Som Zoltán[315], Erdősi Péter Máté[316], Papp Gergely Zoltán[317], Pólya Balázs[318]:

Információbiztonsági pillanatkép és helyzetértékelés a magyar közigazgatásban.

Különös tekintettel az e-szolgáltatások és e-befogadás, a jelszóhasználati nemzetközi kitekintéssel és az Ibtv. tervezett változásaira, mindezek gazdasági hatására

Absztrakt: A 2013. évi L. számú törvény (Ibtv.) és a Nemzeti Közszolgálati Egyetemen megkezdett Elektronikus Információbiztonsági Vezetőképző szak elmúlt egy évét tekintjük át és elemezzük a tapasztalatok alapján. Célunk megfogalmazni olyan sarkalatos pontokat és javaslatokat, melyek támpontot jelenthetnek a jövőre vonatkoztatva. A jelenlegi Ibtv. változás tervezet kapcsolódik továbbá az Európai Digitális Menetrend „Bizalom és biztonság" elnevezésű 3. pillérét alkotó célok megvalósítását részletező, „Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér" címmel közzétett közös közleményben megfogalmazott, „a kibertámadásokkal szembeni ellenálló képesség megteremtése" prioritáshoz. Mindezek nem csak társadalmi, biztonsági, hanem gazdasági kérdéseket is felvetnek, melyek ilyenformán a jelenlegitől eltérő megközelítést, kommunikációt és tudásátadást is megkívánhatnak. Az új technológiák, melyek beépülnek a hétköznapjainkba, határai elmosódnak, sokkal tudatosabb oktatást, edukációt és kommunikációt igényelnek a szolgáltatók részéről is. Tanulmányunkban rá kívánunk mutatni, hogy a növekvő e-kormányzati infrastruktúra milyen szükséges előzetes felkészítést igényel az állampolgárok és az őket kiszolgáló, az infrastruktúrát kezelő és üzemeltető személyzet és oktatásuk szempontjából. Mindezt elsősorban informatikai biztonsági szempontból megvizsgálva, kitérve azonban az e-szolgáltatások e-befogadására, az e-hitelességre és a gazdasági tényezőkre is. Szükséges rávilágítani olyan kérdésekre is, mint az információbiztonság szintjének mérése, a jelszóhasználati szokások ügye, valamint arra is, hogy a (jelenlegi) viszonylag kis számú szakember képes lesz-e ezeket befolyásolni, képesek lesznek-e a szükséges (társadalmi) folyamatok beindítására a szükséges mértékben.

A téma pontosítása és aktualitása

Az információbiztonság szabályozására a 2013. évi L. törvény (Ibtv.) [1] tett a közelmúltban jelentős lépéseket, amely előírta a képzést és képesítést megszerzését. Erre azonban több évnyi határidőt hagyott, mellyel az érintett szervezetek egyes vélemények szerint éltek, vagy visszaéltek.[319] Másrészről a változások szükségszerűen további területeken is változásokat kell, hogy indukáljanak, hiszen az információ és annak kezelése offline módon vagy elektronikus információs rendszerekben, egész pontosan az információs rendszerek üzemeltetése kevésbé szabályozott, nem kötött hasonló nemzetközi sztenderd szerinti végzettséghez jelenleg. Tehát míg az Ibtv. nemzetközi minősítéshez vagy a Nemzeti Közszolgálati Egyetem Elektronikus Információbiztonsági Vezető (későbbiekben: NKE EIV) képzése elvégzéséhez köti az ilyen pozíció betöltését - türelmi idővel, addig az informatikai rendszerek tervezésére, bevezetésére, üzemeltetésére egyenlőre nem létezik ilyen jellegű megkötés,

[315] Nemzeti Közszolgálati Egyetem, Közigazgatás-tudományi kar, Közigazgatás-tudományi Doktori iskola és a Technológia es Innováció Kutatóközpont PhD hallgató, E-közszolgálati Fejlesztési Intézet, som.zoltan.kdi@office.uni-nke.hu

[316] Nemzeti Közszolgálati Egyetem, Közigazgatás-tudományi kar, Közigazgatás-tudományi Doktori iskola és a Technológia es Innováció Kutatóközpont PhD hallgatója. erdosi.peter.kdi@office.uni-nke.hu

[317] Nemzeti Közszolgálati Egyetem, Közigazgatás-tudományi kar, Közigazgatás-tudományi Doktori iskola és a Technológia es Innováció Kutatóközpont PhD hallgatója. papp.gergely.kdi@office.uni-nke.hu

[318] Humánerőforrás szervező mesterszak, Gödöllő, polya-pub@bnet.hu

[319] Az Ibtv. A 2013. évi L. trv. Az állami és önkormányzati szervezetek információbiztonságáról. Az érintett ezres nagyságrendű szervezetek eddig mindössze 62 főt iskoláztak be az EIV képzésbe.

ajánlás, előírás. Meg kell jegyezni, hogy bár nemzetközi szinten ilyen szabvány létezik (ISO 20000), ennek alkalmazása is számos problémát vet fel. A téma roppant aktuális, hiszen „...tény, hogy közigazgatás megszervezése a mai világban informatikai számítástechnikai eszközök nem lehetséges”[320] a közigazgatásban is egyre fontosabb a mérés, a hatékonyság a naprakész és aktuális információk elérése [10] és a rendszerek közötti automatikus információcsere, általában véve az interoperábilis (együtt)működés[321],[322]. Mindezek nem megvalósíthatók modern információs rendszerek nélkül, melyek fejlesztését EU irányelvek is támogatják, így a közigazgatás kitettsége is ezen folyamatok következményeként értelmezhető és szükségszerűen növekszik.

Általában van jelen a modern világban az információéhség, amelyet társadalmi, gazdasági, geopolitikai vagy egyéb érdekek is erősítenek, táplálnak. Erre 2001-ből jó példa a Magyarországon felfedezett poloska program, de a 2010-es Stuxnet vagy a 2007-ben megtörtént Észtország elleni kibertámadás is egy-egy példa az ismertté vált esetek közül. Egyetlen egységnyi adat, információ vagy akár egy e-mail cím is eladható és értéket képviselhet megfelelő helyeken, amíg a hiteles információ felhasználási kötelezettsége nem lesz általános érvényű előírás. A magyar közigazgatás vonatkozásában vizsgálva az elektronikus hitelesség kérdéskörét, az elektronikus aláírás és az e-ügyintézés bevezetése és elterjedése, főleg annak időbeli lefolyása és hosszú távú következményei vetnek fel komoly kérdéseket. [323]
Kutatásaink alapján kimutatható, hogy az információbiztonsági helyzet egy képzelt és magasabb szinten van a megkérdezettek válaszainak analízise szerint, mint az a mérések alapján kimutatható. Vizsgálatunkat azonban az információbiztonsági helyzetkép méréséből [324] továbblépve új megközelítésben folytattuk tovább: Milyen kompetenciák szükségesek az e-szolgáltatások terjedéséhez, az e-ügyintézéshez állampolgári és szolgáltatói oldalon – célszerűen külön-külön vizsgálva [45].

