetve információbiztonsági szempontból az egyet nem értés az elvárt attitűd. Ebből a nyolc változóból, annak kiértékeléséből készítettem indexet. Ennek eredményeképpen a közszférában 4,33-as átlagos értéket kaptam, míg az üzleti szférában ennél valamivel magasabb átlagos értéket, 4,38-at az aggregált index értékre. Ezzel kapcsolatban fontos kiemelni, hogy mivel összesített indexről van szó, ezen eltérés rendkívüli, és bizonyítja, hogy a közigazgatásban e tekintetben elmaradás tapasztalható.

Az üzleti és közigazgatási szféra komplexebb összehasonlítása érdekében statisztikai próbákat végeztem. A beérkező adatok feldolgozásához az IBM SPSS statisztikai programcsomagját alkalmaztam. A statisztikai próbák szignifikáns különbségeket mutattak az üzleti és közigazgatási szférában dolgozók válaszai között.

A második hipotézisem keretében azt a kérdést vizsgáltam meg, hogy az információbiztonsági szabályalkalmazás gyakorlata jelenléti oktatás keretében vagy az írásbeli szabályozás keretében fejleszthető-e hatékonyabban, amelyhez a bejelentési esetszámot mint indikátort hívtam segítségül.

Hipotézisem alátámasztása érdekében két külön munkaszervezetnél is volt lehetőségem vizsgálatot végezni, azaz a kiadásra kerülő IBSZ (információbiztonsági szabályzat) és IBP (információbiztonsági politika) kihirdetése előtti és utáni értékek, havi bontásban rendelkezésemre álltak. Ezen intervallumok, azaz az információbiztonsági szabályzat kihirdetése előtti, majd az azt követő értékek, valamint a jelenléti oktatást megelőző és az azt követő trendek, az elvégzett statisztikai próbák alapján szignifikáns eltérést mutattak.

Az e-learning megoldás során a SCORM (Sharable Content Object Reference Model, azaz: megosztható tartalmi objektumok hivatkozási modellje) egyfajta szabvány csomagba importálható, így tetszőleges LMS (Learning Management System, azaz: oktatási keretrendszer) rendszerben lejátszható. A vizsgálat során a Moodle (LMS) rendszert alkalmaztam, mivel az adott vállalatnál az állt rendelkezésre. Az e-learning kurzusoknál a Moodle rendszer által adott lehetőségek kerültek felhasználásra, azonban tutor, vagy egyéb humán erőforrás bevonás nem történt, tehát pusztán elektronikus tartalom volt elérhető a résztvevőknek. Az e-learning kurzusok intranethírként, nem kötelező tananyagként kerültek meghirdetésre. (Pont úgy, ahogy a szabályzatok publikációja történt.) Fontos mozzanat, hogy az e-learning rendszerek alkalmazásához is szükséges előzetesen meglévő IKT-jártasság, így ennek felmérése és az alkalmazás támogatása mindenképp szükséges (Bujdosó 2014).

Az E-mail biztonsági alapok e-learning kurzusnál a sikeres teszthez 80%-os eredményt kellett elérni. A 2.853 kitöltési próbálkozás 2.196 egyedi személyhez tartozott. Az e-learninghez kapcsolódóan, de attól különállóan publikált kérdőívet 902 egyedi válaszadó töltötte ki, értékelte a képzést egy ötfokozatú skálán, valamint megjelölte, hogy miért találta azt hasznosnak. A Jelszóbiztonság kezdő szinten című e-learning tananyaghoz tartozó tesztet 1.976 egyedi kitöltő kezdte el megoldani, 2.902 darab próbálkozás történt. A sikeres teszthez 75%-os eredményt kellett elérni. Az e-learninghez kapcsolódóan, de attól különállóan publikált kérdőívet 901 egyedi válaszadó töltötte ki, értékelte a kurzust egy ötfokozatú skálán, valamint megjelölte, hogy miért találta azt hasznosnak. Az Adathalász támadások elleni védekezés lehetőségei című e-learning tananyaghoz tartozó tesztet 2.667 egyedi kitöltő kezdte el megoldani, 3.454 darab próbálkozás történt. A sikeres teszthez 70%-os eredményt kellett elérni. Vizsgáltam az információbiztonsági szabályzat kiadása előtti, utáni és az e-learning publikáció előtti és utáni időszakokat, valamint a felhasználói bejelentések számával való összefüggést.

A disszertációmban bemutatott kutatás nem a közigazgatás egészére, nem annak minden egyes munkavállalójára kiterjedő mérés, azaz nem tekinthető reprezentatív mintának. Mindazonáltal a vizsgálatból a kérdőív kitöltőire érvényes következtetés vonható le, s egy adott időpontra vonatkoztatva egy megközelítőleg jó, pontos képet kaphatunk belőle.