Az EU irányelvei és Magyarország törekvései egybeesnek abban a tekintetben is, hogy a közigazgatási szolgáltatások elektronikusan elérhetőek legyenek a polgárok számára. Esélyegyenlőség, interoperabilitás: mindenki bárhonnan elérje a szolgáltatásokat, az egyes rendszerek átjárhatók legyenek szolgáltatói és ügyfél szempontból is. Mindezen változások azonban előre nem kiszámítható további változásokat indukálhatnak társadalmi szinten. Maga az elektronikus aláírás, az elektronikus hitelesség és hitelesség-szolgáltatók már évek óta elérhetők, azonban az elektronikus aláírás láthatólag nem terjedt el robbanásszerűen[19]. Így vizsgálatunk ebből a szempontból is felteszi a kérdést, vajon mi szükséges az e-szolgáltatások robbanásszerű elterjedéséhez. Szolgáltatói és szolgáltatás-igénybevevő oldalon külön-külön célszerű ezt a kérdést megvizsgálni. Első körben mindkét területen meg kell vizsgálni a szükséges kompetenciákat. Ezt a vizsgálatot le kellett választani a digitális kompetenciákról, külön kellett megvizsgálnunk. Ennek egyik fő oka az volt, hogy meglátásunk szerint csak az képes az információbiztonságot készségszinten művelni, vagy a (hiteles) elektronikus utat használni, vagy azt ajánlani közszolgálati oldalon a napi gyakorlatban, aki maga is magabiztosan képes azt használni és eligazodik az adott területen. A közigazgatási kutatási tapasztalataink arra mutatnak rá, hogy ez a kompetencia még fejlesztésre szorul az információbiztonság vonatkozásában is [26].
Fontos megemlíteni, hogy mérési módszertan és mérés nélkül azonban nem biztos, hogy megfelelő pontossággal érzékelhető a változás [12], [23], [24]. Így a fejlesztés kidolgozása és megkezdése előtt

---

320 Bukovics István: A fenntartható közigazgatás, fenntartható biztonság elmélete,

321 Som Zoltán, Az információbiztonság újraértelmezése az EU interoperabilitási programja és a gyorsan változó technikai környezetek hatására.

322 Fleiner Rita - Munk Sándor, Közigazgatási adatbázisok összekapcsolásának biztonsági kérdései, http://hadmernok.hu/2012_4_fleiner_munk.pdf, P.:121 Letöltve: 2015.06.01

323 Az e-ID bevezetése kapcsán is, Az egységes elektronikuskártya-kibocsátási keretrendszerről szóló 2014. évi LXXXIII. törvény módosítása.

324 Illéssy Miklós – Nemeslaki András – Som Zoltán: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban, Információs társadalom, Társadalomtudományi folyóirat, 14:(1) pp. 52-73. (2014)

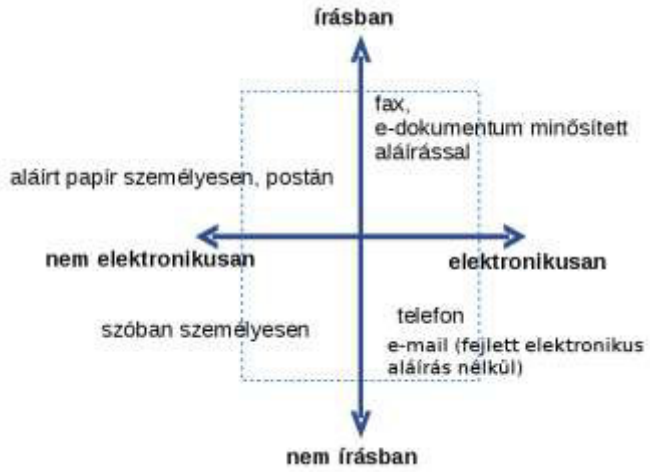
mindenképp fontos az aktuális helyzet metrikán alapuló feltérképezése. Ebből a szempontból az Ibtv. számos szakkifejezésnek megadja a definícióját, azonban az EIV-ben sincs komplex módszertani ajánlás az információbiztonsági tudatossági szint - legalább ordinális, de inkább skaláris skálán történő - mérésére, fejlesztésére.
Az információbiztonság másik jelentős kihívója a hármas paradoxon elvárás, azaz "jót, gyorsan, olcsón". Amely általában valamelyik terület(ek) rovására valósul meg. A gyorsan, vagy olcsón kivitelezett rendszerek fajlagos költsége magasabb lehet hosszútávon. Így még további nyitott kérdései vannak az információbiztonság mérési keretrendszerének [7].

Mottó:
„Amit nem tudunk mérni,
azt nem is ismerjük igazán."
(Harrington)

Közigazgatási e-szolgáltatások, információbiztonság
Az információbiztonság speciális helyzetben van jelenleg. A nemzetközi minősítéssel rendelkező és jellemzően a forprofit szektorban tevékenykedő munkavállalók munkáját anyagilag is jobban elismerik ebben a szektorban. Így voltaképpen a közigazgatási információbiztonság jelenleg és nagyságrendileg 60 kiképzett munkavállalóval számolhat ma Magyarországon. Véleményünk szerint ezen szakemberek szerepe és felelőssége ahhoz hasonlítható, mint amikor a jogi szabályozás megkezdődött a taníttatásnak, tankötelezettségnek és ezzel párhuzamosan növekedett az igény az egyházi, majd később állami tanítókra is. Kétségtelen, hogy történelmi idők ezek, melyek a gyorsan változó világunkban újabb és újabb kihívások elé állítják a terület első, államilag képzett szakembereit.

Ezen szakemberek elsődleges feladata az útmutatás, hiszen a több tucat, vagy alkalmanként több ezer munkavállalót foglalkoztató munkaszervezetekben az ő felelősségük nemcsak az információs vagyon megóvása, és nemcsak az információbiztonsági képzések révén a tudatossági szint emelése. Hanem mindezt olyan módon kell tudnia megvalósítani, hogy mint a legnagyobb munkáltató, a közigazgatás megfelelő és centrális központja kiindulópontja legyen az információbiztonsági tudásnak a munkavállalókon és ezen keresztül szinergikus folyamatokon át széles társadalomi rétegekre is kifejtse a hatását.

Meg kell vizsgálni tehát, hogy mi befolyásolja az e-szolgáltatások nyújtását és igénybevételét? Míg régen ezt a digitális írástudásra vezették vissza, ma már látható, hogy „Összességében a szocio-demográfiai tényezők (nem, végzettség, jövedelem, életkor, településtípus) csak az esetek 12 százalékát magyarázzák." [Döme-Reich, 2011] Ezen kívül vajon milyen tényezők befolyásolhatják a közigazgatási szolgáltatások nyújtását a közigazgatási szolgáltatások igénybevételével kapcsolatban? Mi szükséges a változáshoz, hogy a közigazgatás valóban szolgáltatást tudjon nyújtani – és ezt a szolgáltatást igénybe tudják venni az állampolgárok? Különösen időszerű ez a kérdés számos e-szolgáltatás, például az eID (elektronikus azonosítás) bevezetése kapcsán is.
A kapcsolattartási formákat az elektronikus-írásbeli Descartes-koordinátarendszerben ábrázoltuk.



1. ábra: Kapcsolattartási formák az elektronikus-írásbeli koordinátarendszerben (Forrás: Erdősi Péter Máté)

A mérés tehát kulcsfontosságú, hogy mind az offline és az online területekről képet lehessen alkotni. Azonban ezzel kapcsolatosan a legfontosabb kérdés az indikátorválasztás [2], [28], [23], [24]. Kutatásaink alapján látszódik, hogy a kérdőíves felmérés gyakran célt téveszthet, mert a kérdéseknek próbálnak megfelelni a válaszadók, így az általuk feltételezett jó válaszokat jelölik meg. Szem előtt kell tartani tehát a megfelelő indikátorválasztáson kívül azt is, hogy a mérés maga hogyan befolyásolja a mérendő területeket [23], [24]. Az is látható, hogy az IKT tudást, a tisztán digitális képességeket [6] le kell választani mind az információbiztonság, mind az e-befogadás és az e-szolgáltatások igénybevételének vizsgálatáról. Tehát célkitűzésként megfogalmaztuk, hogy amit szeretnénk mérni, ahhoz válasszunk indikátorokat, de kompetencia alapon - így közelítettük meg ezt a kérdést az adott területeken. Az e-közigazgatások trendjei azonban azt mutatják, hogy egyes területeken további fejlesztések, információk szükségesek a mérés komplex elvégezhetőségéhez, elképzelhető, hogy adattárházak létrehozására lenne szükség [43].