# 3 AZ ÉRTEKEZÉS FELÉPÍTÉSE ÉS A VIZSGÁLAT LEÍRÁSA

Dolgozatom központi kérdése annak vizsgálata volt, hogy információbiztonsági tudatossági szempontból, hol helyezkedik el a közigazgatási szféra, illetve hogyan lehetséges hatékonyan fejleszteni az információbiztonsági szabályalkalmazási hajlandóságot, és milyen módon használható fel az e-learning az információbiztonsági oktatások során. Az információbiztonsági szabályalkalmazás, a nemzeti kibertudatossági szint fejlesztéséhez nem elegendőek tisztán információbiztonsági (szakmai) válaszok – összetett problémák megoldásához összetett válaszok szükségesek. Az első fejezetben ezek mentén a téma aktualitását és jelentőségét fejtettem ki.

Az második fejezetben megállapítottam, hogy a magyar szakirodalomban még nincs elterjedve az interdiszciplináris megközelítés, így a különböző motivációs elméletekre vagy külföldi kutatók által a témában elvégzett mérésekre való hivatkozást ezen a területen nem találtam. Ugyanakkor ezen új területek, ezen elméletek több, mint egy évtizede már a kutatók látóterébe kerültek.

A szakirodalom feldolgozása után hipotézisem vizsgálatához kérdőíves felmérést alkalmaztam. Ezen felmérés újszerű módszerek felkutatását és felállítását igényelte. A harmadik fejezetben bemutattam kutatásom alanyait és módszereit, amelynek keretében egy saját modellt is kidolgoztam, amely az 5W+1H modellen, azaz Kipling Módszerén alapul. Ez a modell hangsúlyozza, hogy a szabályzatok és a humán tényezők együttes kezelésében látom a fejlesztési lehetőségeket, annak érdekében hogy az információbiztonsági tudatosság egy magasabb szintet érjen el, amely nem csak személyes érdekünk, hanem a KÖZ érdeke is.

A modell egy támogató eszköz lehet az információbiztonsági tudatosság fejlesztési programjához, s abban nyújt segítséget, hogy az egyén, hogyan tudja képzés által hatékonyan elsajátítani az írott szabályozást. Ezt a modellt személyes jelenlétű oktatások során alkalmaztam, többezer fős mintán vizsgálva hatékonyságát. Valamint e modellt alkalmaztam e-learning megtervezéséhez és létrehozásához. Három ilyen e-learning kurzus esetszámait és eredményeit elemeztem többezer fős mintán, s az eredmények igazolták létjogosultságát.

A negyedik fejezetben az önbevalláson alapuló kérdőívekre adott válaszokat többféle statisztikai módszerrel elemeztem. A kérdőív eredményeit felhasználva feltártam a közigazgatási szféra lemaradását az információbiztonsági tudatosság szempontjából az üzleti szférához képest, amit statisztikai módszerekkel is igazoltam. A kutatások eredményeként a kérdőíves vizsgálatokat interjús vizsgálatokkal egészítettem ki, valamint tantermi, élő oktatásokat tartottam, e-learning tananyagot készítettem, és mindezeket teszteltem. A

feltételezésem az volt, hogy a jobb szabályértés, a jobb elfogadás, nagyobb szabálykövetési, alkalmazási hajlandóságot feltételez. A kutatásom eredményei ezt alá is támasztották, ennek oka az lehet, hogy az ember kongruens viselkedése élő szituációban, saját élmény megtapasztalása közben könnyebben változtatható.

A vizsgálat alapján fény derült arra is, hogy a jelenléti, élő oktatás a leghatékonyabb. Fontos szerepe lehet ebben az interaktív visszakérdezési lehetőségnek. Aktív csoport esetében, a régóta bent tartott (fel nem tett, megválaszolatlan) kérdések feltevésével egymást támogatják a csoport tagjai. Míg az e-learning képzés esetén nem volt ekkora mértékű változás kimutatható, azonban más tényezők, megfelelő indikátorválasztás mellett lehetséges a középtávú változások vizsgálata, kimutatása, ha a központi koordináció mellett a mérések és visszajelzések széles közigazgatási körből rendelkezésre állnak. A bevezetett szakszavakra történő későbbi építkezés egy lehetőség, ami jobban befogadhatóvá teszi a szabályalkalmazási gyakorlat további fázisait a megteremtett közös nyelv és alapvetések bevezetését követően.

Az értekezés következtetései és javaslatai - amelyek az ötödik fejezetben találhatóak - magára az információbiztonsági vezetőképzés alapdilemmájára is segíthetnek legalább részben megoldást találni, azaz, hogy hogyan növelhető a közigazgatási információbiztonsági vezetők vezetői hatékonysága. A vezetői hatékonyságot növelheti, ha a mérési eredmények rendelkezésre állnak; kockázatokkal arányosan a célterületen lehetséges eredményeket elérni. Információbiztonsági vezetőként fel lehet használni azokat a tudományos eredményeket, amelyek megmutatják, hogyan lehetséges szabálykövetési hajlandóságot fejleszteni. Az értekezés legfőbb újszerűségét szemléletmódja, a szakirodalom nem pusztán információbiztonságról szóló részének hiánypótló elemzése adja, amely kitágítja a szakterület határait. A kezdetben felvetett kutatási problémát maradéktalanul körbejártam, saját modellt állítottam fel, amellyel megvizsgáltam a tárgykört, s végül megválaszoltam a felvetett kérdéseket.