Kompetencia alapú megközelítés

A kompetencia-típusokon belül külön kellett választanunk a technológiai és nem technológiai kompetenciákat, hiszen a digitális kompetencia nem kizárólag technológiai aspektusú. Ezt követően van arra lehetőség, hogy egy összkép alapján vagy munkaszervezeti és egyéni szinten azonosítsuk be azokat a kompetenciákat, amelyek fejlesztése javasolt.

Kutatóként fel kell tenni a kérdést, hogy mi a kompetenciafejlesztéssel elérendő cél, azaz mely célokat képes ez a megközelítés támogatni?

A magabiztosságot a döntéshez (papír vs. digitális szolgáltatás)

Elektronikusan hiteles és biztonságos közszolgáltatás eléréséhez.

Tudatos és biztonságos szolgáltatás, a tudás és tudatosság átadásának képessége a szolgáltatás nyújtás során valamint a munkaszervezeti kultúra fejlesztésének részeként.

Olyan mérési és értékelési rendszer (módszertan) kidolgozása, amely alapján számszerűsíteni, mérni lehet a fejlődést, egyéni és munkaszervezeti szinten. Megfelelő indikátorok választásával.

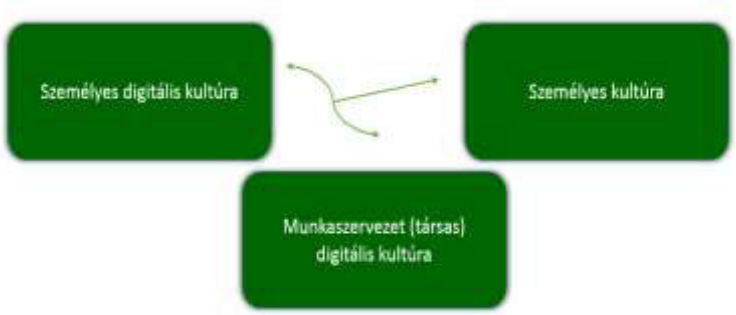
A magabiztos digitális írástudáson kívül további kompetenciák is szükségesek. Hiszen szabályozási alapelvként is megjelenik, hogy – *bizonyos közérdekeket kivéve* – senkit sem lehet kényszeríteni a digitális szolgáltatások használatára, így ez az egyén szabad döntésének kérdése. Természetesen meg lehet nehezíteni különböző mértékben az alternatív útvonalakat, gráfként tekintve az adott célhoz vezető különböző utakra, úgymond azok súlyozásán, útvonalköltségén lehet változtatni – mindaddig, amíg a nehezítés preferenciáit az igénybe vevő és a szolgáltatást nyújtó azonosan értékelik. Akkor

születik arról döntés az igénybe vevőnél általánosságban véve, hogy offline vagy online módon veszi igénybe a szolgáltatásokat, ha az igénybe vevő kompetens, ismeri az ehhez szükséges technológiákat és azokat magabiztosan használni is képes. Ezen kívül a szolgáltató képes a tudás reprodukálására és szolgáltatói szinten a tudás átadására is. Ha ez a kompetencia szolgáltatói oldalon, a munkavállalóban nincs meg készségszinten, akkor ennek esélye, hogy az ügyfélnek az online mód lesz ajánlva, a tapasztalatok szerint csökken.
Tudjuk, hogy eltérő kompetencialisták léteznek a kompetecia-menedzsment tudományában. De számunkra nem is ezek egyeztetése a fontos, hanem azoknak a kompetenciáknak az azonosítása, amelyek fejlesztésével a szolgáltatásközpontú megközelítésben pozitív, növekvő változást érhető el.
Emellett természetesen megfelelő indikátorok is szükségesek ahhoz, hogy a változást (bármilyen irányú is) megfelelő érzékenységgel lehessen mérni, kimutatni. [45], [15]
Minél több online szolgáltatást veszünk igénybe (szolgáltatói – ügyfél oldalon) annál precízebbé válhat a mérés. Természetesen a mérésre is igaz a méretgazdaságosság. Azaz míg a papír alapú szolgáltatások mérése fajlagosan drága - a munkaerő ráfordítás miatt, addig az elektronikus szolgáltatások során keletkező adatok aggregálása egy-egy elemi eseményre vetítve minimális, de mindenképpen kisebb nagyságrendet képvisel.

Kompetenciatérkép

Azon kompetenciák azonosítására, melyek fejlesztésével jelentős változás érhető el a e-szolgáltatások biztonsági és szolgáltatás központú (megközelítésű) innovációjában, úgynevezett kompetenciatérképet szükséges létrehozni. Ezen a térképen, miként a valóságban is, szerepelhetnek közeli és távoli, súlyozottabban figyelembe veendő vagy csak részlegesen fontos területek, kompetenciák is [13]. Sőt, további döntés kérdése, hogy mely kompetenciák milyen módszerrel fejleszthetők és ezek oktatásszervezése hogyan válhat méretgazdaságossá. Ahogy már arról szó volt, kiemelten fontos ezen kompetenciák transzparens különválasztása a digitális és IKT kompetenciáktól. A különválasztást követően az ‘Etnikai-kulturális különbségek’ és a ‘Digitális kultúra különbségek’ összehasonlítása is meg kell, hogy történjen. Többféle térkép (kompetencialista definíció) is létezhet erre nézve. Itt ki kell térni egy jellemző hibára, melyet legkönnyebben az információbiztonsági szabályzat jellemző kialakítási gyakorlatával tudunk szemléltetni. Általános gyakorlat, hogy munkaszervezetenként egyetlen információbiztonsági szabályzat létezik, és ez kerül kiadásra. Amely gyakorlat nem minden esetben nevezhető a célnak megfelelő követendő példának, hiszen a munkaszervezetek különböző típusú, képzettségű és feladatkörű munkavállalókra, szubjektumhalmazokra bonthatók. Jól elkülöníthetők a fizikai beléptetést végző portás, biztonsági őr vagy az irodai munkavállaló, a menedzsmentben dolgozó vagy gyártásban résztvevő beosztottak kompetenciái. A kompetencia (és szolgáltatás) szempontú megközelítés tehát addicionális értéket képvisel, mivel nem feltétlenül munkakörök alapján tagolja a munkavállalókat, hanem egyéni kompetencia térkép alapján képes hatékonyan támogatni a munkaszervezet fejlesztését. Hiszen a digitális kompetenciák elterjedéséhez szükségesek a nem digitális kompetenciák is! Kizárólag a digitális kompetenciák vizsgálatával nem jutunk eredményre! Nem értjük meg, miért nem terjednek el az egyes kompetenciák. Tehát ez nem lehet kizárólag technológiai kérdés, összefüggéseiben kell az elterjedést vizsgálni, melyhez sok esetben ajánlott az adott környezet, munkaszervezeti kultúra és egyéb körülmények figyelembe vétele is. Ha ezt vizuálisan szeretnénk megjeleníteni, akkor a vizsgálandó kulturális kérdéseket hármas csoportba lehet rendezni:

- Személyes kultúra
- Személyes digitális kultúra [6]
- Munkaszervezet (társas) digitális kultúra [18]



2. ábra: Kulturális csoportosítások a kompetenciák megközelítésében (Erdősi – Som)

Kompetencia fejlesztés a közmenedzsmentben

Az elektronikus hitelességgel kapcsolatos kompetenciákat könnyű lenne elintézni azzal, hogy ezek funkcionális (szakmai, digitális) kompetenciák, melyeket tanfolyamokon (például ECDL elektronikus aláírás tanfolyamon [325]) meg kell tanulni és a kompetencia előállott. A KET. hatósági kapcsolattartásra vonatkozó előírásaiban az a kitétel, hogy hatósági ügyintézésben, a kommunikáció során a tisztviselőnek előnyben kell részesítenie az elektronikus utat, felveti a szakmai kompetenciákon túlmutató kompetenciák szükségességét is, hiszen amellett, hogy a tisztviselőnek ismernie kell a technológiát, ezen túl készségszinten és magabiztosan képesnek kell lennie annak használatára, valamint motiváltnak is kell lennie ahhoz, hogy előnyben tudja részesíteni azt [18].

Ezek miatt az elektronikus hitelességgel kapcsolatos kompetenciákat véleményünk szerint - *legalább* - az alábbiak jelenthetik:

- szakmai kompetencia (hitelesség felismerése, készítése, ellenőrzése, megőrzése)
- szociális kompetencia (legyen részese az elektronikusan hiteles digitális világnak, érezze jól magát benne – a hitelesség új dimenziójával együtt)
- innovatív kompetencia (fejlessze az elektronikusan hiteles digitális világot különböző helyzetekben ennek használatával vagy megkövetelésével, vagyis vegye észre és használja ki ezeket a helyzeteket is) [18]

Felmerül a kérdés, hogy hol van ennek a helye, a jelenlegi oktatási, fejlesztési területeken hova illeszthető, milyen oktatási forma lenne a legjobb. Számos nyitott kérdés van még jelenleg, amelyek azonban komplex társadalmi kérdéseket vetnek fel. Így ezeket nem is feltétlenül érdemes lokálisan és különállóan kezelni, de ezekre hatékony válaszokat szükséges adni. Ennek egyik legfőbb oka, hogy életünk és a közigazgatás területein is nem csak egyre több helyen vannak jelen az információs rendszerek, hanem egy mélységi változás is megindult ezeken a területeken. Azaz a rendszerek összetettebbekké váltak, így sokkal mélyebb és specifikusabb tudást igényel a megfelelő minőségű ember – információs rendszer interakció.

A személyes digitális kultúra részhalmaza a személy kultúrájának. Abban kell tehát segíteni, hogy az egyén kultúrájába minél jobban képes legyen beilleszkedni a feladatellátáshoz és a hétköznapi élethez is szükséges előzetesen azonosított kompetencia-halmaz. Természetesen számos nyitott kérdés van még itt is. Viszont a kérdés olyan nagyságrendű és horderejű, amely megítélésünk szerint össztársadalmi és nemzetgazdasági jelentőségű is egyben. Ennek egyik oka, hogy Rice szerint a legnagyobb hatás a társadalom egészére a közigazgatáson keresztül lehet gyakorolni [63]. Ennek oka az érintett embertömegből, annak létszámából következik. Valamint a kompetenciák fejlesztésével az ember-ember és szolgáltató-ügyfél kapcsolatokon történő direkt és indirekt ismeretátadással is (ezek különböző társas-társadalmi csatornák). A jelenlegi képzésekben nem ismerünk olyan gyakorlatorientált oktatást, ahol a kulturális- és kompetencia-különbségek áthidalására és a másik fél fejlesztésére vonatkozó jó gyakorlatot (best-practice) alkalmaznák.

[325] ECDL Elektronikus hitelesség, elektronikus aláírás modul http://www.njszt.hu/ecdl/syllabus/elektronikus-hitelesseg-elektronikus-alairas

A szociális érzékenység, a másik segítése, a másik elfogadása, a másik fejlesztése jelentős részben egyéni (szervezeti) kompetencia kérdése [18], [19]. Ennek fejlesztése egyéni-munkaszervezeti-társadalmi szinten fontos, hiszen a gyorsan változó és egyre inkább elektronikusan elérhető szolgáltatások megismerése, annak megismertetésére való törekvés már nem történhet (és nem is történik meg jelenleg az) iskolarendszerű képzésben [33], így csak ilyen indirekt tudásátadással lehet felvenni a megfelelő fordulatszámot a változások, a fejlődés gyorsaságával. A tudás átadásának sebessége és színtere jelentősen megváltozott az elmúlt évtizedekben és ez különösen tetten érhető az információs rendszerek használatával kapcsolatban [53]. Tapasztalataink alapján, amit a EU Safer Internet Programban közreműködve mértünk fel, már általános iskola 4. osztályától ajánlott tudatosító oktatásokat szervezni és ilyenen résztvenni [54]. Ennek oka, hogy itt sikerült azonosítanunk egy olyan váltást, hogy ettől az életkortól kezdődően szignifikánsan több gyermek rendelkezik internetképes – okos – eszközzel [33], [53], [54]. Ugyanakkor országos szinten viszonylag kevés iskola veszi igénybe a program nyújtotta ingyenes oktatási lehetőséget.

Jelszóhasználati, információbiztonsági kutatás - eredmények, javaslatok

Kutatásaink igazolták, hogy az egyéni és munkaszervezeti kultúra döntően befolyásolni képes a munkaszervezeti információbiztonsági szintet. Ezt számos tényező befolyásolja mind kompetencia, mind magánéleti, mind munkaszervezeti és szabályozási nézőpontokból tekintve is. A szabályozás önmagában nem indukál kompetenciabeli változásokat, erre jó példa a jelszóhasználati szokások vizsgálata és következtetései is. Ilyen irányú kutatásunk alapján látszódik, hogy 15 év alatt nem történt nagyságrendi elmozdulás a jelszóhasználat terén, a szabályozás fejlődésével ellentétben[54]. Tehát önmagában a szabályozás csak egy tényező, a tudás és a szükséges kompetencia lehet az ami működővé teszi a rendszert, a célhoz igazítva. A jelszóhasználati szokások tehát értékes indikátorai az információbiztonság, pontosabban az egyéni információbiztonsági kultúra, illetőleg a szervezeti információbiztonsági kultúra és gyakorlat elemzésének[4]. Az e-befogadás vonatkozásában viszont még ennél is tovább kell menni, tehát a szabályozáson, a tudáson (hogy miért szükséges ez, ennek használata) és a kompetencián kívül a magabiztos használat, a komfortzónán belülre tolódás teszi valóban élővé az adott eljárást. Az e-befogadás biztonságtudatos és magabiztos használatot is jelent egyben. A fentiek kiegészítéseként, részben összegezve az eddigi információkat, azonban ez nem lehet egyetlen célja valamilyen folyamatnak, sokkal inkább valamilyen függvény határértékeként lehet rá gondolni, amelyre a konvergencia kritériumok alapján időpontokhoz kerül definiálásra a küszöbszám. Ezek a küszöbszámok már lehetnek célok, melyek mérhetők, időhöz és munkaszervezethez, valamint egyénhez rendelhetők. Ennek hiányában bármilyen nagyszerű eredmény csak az adott időpillanatban lesz értelmezhető, így a lemaradás jelzőjeként és a fejlődés megrekedéseként lehet rá kizárólag gondolni. Ennek oka, hogy a fentiekben foglalt információs rendszereken, eljárásokon és kompetenciákon túl maga a tudás is avul. Ezen avulás mértéke, nagysága, azaz a változás gyorsasága jelen információink és tapasztalatunk alapján gyorsul, így nem rögzíthető egyetlen cél, csupán (soha el nem érhető) határértékként tekinthetünk a folyamatcélokra. A nemzetközi és hazai tapasztalatok is ezt támasztják alá. A szükséges IKT képességek változnak, a szervezett és automatizált (programozott) ‚bűnözés' és átverős programok egyre 'intelligensebbek', így az ezek kivédésére készített algoritmusok és tudásfejlesztések csupán a létező formákat képesek lekövetni, utólag. A kérdés vagy feladat tehát nem a megelőzés, bár a fentiekben említett küszöbszámok és fejlesztési célkitűzések meghatározása önmagában preventív és jelentős eredménynek számít a biztonság terén. Sokkal inkább a működési struktúra megteremtése és egyes időpontokhoz rendelt küszöbszámok vizsgálatakor annak szükségszerű finomítása a feladata az információbiztonságnak. Ez azonban nem lehet kizárólag állami feladat, sokkal inkább az információs rendszerek mintájára, mint ahogy azok is minden platformon az élet minden területén megjelennek, a felelősség és annak felvállalása, a feladat is meg kell, hogy jelenjen más területeken is. A megoldási javaslatok kidolgozása, a szerepvállalás kiszélesítése perspektíva-váltást hozhat ezen a területen.