Disszertációmban azokra a gyökérokokra világítok rá, amelyeknek megértése és feltárása alapja lehet egy olyan transzformációnak, amire szükség van a szokások és mélyben megbúvó, alattomos, rossz gyakorlatok, csoportnormák megváltoztatásához. Egyike ezeknek az információbiztonsági szabályzatok kiadásának menete, azok gyakorlatba való átültetéséhez nyújtott támogatás hiánya.

# 4 ÖSSZEGZETT KÖVETKEZTETÉSEK

Első hipotézisem alapján, azt elvetve, a közigazgatási szférában – összevetve az üzleti szférával – lemaradás tapasztalható az információbiztonsági tudatosság tekintetében.

A tudatosság mérésére a jelszóhasználati szokások kérdőíves felmérését választottam. A jelszó (általánosságban) mint hitelesítési eszköz kiváló indikátora az információbiztonsági tudatossági szintnek, a szabályalkalmazási gyakorlatnak azáltal, hogy kvantifikálható, mérhető, összehasonlítható. Az információbiztonság tekintetében felmerülő bizalmasság, sértetlenség, rendelkezésre állás közül többet, de legalább a bizalmasságot tipikusan valamilyen hozzáférési kontrollal, valamilyen hitelesítést biztosító eszközzel, például jelszóval valósítják meg. Széles körben elterjedt a hitelesítési eszközök használata, talán kijelenthető, hogy nincs olyan hely, ahol ilyet nem alkalmaznak – talán csak publikus információk esetében. Ezért a jelszó alkalmas mind a széleskörű felmérésre, mind pedig – kvantifikációja révén – idősoros mérési pontok előállítására, változása révén az információbiztonsági szabályok alkalmazási gyakorlatában történő változás nyomon követésére.

Megállapítottam, hogy az információbiztonsági tudatosság szintjének tekintetében a magyar közigazgatás területén lemaradás tapasztalható a magyar üzleti szférával összehasonlítva, azaz a H1-t elvetettem.

Az információbiztonsági tudatosság, a szabálykövetési hajlandóság növelése érdekében számos különböző lehetősége van a munkaszervezeteknek, amely nem korlátozódik kizárólag az élő és e-learning, formákra. A számos lehetséges megoldásra, tetszőleges kommunikációs csatornára általánosságban alkalmazható modellt dolgoztam ki. Ezt a modellt alkalmaztam az általam elvégzett mérések során, az élő oktatásban és az e-learning képzésben vizsgált két különböző munkaszervezetben.

A második hipotézisem szerint az információbiztonsági szabályalkalmazás gyakorlata jelenléti oktatás keretében hatékonyabban fejleszthető az írásbeli szabályozáshoz képest, amihez a bejelentési esetszámot mint indikátort hívtam segítségül.

Megállapítottam, hogy az információbiztonsági szabályalkalmazás gyakorlata jelenléti oktatás keretében hatékonyabban fejleszthető az írásbeli szabályozáshoz képest, azaz a H2 hipotézisemet elfogadottnak tekintettem.

Ezt követően a harmadik hipotézisemből kiindulva azt vizsgáltam meg, hogy az információbiztonsági szabályalkalmazás gyakorlata e-learning oktatás keretében fejleszthető-e. Kimutatható-e az általam választott indikátor segítségével a szignifikáns változás?

Vizsgáltam az információbiztonsági szabályzat kiadása előtti, utáni és az e-learning publikáció előtti és utáni időszakokat, a felhasználói bejelentések számával való összefüggést. Statisztikai próbák alapján nem volt kimutatható jelentős eltérés ($F=1,126$, $p=0,303$) a szabályzatpublikáció és az e-learning képzés között a bejelentések számában. A szabályozás nélküli szakaszhoz képest nem vizsgálható az eltérés, mert nincs elegendő adat. Ugyanakkor más lehetséges indikátorokat vizsgálva jelentős volumen változás volt fellelhető.

Bár statisztikai próbákkal nem volt kimutatható korreláció, ugyanakkor hangsúlyoznám, hogy miért is kiemelkedő jelentőségű ezen megfigyelésem. Az adott munkaszervezetben vizsgálva kvantifikálható értékeket: a teljes szabályzattár átlagosan havi 400 darabszámos megnyitásával szemben itt a többezres megtekintésen túl ezres nagyságrendű önkéntes tanulás, majd feladatmegoldás és ezres nagyságrendű visszajelzés volt mérhető. Valamint az önkéntesen, saját belső indíttatásból elvégzett e-learning modul kapcsán a nagyságrendileg háromezer fő által elvégzett tananyagot követően a munkavállalók önkéntesen vizsgát tettek, azt esetenként többször javították, újra elvégezték, és a szintén önkéntes visszajelzésre alkalmas kérdőívet is magas százalékos arányban töltötték ki. A modellem alapján kidolgozott, nem kötelező e-learning képzéssel és a hozzá kapcsolódó tevékenységekkel önkéntes módon sikerült elérni a vizsgált munkaszervezet munkavállalóinak, nagyságrendileg 60%-át. Megállapítottam, hogy az információbiztonsági szabályalkalmazás gyakorlata e-learning oktatás keretében fejleszthető, ugyanakkor ennek eredményeit összevetve az írásbeli szabályozásnál mért eredményekkel, a különbség statisztikailag nem kimutatható szignifikánsan, azaz a H3 hipotézisemet elvetettem. Ugyanakkor kiemelkedő jelentőségűnek tartom, hogy a modellem alapján megtervezett és kivitelezett, javaslataim alapján összeállított (nem kötelezőnek, hanem érdekesnek, magánéleti vetületben is alkalmazhatónak kommunikált) 3 darab különböző, információbiztonsági oktatási tananyagokat nagy volumenben dolgozták fel önkéntesen a résztvevők. További mérések és vizsgálatok keretében érdemes lenne annak kutatása, hogy milyen jelentősége van, hogy az itt óvatosan bevezetett szakszavakra építkezés milyen módon gyorsítja, támogatja, teszi jobban befogadhatóvá a szabályalkalmazási gyakorlat további fázisait. Továbbá lehetséges annak vizsgálata, hogy szükséges-e más indikátort választani vagy egyéb kérdőíves felmérést végezni a jövőben.