Amíg nem magabiztos a tudás, nem mindenki mozdul ki szívesen a komfortzónájából. Ha az első

próbálkozás nem volt sikeres, akkor ennek esélye tovább csökken, ahogyan az R.S. Nadler 1993-ban kidolgozott komfort-zóna modelljéből levezethető. Érdekes és kontraindikatív megállapítást ezzel kapcsolatosan, hogy ezek szerint a fejlődéshez, az új tudás megszerzéséhez az egyénnek ismeretlen területre – saját komfortzónáján kívülre – kell hatolnia, hogy oda visszatérhessen a tanultak magabiztos alkalmazása révén – ez tehát nem jöhet létre kizárólagosan a komfortzónán belül maradva.

Az a cél fogalmazható meg ezzel kapcsolatosan tehát, hogy a szolgáltatást nyújtó magabiztos tudással rendelkezzen a digitális ügyintézés minden területén, továbbá képes legyen elfogadni az eltérő digitális kultúrával rendelkező ügyfelek különbözőségeit és támogatni legyen képes őket a döntéshozatalban.

Különösen aktuális ez a 2016 januárjától induló e-ID bevezetésének vonatkozásában, hogy minden érintett tisztában legyen a következő alapfogalmakkal, azok között magabiztosan tudjon a napi szintű ügyintézése között választani, döntéseket hozni, lehetőleg a saját komfortzónáján belül. Nem valószínű, hogy kényszerrel meg lehet tanítani az elektronikus ügyintézést állampolgárok milliói számára.

Alapfogalmak

A hitelesség fogalomrendszerében megkülönböztetik a hiteles, hitelesítés és hitelesség fogalmakat, az alábbi módon:

- hitelesítés: az állított azonosság megerősítése
- hitelesség: a forrás ismert és a tartalom eredeti
- hiteles: a forrás és a tartalom eredetisége megerősítetté vált

Ezekből a definíciókból az következik, hogy az önmagában megtett állítás sosem számíthat hitelesnek, mert azt minden esetben további tevékenység (megerősítés, verifikálás) révén nyerheti csak el, így nincs „önmagában való hitelesség”. Ebből elvégezhető az információk osztályozása a hitelesség szempontjából:

1. **hiteles információ:** a forrás és a tartalom eredetiségének ellenőrzését elvégezték, aminek az eredménye pozitív és hozzáférhető.
2. **hitelesíthető információ:** a forrás és a tartalom eredetiségének ellenőrzését nem végezték még el, de ennek semmi akadálya nincsen, az érvényesítési adatok rendelkezésre állnak, és a hitelesítés bármikor elvégezhető.
3. **nem hiteles információ:** egyrészről a hitelesítés során negatív ellenőrzésre jutott információt, másrészről az érvényesítési adatokkal nem rendelkező információt nevezzük nem hiteles információnak
    a) **hamis információ**: a forrás és a tartalom eredetiségének ellenőrzését elvégezték, aminek az eredménye negatív (nem eredeti a forrás vagy megváltozott a tartalom) és az ellenőrzés eredménye hozzáférhető
    b) **nem hitelesíthető információ:** a forrás és a tartalom eredetiségének ellenőrzése nem végezhető el, mert a teljes körű ellenőrzéshez szükséges egy vagy több érvényesítési adat nem áll rendelkezésre.

Ezeket a definíciókat a következő ábrában foglaljuk össze és jelöljük az állapotváltozások dinamikáját is.

3. ábra: Hiteles és nem hiteles információ (Forrás: Erdősi Péter Máté)

A hiteles információból akkor lesz hitelesíthető, ha változás következik be az érvényesítési adatokban vagy magában az információban, de az ellenőrzést még nem végezték el. A hitelesíthető információból nyilvánvaló módon lesz hiteles, amint a sikeres ellenőrzést elvégezték. Azonban ha az ellenőrzéshez szükséges egy vagy több érvényesítési adat eltűnik, akkor az információ átkerül a nem hitelesek közé, míg ha felbukkan olyan érvényesítési adat, mellyel a hitelesítés mégis elvégezhető, ebben és csak ebben az esetben lesz a nem hiteles információ hitelesíthető.
Keletkezésüket tekintve az információk lehetnek hitelesíthetők és nem hitelesíthetők, a hitelesítés eredménye teszi őket hitelessé és nem hitelessé. A hitelességnek a jelentősége az elektronikus ügyintézésben mutatkozik különösen meg [19]. Mindezen döntések és a döntés meghozatalához szükséges tudás implicit módon jelen volt eddig is a mikro hétköznapokban, és elemi eseményeinkben, magánéletben vagy munkahelyi környezetben is. El kellett dönteni rákattintunk-e valamire, elindítunk-e egy ismeretlen programot, milyen új jelszót választunk, stb. Azonban a változás sebessége és a hiteleség iránti igény explicitté válása felerősíti ezek jelentőségét.

Mottó:
„A mérés kulcsfontosságú.
Ha nem tudunk valamit mérni,
akkor nem tudjuk irányítani.”
(Robert S. Kaplan, David P. Norton)

Lehetséges megoldások: szükséges teendők és várt eredmények

A téma összetettsége és aktualitása jól érzékelhető, melyet tovább árnyalnak és erősítenek az aktuális magyarországi változások is. Az adatok és információk pénzt és értéket képviselnek, így mind az automatizált és tömeges visszaélések, mind a célzott információszerzés révén bevételforrási lehetőséget jelenthetnek bizonyos csoportoknak. Ez a két fő halmaz pedig mindenkit tartalmaz, aki valaha is kapcsolatba került információs rendszerrel, róla vagy vele kapcsolatban bármi elektronikus úton tárolásra került, tehát létezik digitális lábnyoma[326].
Ezen kívül EU gazdasági és nemzetgazdasági szinten is mérhető hatása van az információs rendszerekkel szorosan összefüggő területeknek, például az e-kereskedelem, távközlés stb. [52]. És bár az Ibtv. számos alapfogalmat tisztázott és definiált, mégis további befolyásoló tényezők tisztázása, feltérképezése válhat szükségessé, így az információbiztonsági tervek mintájára ennek időszakos felülvizsgálata szükséges. Vannak területek, ahol egyes országokban már léteznek jó

[326] Napjainkban születendő gyermekek egyik első digitális lábnyomának tekinthető a legelső ultrahangfelvétel.

gyakorlatok, jórészt az ottani kulturális és munkaszervezeti körülményekre adaptálva. Így a nemzetközileg már használt módszertan implementálásának vizsgálata a hazai körülményekre jó és nagyon aktuális kutatási terület lehet. A jelszóhasználati kérdőív, amely ezer fő feletti (többségében egyetemista) kitöltőnél tart jelenleg, az mutatja, hogy a jövő munkavállalói tekintetében - bár használják az információs rendszereket, de - a biztonságtudatosság nem mutat szignifikáns fejlődést. Részlegesen hasonló állítás fogalmazható meg az e-befogadás és az ehhez szükséges kompetenciák vonatkozásában is [53], [34].