# 5 ÚJ TUDOMÁNYOS EREDMÉNYEK

Értekezésemben elsőként felmértem az információbiztonsági szintet a magyar közigazgatási szférában. A szakirodalom áttekintése során fellelt információbiztonsági modellek, valamint

többéves egyetemi és egyéb (SIP) oktatási tapasztalataim alapján kidolgoztam egy saját kérdőívet. Ezen kérdőív három részből állt: egy demográfiai, egy jelszókezelési, valamint egy IKT-jártassági blokkból. Ezen kérdőív segítségével is bizonyítottam, hogy a jelszókezelési szokások (a jelszó mint hitelesítési eszköz kezelése) megfelelő indikátorai lehetnek az információbiztonsági tudatossági szint mérésének. Ennek segítségével részben azonosíthatóak az információbiztonsági kockázatok, a tudásszint és a szabálykövetési hajlandóság. A kérdőívet az azonosítással, jelszókezeléssel kapcsolatos releváns, kiemelkedő kockázatok azonosítására dolgoztam ki. Az azonosított kockázatok alkalmasak lehetnek az információbiztonsági szakemberek számára későbbi hasznosításra, illetve széles spektrumban a teljes közigazgatásban egységes figyelembevételre.

Az általam kidolgozott információbiztonsági kérdőív segítségével feltártam az információbiztonsági szintet a magyar közigazgatási szférában. A felmérést kiértékeltem, és megállapítottam, hogy a közigazgatási szférában az információbiztonsági szint (jelszóhasználat, mint ami az információbiztonság indikátora) tekintetében lemaradás tapasztalható az üzleti szférával összehasonlítva.

A kérdőívet összesen 1.243 fő töltötte ki az üzleti és a közigazgatási szférából. Likert skála, kvantitav értékek és szabadszavas mezők segítségével a kérdőívben demográfiai, információbiztonsági és IKT-jártassággal kapcsolatos kvantifikálható adatokat gyűjtöttem. Egyes változókból összetett indexet képeztem. Egyes skála típusú kérdések, az alkalmazott index és szabadszavas mezők kvantifikálása után mindezen adatok tudományos kiértékelése során megállapítottam, hogy a magyar közigazgatásban információbiztonsági tudatosság szempontjából lemaradás tapasztalható. Tézisem alátámasztására felhasználtam a 2013-as Illéssy, Nemeslaki, Som kutatások nyers adatait is, ezeket az eddig nem kiértékelt, nem publikált adatokat újra kiértékeltem, ami nem támasztotta alá tézisem, és az eredmények pontosabb megértéséhez nyújtott információkat.

Kutatásom során egy általam kidolgozott újszerű modellt alkalmaztam a közigazgatásra.

Kutatásaim során áttekintettem a vonatkozó nemzetközi és hazai szakirodalmat. Számos modellt és környezeti befolyásoló tényezőt azonosítottam, és azzal kapcsolatos kutatásom vonatkozásában a nemzetközi szakirodalmat áttekintettem. Kitértem a modelleken túl olyan okokra és szervezeti tényezőkre, amelyeket eddig a magyar szakirodalomban nem vizsgált még senki. Ennek során azt tapasztaltam, hogy a magyar szakirodalomban számos modellnek és tudományos vizsgálatnak, megközelítésnek említés szintjén sincs nyoma. Ezen újszerű megközelítések és modellek egybevágtak kutatásaimmal és kialakított oktatásmódszertani megfigyeléseimmel. Ezt az újszerű megközelítést, a feltárt szakirodalmi elméleteket és