A vizsgált területeken, (információbiztonság, e-befogadás, kompetencia térkép) pontos mérés nem lehetséges, helyette kritikus indikátorok és tényezők azonosítása - azaz indikátorválasztás lehet az előrelépés kulcsa. A témának nemzetközi szinten azonban már politikai vonatkozása is lehet, hiszen az események (esetleges támadások tapasztalatai) és annak megosztása, valamint az esemény- és az információátadás, illetve az információáramlás sebessége változó lehet. A belföldi helyi fejlődéshez így sokkal inkább azonosítani kell azokat a piaci szereplőket - kicsit az Ibtv. mintájára - akik az adott szektorban szolgáltatnak, de nem végzik el a látens módon pedig szükségessé váló ismeretterjesztést és oktatást, vagy ez nem kellőképpen transzparens. Az ajánlások megfogalmazása nagyon ajánlott eleme a megvalósításnak, például szolgáltatók kötelezettségei, tipikus visszaélési lehetőségekre ellenlépések, awareness, szélesebb kör megszólítása vonatkozásában. Természetesen mindezekre lehetőséget kínál az oktatási rendszer az EIV-ben részt vettek által, ahogy egyébként a törvény elő is írja az ebben való kötelező részvételt. Azonban másik oldalról is meg kell közelíteni a kérdést és erre megoldási javaslatunk szintén létezik. Az előzőekben bemutatott modellünkhöz hasonlóan azt ajánljuk, hogy a szolgáltató vállaljon nagyobb részt ebből a feladatból. Például az adott bankkártyák elleni leggyakoribb visszaélési támadási formák elleni védekezési ismeretek (a felkészítés, a tájékoztatás) legyen hangsúlyosabban a pénzügyi szolgáltató feladata, kötelessége. Végső soron a védelem törvényben foglalt normatíva és ennek további kontrollja, illetve az állampolgárok védelme egy kiberkonfliktusban jelenleg állami felelősség [33]. Ugyanez analóg módon megvalósítható máshol is, ahol szolgáltatást nyújtanak (pl. telekommunikációs vagy más területen). A szolgáltatónak a megfelelő tájékoztatás, ismeretátadás járulékos kötelezettsége kell, hogy legyen, törvényi szabályozással. Így kialakulhatnának azok a white-paper ajánlások, melyeket a szektor nagyobb képviselői (akár közösen) állítanának össze a leggyakoribb (legnagyobb számú) visszaélések eliminálására [34]. Terjedelmi okokból csak egyetlen további példára szorítkozva, a törvénykezési egységesség megteremtése is fontos. Tehát amíg az adatvédelem előírja a szolgáltatónak, hogy milyen adatalanyi hozzájárulás szükséges a személyes adatok kezeléséhez, addig arról már nem rendelkezik, hogy az ilyen esetekben (pl. webes regisztrációk, hírlevél feliratkozások, vagy vásárlások alkalmával) milyen szintű biztonságot kell az ügyfélnek biztosítani, vagy tőle elvárni, például a jelszó hosszúsága, jelszó tárolása, adatok tárolása, terén. Így könnyen elképzelhető (kizárólag elvi szinten), hogy egy-egy ilyen szolgáltató a több ezres – tízezres adatbázisát és a hozzájuk kapcsolódó jelszavakat is nyílt szövegként (plaintext) tárolja [54], ami biztonsági szempontból erősen kifogásolható. Az egységes white-paper és best practice létrehozása az adott szolgáltatói szektorban egységes alapot teremthet, és a szolgáltatók számára is elegendő az, ha az adott témát lehivatkozzák (pl.. Jelszóválasztási ajánlás). Míg más eltérő területeken, amelyek egyediek, természetesen egyedi lehet a felelősség és a feladat is. Azonban ki kell mondanunk: a szolgáltatói szektornak is felelőssége van az ismeretek átadásában, a kompetenciák fejlesztésében. Az LLP-t nem elegendő egyetlen bemeneti ponton egyszer megtartani, mint valamilyen képzést, ez a fejlődés része kell, hogy legyen, annak fenntartása érdekében [46], [47]. Ez egyaránt érdeke a szolgáltatónak és az államnak, valamint természetesen az állampolgárnak is. Tehát míg a kultúra (tudás, képzettség és tapasztalat; skill, knowleadge and experience) azt mutatja, hogy nem éri el az optimális hatásfokot, nem elegendő a képzés önmagában, ha az nem válik készségszintűvé. Feltehetjük a kérdés, hogy a jelenlegi frontális oktatási módszertan mennyire képes ennek megvalósítására. Először ennek megválaszolásához azonban fel kell térképezni, hogy milyen kompetenciákra van szükség és ehhez kell hozzárendelni a képzési, fejlesztési programot. Ennek indoka az, hogy a személyes digitális kultúra az részhalmaza a személy kultúrájának, így jelen tanulmány:

a) felsorolja a kompetencia-típusokat

b) megállapítja, hogy a digitális kompetencia nem kizárólag technológiai aspektusú
c) és meghatározza azokat a komptencia-típusokat, melyeket fejleszteni javasolt az elektronikusan hiteles és biztonságos közszolgáltatás eléréséhez (innovatív stb.)

Ezek fejlesztése pedig a közmenedzsment oktatás feladata [18]. Végső soron pedig a felmérés és kompetenciatérkép létrejöttének további várt hozadéka lehet a személyek etnikai-kultúrális különbségeinek hasonlítása a digitális kultúrában létező különbségekkel (digital gap). A digitális kompetenciák kulcskompetenciáknak számítanak ma az informatikafüggő világban. Az elektronikus hitelességgel a különböző kompetencia-modellek parciálisan foglalkoznak, de szükségessége nyilvánvalóan kiderült és megfogalmazódott. A teljesen elektronikus közigazgatási ügyintézésben az elektronikus hitelesség esszenciális, aminek különböző formái létezhetnek. A köztisztviselő akkor tudja előnyben részesíteni az elektronikus írásbeli formákat a többivel szemben, ha nemcsak megtanulja ezek alkalmazását technikai képességként, hanem innovatív módon szociális érzékenységgel is használja ezt az élet minden területén.
Ehhez az infrastrukturális feltételek léteznek ma Magyarországon, azonban ennek a kompetencia alapú humán erőforrás menedzsmentben lényegi nyoma jelenleg nincsen. A közeljövő feladatai között javasolt ennek is szerepelnie, az e-közigazgatás fejleszthetősége és nagyobb hatékonysággal történő alkalmazása érdekében.