modelleket alkalmaztam a közigazgatásra a kutatásom során. Hangsúlyozni kívánom, hogy itt a jelentős és pozitív változást az oktatási modell és módszertan kidolgozása és azon túl annak alkalmazása jelenti, amelyet és amelynek mérési eredményeit disszertációmban bemutattam.
Kutatásaim, az NKE EIV-ben való oktatás során gyűjtött kutatási kérdőívem révén, a Safer Internet Programban és üzleti szférában szerzett oktatási tapasztalataim alapján kidolgoztam az információbiztonsági tudatos viselkedés átültetéséhez egy modellt, valamint a modellem alapján egy mintaelőadást. A modellem figyelembevételével készült el három e-learning anyag. Ezen e-learning anyagok alkalmazása, tesztelése, mérése és tudományos kiértékelése megtörtént. Továbbá részben magyar, részben az interdiszciplináris területeken feldolgoztam a nemzetközi szakirodalmat. A humán tényezők viselkedést befolyásoló tényezői közül az alábbiakat vettem figyelembe: a Theory of Planned Behaviour (TPB, A tervezett viselkedés elmélete), a General Deterrence Theory (GDT, Az általános elrettentés elmélete), a Protection Motivation Theory (PMT, A védelmi motivációs elmélet), a Technology Acceptance Model (TAM, A technológia elfogadási modell). Ezek mellett azonban összesen több mint 54 hasonló elmélet létezik, amelyek valamilyen módon magyarázzák az ember szabálykövetési, szabályalkalmazási hajlandóságát, döntési mechanizmusát. Ide sorolhatóak még egyéb interdiszciplináris tényezőként a tudásmenedzsment, a személyes awareness preferenciák, vagy épp az elrettentési, visszatartási modellek is. Kemény (hard) tényezőként a szabályozást vizsgáltam disszertációmban nemzetközi szakirodalmi kitekintéssel. Az információbiztonsági (munkaszervezeteken belüli) szabályozás tekintetében számos javaslatot fogalmaztam meg, amely hatékonyan képes támogatni a szervezeten belüli információbiztonsági (megértési és) szabálykövetési hajlandóságot. Az információbiztonsági szabályzatok ismeretére, ismertségére vonatkozó megfigyeléseim a bemutatott kutatásokban, ahol lehetőség volt kvantifikáltam, bemutattam. Javaslatokat fogalmaztam meg, hogy a szabályzatok kialakítása, bevezetése, kommunikációja és beltartalmuk vonatkozásában milyen, - megfigyeléseim alapján jelenleg és jellemzően nem alkalmazott – szempontokat lenne szükséges alkalmazni, változtatni, fejleszteni.
Így voltaképpen a modellem kialakítása során mindkét területen feldolgoztam a nemzetközi szakirodalmat. Ugyanakkor a szakirodalom számos esetben anonimizált szervezetekről és esettanulmányok bemutatásáról szólt, s nem volt megállapítható, hogy közigazgatási vagy más típusú munkaszervezetről volt-e szó. Általánosságban viszont elmondható, hogy ezek mindegyike számítógépesített munkakörülmények között dolgozó, fehérgalléros munkavállalók bevonásával készült, ahova a közigazgatás is sorolható. Az egyik vállalat esetében, bár rendelkezik gyártókapacitással, azaz olyan munkavállalói is vannak, akik nem

vagy jellemzően nem számítógépen dolgoznak, ezen munkaköröket nem érintette a kutatás, mivel abba csak a számítógéppel rendelkező munkavállalókat vontam be. Így a hasonló munkakörök, számítógépesített fehérgalléros munkakörök miatt mindenképpen releváns a kutatási eredményem a közigazgatás számára is.

Ezen modell alkalmas lehet arra, hogy jelentősen befolyásolja a szabálykövetési hajlandóságot, és így a gyakorlatba ültesse át a szabályzatban megfogalmazott információbiztonsági alapelveket.

Az általam kidolgozott, disszertációmban bemutatott modellt élő és e-learning képzésekre is alkalmaztam. Az alkalmazhatóságát és alkalmazásának eredményeit többezer fős mintán lemértem. Újszerű, nem kizárólag információbiztonsági szempontú, hanem interdiszciplináris megközelítése révén hatékonyabban lehet képes támogatni a tudatossági stratégia, programok, oktatások, tréningek megvalósítását. Olyan eszközöket ad a menedzsment és az információbiztonsági szakterület kezébe, amelyeket alkalmazva jelentős és pozitív irányú változásokat tudnak elérni. A modell lényege, hogy nem kizárólag a szakmai mondanivalóra koncentrál, hanem az azt körülvevő tényezőket is hasonló súllyal kezeli. Így nem csak a Miért? és Mit?, hanem a Hogyan?, Kinek?, Mikor?, Hol?, Ki? és Mérés területek is hasonlóan fontosak az eredmény érdekében. A modell magában foglalja, mondhatni garantálja a mérés és visszacsatolás, a ciklikusság miatt a program sikerét, az információbiztonsági képzés fejlődési lehetőségét.

Az ezen modell alapján kidolgozott mintaelőadásomat nagyságrendileg 4.500 fős mintán teszteltem. Ennek eredményei azt mutatják, hogy a jelenléti oktatás hatékony, a szabályalkalmazási gyakorlatban mérhető eredményeket ér el. Megnőtt a bejelentések száma, tehát a résztvevők tudatosan alkalmazzák az új ismereteket. Viszonylag rövid idő alatt lehet elérni hathatós eredményt; míg e-learning kapcsán ilyen kiugrásokat nem sikerült kimutatni. Elképzelhető, hogy hosszabb távon e-learning, annak bizonyos módozata révén eredményes lehet, bár volumenében nem kecsegtet hasonló hatással.

Bizonyítottam, hogy oktatással fejleszthető az információbiztonsági tudatossági szint és a szabálykövető magatartás.