Köszönet
Jelen tudományos cikk létrejöttéhez nagymértékben hozzájárul, ezét köszönetüket fejezik ki a szerzők Prof. Dr. Nemeslaki Anrdásnak, Dr. Krasznay Csabának, Dr. Muha Lajosnak. Valamint köszönik a megjelenési lehetőséget a 6. Báthory–Brassai Konferenciasorozat (2015) szervezőinek, ahol az előadást követő rengeteg kérdés arról tett tanúbizonyságot, hogy a téma érdekes és nagy érdeklődésre tart számot tudományos berkekben is.

Referenciák

[1] 2013. évi L. trv. az állami és önkormányzati szervezetek információbiztonságáról
[2] Ágh Attila, Kaiser Tamás és Koller Boglárka (szerk.): Többemeletes vagy többsebességes? A differenciált integráció változatos formái az EU-ban. 2013
[3] András Nemeslaki, Péter Sasvári: Empirical Analysis of Information Security Awareness in the Business and Public Sectors of Hungary, In: Alexander Balthasar, Blaž Golob, Hendrik Hansen, Balázs Kőnig, Robert Müller-Török, Alexander Prosser (szerk.), Central and Eastern European e|Dem and e|Gov Days 2015: Time for a European Internet?. Konferencia helye, ideje: Budapest, Magyarország, 2015.05.07-2015.05.08. Wien: Austrian Computer Society, 2015. pp. 405-418.
[4] Andreasson, Kim. Cybersecurity: Public Sector Threats and Responses. Auerbach Publications, 2012.
[5] Anusca Ferrari, Editors: Yves Punie and Barbara N. Brečko: DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe. European Commission, Joint Research Centre, Institute for Prospective Technological Studies. JRC83167 report. 2013.
[6] Brenda Eschenbrenner: Towards a Model of Information Systems User Competency. Dissertations and Theses from the College of Business Administration, University of Nebraska – Lincoln. 2010.
[7] Brotby, W. Krag, and Gary Hinson. "Chapter 3-The Art and Science of Security Metrics".PRAGMATIC Security Metrics: Applying Metametrics to Information Security. Auerbach Publications. 2013.
[8] Budai Balázs Benjámin, Kőnig Balázs, Törley Gábor, Orbán Anna: Elektronikus Közigazgatás szervezés, közigazgatási technológia, Budapest: Nemzeti Közszolgálati Egyetem, 2012. 138 p.

[9] Budai Balázs Benjámin: Az e-közigazgatás elmélete, második átdolgozott kiadás. Akadémiai Kiadó, 2014. ISBN 978 963 05 9498 1. pp.108-109
[10] Bukovics István: A fenntartható közigazgatás, fenntartható biztonság elmélete
[11] Cserny Ákos, Nemeslaki András: Az e-szavazás lehetőségei és korlátai Magyarországon In: Cserny Ákos (szerk.) Választási dilemmák: Tanulmányok az új választási eljárási törvény nóvumai és első megmérettetése tárgyában. 262 p. Budapest: Nemzeti Közszolgálati Egyetem, 2015. pp. 237-262.
[12] Darrell Huff, How to Lie with Statistics
[13] Defining the Core Competencies. Leadership Development Program, 2012. University of California, Berkeley
[14] Department Of Defense Law Of War Manual, US Department of Defense published, http://www.defense.gov/pubs/Law-of-War-Manual-June-2015.pdf
[15] Dr. Szabó Szilvia PhD: Kompetencia alapú emberi erőforrás gazdálkodás. Nemzeti Közszolgálati Egyetem, Budapest, 2014. ÁROP–2.2.21 Tudásalapú közszolgálati előmenetel. ISBN 978-615-5491-15-3. p.23.
[16] Dr. Venkatesh. J, Ms. Aarthy. C: Information Technology Research Model for Enhancing Ability of Business Managers. 2012. International Journal of Emerging Technology and Advanced Engineering (www.ijetae.com). ISSN 2250-2459, Volume 2, Issue 4, April 2012. pp.263-264. [17] ECDL Elektronikus hitelesség, elektronikus aláírás modul http://www.njszt.hu/ecdl/syllabus/elektronikus-hitelesseg-elektronikus-alairas
[18] Erdősi Péter Máté: Elektronikus hitelesség az e-közigazgatási kompetencia-menedzsmentben, megjelenés alatt
[19] Erdősi Péter Máté: Magyar bizalmi szolgáltatások felügyeletének összehasonlító elemzése
[20] Fleiner Rita-Munk Sándor, Közigazgatási adatbázisok összekapcsolásának biztonsági kérdései, http://hadmernok.hu/2012_4_fleiner_munk.pdf p.121 Letöltve: 2015.06.01
[21] GoI-UNDP Project: 'Strengthening Human Resource Management of Civil Service': Competency Dictionary for the Civil Services. Letöltve: 2015. április 26., http://persmin.gov.in/otraining/Competency%20Dictionary%20for%20the%20Civil%20Services.pdf
[22] Hadarics Kálmán: Nyílt forráskódú szoftverek sebezhetőségeinek vizsgálata
[23] Havasi Éva, Az indikátorok, indikátorrendszerek jellemzôi és statisztikai követelményei, 2007
[24] Havasi Éva, Burjánzó számok, mutáns adatok
[25] Herold, Rebecca. Managing an Information Security and Privacy Awareness and Training Program, Second Edition. Auerbach Publications. 2011
[26] Horváth Katalin, Kőnig Balázs, Orbán Anna, Törley Gábor, Orbán Anna (szerk.): A közigazgatási informatika alapjai, Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., 2013. 198 p. (ISBN:978-615-5344-08-4)
[27] Illéssy Miklós – Nemeslaki András – Som Zoltán: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban, Információs társadalom, Társadalomtudományi folyóirat, 14:(1) pp. 52-73. (2014)
[28] Kaiser Tamás, Hatékony közszolgálat és jó közigazgatás–nemzetközi és európai dimenziók
[29] KET: 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól, kihirdetve 2004. december 28-án.
[30] Kiely, Laree, and Benzel, Terry (2006). "Systemic security management. Security & privacy."IEEE 4, no. 6:74–77.
[31] Kirsti Ala-Mutka: Mapping Digital Competence: Towards a Conceptual Understanding. European Commission, Joint Research Centre, Institute for Prospective Technological Studies. JRC67075 Technical Notes. 2011.
[32] Kovács Zoltán (2012): Felhő alapú informatikai rendszerek, mint nemzetbiztonsági kihívás. A 2012. május 24-én a Nemzeti Közszolgálati Egyetemen rendezett Nemzetbiztonsági kihívások, nemzetbiztonsági szolgálatok c. szakmai konferencián elhangzott előadás szerkesztett változata. Hadtudomány, 2013(1-2). 5-12.p.