Bizonyítottam, hogy az általam kidolgozott modell alkalmazása által az információbiztonsági oktatás segítségével az információbiztonsági előírások ismeretén túl a tudatos és szabálykövető viselkedésben is pozitív változás érhető el. Kiscsoportos oktatás előtt és után elvégzett kérdőíves méréssel ezen mintaelőadást nagyságrendileg 4.500 fős mintán teszteltem. Ezen mintán számszerűen kimutatható igazolt hatása volt a felhasználók információbiztonsági tudatossági viselkedésének, hiszen a jelenléti oktatásban résztvevők esetében szignifikánsan

megnőtt az információbiztonsági tudatosság, a szabálykövetési hajlandóság; s a szabályt a napi gyakorlatban alkalmazták. Az e-learning anyagok kidolgozására is alkalmaztam modellem; az így kapott adatokon statisztikai módszerekkel nem volt kimutatható szignifikáns pozitív változás, de a kurzus értékelése, a visszajelzések és a mozgósított létszám tekintetében jelentős áttörés volt.

Compliance Check Distance, (CCD) azaz a nemmegfelelőségi gyakorlatból való kockázat kezelésének kidolgozása járulékos eredmény volt a kutatások során. Amely kezdeti empirikus megfigyelést későbbiekben tudatosan alkalmaztam és vizsgáltam. A CCD alkalmazása (az élő oktatás során biztosított) informális csatorna lehetőségével nagymértékben segítheti a fennálló kockázatok feltárását a szabályozási környezettel való ütköztetése.

A nemmegfelelőségek kezelése lehet előzetes, feltáró, (preventív) illetve utólagos (detektív és korrektív tevékenységek). A szabvány alapján egy-egy tanúsítás elvárja, hogy minden évben nevezzenek meg egy fejlesztési területet. Viszont arra nem térnek ki, hogy mikor mérünk valamit valaminek az érdekében. Valamint a jó mérési eredmény esetén, ha mindent rendben találnak, akkor miért kellene azt újból vizsgálni, miért kellene rajta változtatni? Ha megvan a jól bevált mérés, gyakorlat, illetve a módszer, akkor miért kellene változtatni? De vajon nem lenne-e szükséges megvizsgálni, hogy jó dolgot mérünk-e? Hiszen "észre kell vennünk azonban, hogy egy mérőeszköz sűrűn használt volta önmagában nem biztosíték a megbízhatóságra" (Babbie 2001). Elképzelhető, hogy rossz szemszögből, rossz dolgot mérünk, s lehet, hogy az egész folyamat az audit ellenére hibát tartalmaz. Mindezen alattomosan növekvő kockázat időben történő érzékelésében segíthet az üzleti területről vett, az üzleti folyamatokban már alkalmazott mérési lehetőség. Azokon a területeken, amelyekkel nincs aktív kommunikáció, nincs rendszeres visszacsatolás, még inkább kialakulhatnak olyan folyamatok, amelyeket nem értünk, nem tudunk helyesen mérni, és nem tudjuk feltárni az információbiztonsági réseket. Ezen nemmegfelelőségek kiküszöbölésére is alkalmas lehet a hármas pontban ismertetett modellem (annak alkalmazása a jelenléti oktatásra), amely visszacsatolást is tartalmaz éppen ezen okokból. A compliance ilyen módon történő fenntartása ugyanakkor rendkívül költséges lehet, ha ezt minden munkafolyamatra fel kívánjuk írni, s a formális logika nyelvén rögzíteni szeretnénk az adott rendszerbe egy munkaszervezetnél. Az általam kidolgozott modell nem képes a teljes Governance Risk management és Compliance (GRC - azaz Információbiztonsági irányítás, Kockázatkezelés és Megfelelőség) terület lefedésére és minden kockázat formalizált felírására, azonban a jelentős eltérések időben történő észlelésére alkalmas lehet, oly módon, hogy a modell révén kapott kimeneti

információk a GRC terület, a CCD bemeneti információját képezi, amely így már feltárható és kezelhető.

# 6 A KUTATÁSI EREDMÉNYEK GYAKORLATI FELHASZNÁLÁSA

Az élő oktatás nagyobb bevonódást, jobb megértést tesz lehetővé, mint a pusztán írásbeli szabályzat elérhetővé tétele. Az e-learning tananyag alkalmas a figyelem felkeltésére és az érintettek bevonására, ugyanakkor szignifikánsan nem befolyásolta a szabálykövetési hajlandóságot. Az élő oktatás során, azt követően az informális, kötetlen kérdésfeltevési, tisztázási lehetőséggel jellemzően éltek a résztvevők a vizsgált munkaszervezetekben, míg az ugyancsak rendelkezésre álló, de önállóan (egyénileg, egyedül) kezdeményezhető kérdésfeltevéssel az e-learning során nem éltek. Az e-learning esetében viszont alacsony költségek mellett, gyorsan, rövid idő alatt lehetséges elérni nagy létszámban a célközönséget és alkalmas lehet arra, hogy gyorsan és nagy tömegek számára teremtsük meg az alapokat a későbbi fejlesztéshez. Ezen megállapításokat statisztikai próbákkal is igazoltam. Jelentős változások úgy érhetőek el, ha az oktatás erősebb bevonódás, jobb megértés révén nagyobb szabálykövetési hajlandóságot eredményez. Ennek a változását folyamatosan lehetséges mérni megfelelő indikátorokkal. Kidolgozott modellem mind az e-learningre, mind az élő oktatásra alkalmazható. A közigazgatásban dolgozó információbiztonsági vezetőket támogatva egy egységes oktatási és mérési módszerrel ez jelentős változásokat hozhat.