[33] Krasznay Csaba, Gabos Erika (szerk.): Önkéntes oktatási tapasztalatok a Biztonságosabb Internet Programban, Konferencia helye, ideje: Balatonalmádi, Magyarország, 2013.09.25-2013.09.27. Budapest: Nemzetközi Gyermekmentő Szolgálat Magyar Egyesület, 2014. 5 p., (KOBAK Könyvsorozat) VII., A média hatása a gyermekekre és fiatalokra, (ISBN:978-963-89962-0-6)
[34] Krasznay Csaba, Szádeczky Tamás: Az információbiztonság és állami szabályozása, In: Nemeslaki András (szerk.), E-közszolgálatfejlesztés: Elméleti alapok és tudományos kutatási módszerek. 353 p., Budapest: Nemzeti Közszolgálati Egyetem, 2014. pp. 249-264. (ISBN:978-615-5491-04-7)
[35] Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban, HADMÉRNÖK VII:(4) pp. 142-151. (2012)
[36] Muha Lajos: Az informatikai biztonság mérése
[37] National e-Government Division, Ministry of Communication and Information Technology, Government of India: eGCF Simplifying Capacity Building – e-Governance Capacity Framework for Digital India with Implementation Toolkit. December, 2014
[38] NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems
[39] OECD: Gazdasági Együttműködési és Fejlesztési Szervezet (Organisation for Economic Co-operation and Development)
[40] Olsina, Luis, and Rossi, Gustavo (2002). "Measuring Web application quality with WebQEM."IEEE Multimedia 9, no.4:20–29.
[41] Orbán Anna: A közigazgatási informatika oktatásának egyes aspektusai, PRO PUBLICO BONO: MAGYAR KÖZIGAZGATÁS; A NEMZETI KÖZSZOLGÁLATI EGYETEM KÖZIGAZGATÁS-TUDOMÁNYI SZAKMAI FOLYÓIRATA 2013:(3) pp. 111-120. (2013),
[42] Orbán Anna: Az e-közigazgatás back- és front-office rendszerei, In: Budai Balázs Benjámin, Kőnig Balázs, Törley Gábor, Orbán Anna, Elektronikus Közigazgatás szervezés, közigazgatási technológia. 138 p., Budapest: Nemzeti Közszolgálati Egyetem, 2012. pp. 21-37.
[43] Orbán Anna: Az e-közigazgatási kutatások trendje: Áttekintés a nemzetközi és hazai irodalmak alapján, In: Doktoranduszok Országos Szövetsége, TAVASZI SZÉL Absztraktkötet 2015. Konferencia helye, ideje: Eger, Magyarország, 2015.04.10-2015.04.12. [hiányzó városnév]: Publio Kiadó, 2015. pp. 281-282., (ISBN:978-963-397-702-6)
[44] Orbán Anna: Success of Online Enrolment System, In: Alexander Balthasar, Blaž Golob, Hendrik Hansen, Balázs Kőnig, Robert Müller-Török, Alexander Prosser (szerk.), Central and Eastern European e|Dem and e|Gov Days 2015: Time for a European Internet?. Konferencia helye, ideje: Budapest, Magyarország, 2015.05.07-2015.05.08. Wien: Austrian Computer Society, 2015. pp. 565-577.
[45] Országos Kompetencia Mérés-Szójegyzék. Letöltve: 2015. április 26. https://www.oktatas.hu/pub_bin/dload/kozoktatas/meresek/OKM_szojegyzek.pdf
[46] Som - Papp, Informatikai bűnesetek, vagy bűnesetek ahol informatikai eszköz van, Kriminálexpo, HISEC, 2014
[47] Som Zoltán, Az információbiztonság oktatási kérdései: igények és lehetőségek, NKE KDI Kutatási Fórum, 2014
[48] Som Zoltán, Az információbiztonság újraértelmezése az EU interoperabilitási programja és a gyorsan változó technikai környezetek hatására. 2013
[49] Som Zoltán, Biztonság támogatása, egyetemi jegyzet, ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel, 2014
[50] Som Zoltán: Az információbiztonság oktatási kérdései: igények és lehetőségek? In: Bende Zsófia (szerk.) A NEMZETI KÖZSZOLGÁLATI EGYETEM KÖZIGAZGATÁS-TUDOMÁNYI KAR KÖZIGAZGATÁS-TUDOMÁNYI DOKTORI ISKOLÁJA 2013/2014-ES TANÉVÉNEK KUTATÓI FÓRUMA: tanulmánykötet. 132 p. Konferencia helye, ideje: Budapest, Magyarország, 2014.05.15 Budapest: Nemzeti Közszolgálati Egyetem, Közigazgatástudományi Kar, 2014. pp. 69-77. (ISBN:978-615-5305-52-8)
[51] Som Zoltán: Cyber security legislation in the EU, p. 1. p. Magyarország, poszter, http://www.nispa.org/files/conferences/2014/posters/Zoltan-SOM_Cyber-security-legislation-in-EU-Poster-NISPAcee-2014-Budapest.pdf (2014)

[52] Som Zoltán: 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. 419 p. Konferencia helye, ideje: Budapest, Magyarország, 2014.05.08-2014.05.09. Wien: Austrian Computer Society, 2014. pp. 115-126. Som Zoltán: A NAT és a biztonságos internetoktatás kapcsolata, kibertudatosság különböző színtereken, In: Gabos Erika (szerk.)

[53]A média hatása a gyermekekre és fiatalokra. VII.. 424 p. Konferencia helye, ideje: Balatonalmádi, Magyarország, 2013.09.27-2013.09.28. Budapest: Nemzetközi Gyermekmentő Szolgálat Magyar Egyesület, 2013. Paper kibertudatosság. (Kobak könyvsorozat; 9.), (ISBN:978-963-89962-0-6)

[54]Som Zoltán: Az internet veszélyei és ajánlás ennek kezelésére, elsősorban a tizenéves általános iskolások vonatkozásában. MÓDSZERTANI KÖZLEMÉNYEK: TANÍTÓK ÉS TANÁROK SZÁMÁRA 2012-53:(2) pp. 21-32. (2013)

[55] Som, Papp: Hungarian trends of password usage, in an international comparison, Ceegov 2015

[56] Sophie Op de Beeck, Prof. Dr. Annie Hondeghem: Managing Competencies in Government: State of the Art Practices and Issues at Stake for the Future. 2011. p121. (letöltve: 2015. május 4.), http://www.planejamento.gov.br/secretarias/upload/Arquivos/seges/arquivos/OCDE2011/OECD_Managing_Government.pdf

[57] Stefani, Antonia, and Xenos, Michalis (2009). "Meta-metric evaluation of ECommerce-related metrics."Electronic Notes in Theoretical Computer Science 233:59–72.

[58] Susan White Perry: Social Equity for the Long Haul: Preparing Culturally Competent Public Administrators. Dissertation submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Public Administration/Public Affairs. 18 November 2005. (Letöltve: 2015. május 4.), http://scholar.lib.vt.edu/theses/available/etd-11282005-141500/unrestricted/SLWPerryDissertation.pdf

[59] Szabó Szilvia: A vezetői kompetencia-fejlesztés tapasztalatai és lehetőségei egyes rendvédelmi szervek hivatásos állománya körében, Doktori (PhD) értekezés, 2008. Zrínyi Miklós Nemzetvédelmi Egyetem, Hadtudományi Doktori Iskola, p.11.

[60] Szakács Gábor: Az emberi erőforrás gazdálkodás fejlesztésének elméleti kérdései a magyar közszolgálatban - „Tudásalapú közszolgálati előmenetel" című 2.2.21 kódjelű ÁROP projekt II. pillére, amely a doktori iskolák tananyagainak fejlesztését teszi lehetővé. Nemzeti Közszolgálati Egyetem, Közigazgatás-tudományi Kar, Budapest, 2014. pp.10-11.

[61] The Tyranny of Numbers – Why counting can't make us happy. HarperCollins Publishers Limited. London. 2001.

[62] Tipton, Harold F., and Micki Krause. "Chapter 46 - Beyond Information Security Awareness Training—It Is Time To Change the Culture". Information Security Management Handbook, Sixth Edition, Volume 1. Auerbach Publications, 2007.

[63] Rice, Mitchell F.: A post-modern cultural competency framework for public administration and public service delivery. The International Journal of Public Sector Management, VoL. 20 No. 7, 2007. pp622-637.