**A közigazgatási szféra által hasznosítható eredmény**

Jelentős támogatás lehet a közigazgatásban dolgozó információbiztonsági szakembereknek, ha kész modellt tudnak alkalmazni, de még nagyobb, ha ez alapján központilag létrehozott tananyagok állnak rendelkezésre, melyek az adott munkaszervezetekben könnyen megoszthatóak. Valamint, ha hasonlóan elérhetőek a képzések előtti és utáni mérésekhez szükséges eszközök, amelyek így közigazgatási szinten válnak transzparenssé, a fejlesztendő területekre irányítva a figyelmet. A központi koordináció növelheti az eredményességet, mivel a mérések és eredmények nagyobb volumenben összehasonlíthatóak és jobban elemezhetőek, mintha szigetszerűen vagy eltérő, nem összevethető mérések állnak rendelkezésre. A jobb megértés és nagyobb szabálykövetési hajlandóság révén mindez a magánéletben is követendő példaként alkalmazódik majd, így a családtagok, rokonok, ismerősök felé csatornát nyitva a változások átléphetik a szigorúan vett közigazgatási határokat, országos szinten éreztethetik majd hatásukat.

**Információbiztonsági szabályzatok kialakítására vonatkozó eredmények**

Kutatásaim rávilágítottak, hogy az írott szabályzat ismerete, beépülése a vizsgált szervezetekben nem alátámasztott. Szerepkör alapú kivonatok készítése, mint arra a szakirodalom és nemzetközi kutatások is rávilágítottak, nem kellőképpen elterjedt. Gyakorlati eredményként a megfelelő szabályozási környezet vonatkozásában az érintettek bevonása a szabályozási folyamatba, a szerepkör alapú kivonatok készítését mindenképp a kiemelkedő felhasználási lehetőségek között szükséges megemlítenem. A szabályozási környezet kialakításának folyamata, a végeredmény felhasználhatósága szempontjából és azt követően a szabálykövetés hajlandóságra gyakorolt hatása miatt is szükséges kiemelten kezelni.

**Nemzeti szintű változások lehetősége**

A közoktatásban dolgozók oktatási programjában nincs információbiztonsággal kapcsolatos képzés. További gyakorlati felhasználásként információbiztonsági eredményeim bekerülhetnek az alap-, a közép- és felsőfokú oktatásba, s kifejezetten azon egyetemi képzésekbe is, ahol a végzést követően a munkába állók fiatalkorúakkal foglalkoznak. A közigazgatásban dolgozó információbiztonsági felelősök alapképzettsége mellett, rávilágítottam egy nemzetközi minősítési rendszer lehetőségének alkalmazására, amely a magyarországi képzési helyek és egyéb képzések összehasonlíthatóságát is elősegítené. Továbbá modellem alkalmazásával az oktatások hatékonysága, a szabálykövetési hajlandóság növelhető.

# 7 A JELENTŐSEBB PUBLIKÁCIÓK JEGYZÉKE

**Hazai kiadású szakfolyóiratban magyar nyelven megjelent tudományos folyóiratcikk**

1. Som, Z. (2018) CCTV-rendszerek interoperabilitás és információbiztonsági megközelítésben. - In: Magyar Rendészet 17: 2 pp. 159-171.
2. Som, Z.; Papp, Gergely Z. (2016) Tudásfejlesztés a kiberbűnüldözésben – lehetőségek és kihívások. - In: Hadmérnök 11: 2 pp. 170-182. , 13 p.
3. Illéssy, M.; Nemeslaki, A.; Som, Z. (2014) Elektronikus információbiztonság - tudatosság a magyar közigazgatásban. - In: Információs Társadalom: Társadalomtudományi Folyóirat 14: 1 pp. 52-73. , 22 p.
4. Som, Z. (2013) Kibertudatosság mint várható eredmény, a 2013. L. törvény távlati hatásai: Budapesten 2013. október 25-én a Haza Szolgálatában c. konferencián elhangzott előadás szerkesztett anyaga. - In: Társadalom és Honvédelem 17: 3-4 pp. 295-302.
5. Som, Z. (2013) A közigazgatási informatikai felelősök oktatásának kérdései. - In: Hadmérnök 8: 4 pp. 223-237., 15 p.

**Magyar nyelvű könyv, szerzőként**

1. Som, Z. (2014) Kockázatmenedzsment gyakorlat, Budapest, Magyarország: Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet (2014), 93 p.
2. Som, Z. (2014) Biztonság támogatása, Budapest, Magyarország: Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, 66 p.

**Könyvrészlet, idegen nyelvű:**

1. Som, Z. (2014) Laws aiding cyber-security in the EU, In: Alexander, Balthasar; Hendrik, Hansen; Balázs, Kőnig; Robert, Müller-Török; Johannes, Pichler (szerk.) Central and Eastern European eGov Days 2014: eGovernment: Driver or Stumbling Block for European Integration, Wien, Ausztria: Austrian Computer Society, (2014) pp. 115-126.

## 8 SZAKMAI ÖNÉLETRAJZ

Som Zoltán 1978. július 19-én született Kazincbarcikán. Jelenleg Dunaharasztin él családjával, feleségével és négy gyermekével. 1998-ban érettségizett a gödöllői Madách Imre Szakközépiskolában. Majd a Szegedi Tudományegyetemen szerzett matematika, fizika, informatika tanári és programozó matematikus diplomákat. Felsőfokú angol nyelvvizsgája után, amelyet 2017 júniusában szerzett meg, 2020 júliusában megszerezte az alapfokú német nyelvvizsgát is.

2003-ban kezdett el a Szegedi Tudományegyetem Rektori Hivatalában dolgozni, mint informatikus, majd informatikai vezető, nevéhez fűződik a Szenátusi és egyéb Rektori Kabineti anyagok digitális előterjesztésének bevezetése. A nemzetközi jó gyakorlat megismerése érdekében Erasmus program keretében Finnországban, valamint Görögországban is járt ösztöndíjasként. A Szegedi Tudományegyetem Juhász Gyula Pedagógusképző karán, 6 féléven keresztül tanította az általános informatikát.

A Szegedi Tudományegyetem Rektorától 2010-ben a Kjt. alapján maximális pontszámot és "kiválóan alkalmas" minősítést kapott.

A tudományos kutatáson túl Zoltán az elmúlt időszakban számos rangos nemzetközi információbiztonsági minősítést is megszerzett. Megszerezte az ITIL vizsgát. Majd az EC-Council-nál Certified Ethical Hacker minősítő vizsgát tett. Az ISACA két biztonsági minősítését, a Certified Information Security Manager (CISM) és Certified in Risk and Information Systems Control (CRISC) minősítéseket is megszerezte. Ezen túlmenően sikeresen teljesítette a 'Cybersecurity and Its Ten Domain' kurzust, amelyet a Kennesaw State University indított a Courserán. Valamint az ISO 27001 Lead Auditor vizsgát is tett. 2013 és 2018 között a Szegedi Igazságügyi szakértői kamara tagja, informatikai igazságügyi szakértőként.

2013-ban jelentkezett a Nemzeti Közszolgálati Egyetemnek az országban elsőként elindított Közigazgatás-tudományi Doktori Iskolájába, az elektronikus közigazgatási rendszerek biztonsága témakörön belül az információbiztonságot befolyásoló humán tényezőkkel kívánt részleteiben is foglalkozni.

2013-tól a Közigazgatás-tudományi Doktori Iskola doktorandusz hallgatója. PhD tanulmányait az információbiztonság témakörében kezdte meg. A későbbiekben lehetősége nyílt csatlakozni: az ÁROP-2.2.17 Új közszolgálati életpálya projekt Elektronikus Információbiztonsági Szakirányú továbbképzési szak átvilágítása c. kutatási projekthez, amelyben aktív szerepet vállalt. 2014 júliusában doktori szigorlatot tett, majd 2016 decemberében kapta meg az abszolutóriumot.

2015-ben az egri Eszterházy Károly Főiskolán megrendezésre kerülő Doktoranduszok Országos Szövetségének éves „Tavaszi Szél" elnevezésű szakmai konferenciáján, a Közigazgatás-tudományi Szekció I. helyezését nyerte el „Az e-befogadás feltételrendszere és annak fejlesztése és az információbiztonság tükrében" című előadásával.

Nem csak tudományos és szakmai, hanem önkéntes oktatási tevékenységet is végez az információbiztonsági oktatások valamint a közigazgatás területén is számos felkérésnek tett eleget:

Az I. Nemzeti Kiberversenyen a Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar hallgatóiból álló csapat felkészítőjeként 4. helyezést ért el, ezért dicséretben részesült.

Több éve részt vesz az Európai Unió Safer Internet Programjában önkéntes oktatóként.

Valamint számos közigazgatási szervezet felkérésének, is eleget tett. Így a Szolnoki Törvényszék, a Csongrád- Csanád megyei kormányhivatal, a Karcagi Járásbíróság és a Szegedi Törvényszék dolgozóinak is tartott már információbiztonsági előadást.

2013-as indulásától egészen 2020-ig a Nemzeti Közszolgálati Egyetem, Elektronikus Információbiztonsági Vezető szak, szakirányú továbbképzési program óraadó oktatója. Nevéhez fűződik a tudásalapú közszolgálati előmenetel program keretében készült alábbi 2 tankönyv: A biztonság támogatása, valamint a Kockázatmenedzsment gyakorlat.

Kutatásainak eredményeit több cikk és hazai valamint nemzetközi konferencia keretében publikálta. Publikációinak száma 29, amelyből:

5 db magyar nyelven megjelent tudományos cikk;

2 db magyar nyelven megjelent könyv;

5 idegen nyelvű és 7 magyar konferencia előadás;

1 idegen nyelvű és 3 magyar nyelvű könyvrészlet;

6 db egyéb publikáció.