NEMZETI KÖZSZOLGÁLATI EGYETEM

Közigazgatás-tudományi Doktori Iskola

Holló Krisztina

A biztonságtudatosság hiánya, mint kockázati tényező vizsgálata
különös tekintettel az adatvédelmi és információbiztonsági szabályok alkalmazására

Doktori (PhD) értekezés

TÉZISFÜZET

Témavezetők:

Dr. Leitold Ferenc

főiskolai tanár

Dr. Péterfalvi Attila

egyetemi docens

Budapest, 2022.

TARTALOMJEGYZÉK

1. A TUDOMÁNYOS KUTATÁS

1.1. A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

Az információs rendszereket ért incidensek nehezíthetik a mindennapos életet, a gazdasági tevékenységek gyakorlását, jelentős pénzügyi veszteségeket, valamint bizalomvesztést és súlyos károkat okozhatnak az európai közösségnek és a gazdasági tevékenységeknek egyaránt. Az értekezés célja a biztonságtudatossági hiány hatásának vizsgálata, továbbá a kockázati tényezők értékelése, elsődlegesen az adatvédelmi és információbiztonsági területre, illetve a hazai információbiztonsági tudatosság hiányának kezelésére vonatkozóan. Az értekezés címének behatárolását és témájának dogmatikai szűkítését szolgálja az adatvédelmi és információbiztonsági szabályozási kérdések korrelációijának hangsúlyozása. Az értekezés hátterében végzett kutatásom alapvetően a közigazgatás-tudomány területére fókuszál, szükségszerűen érinti az informatikai és a jogtudomány azon területeit, amelyek az eredmények szempontjából relevánsak, ugyanakkor a közigazgatás tudományterületeken elért eredményként terjesztem elő. A választott kutatási terület komplex és több tudományterületet érintő sajátossága tekintetében további behatárolás és pontosítás szükséges. Az értekezés súlypontját meghatározva, a biztonságtudatosság hiányára vonatkozó vizsgálatokat elsődlegesen az információbiztonsági tudatosság hiányára, valamint kiterjesztve az adatvédelmi és információbiztonsági alapelvek és szabályok összefüggéseire, alkalmazására, tudatosítására és információbiztonság-tudatosságnövelési program alapján a tudatosítási szintek vizsgálatára, a hiány okozataként megvalósuló incidensek tényezőire, ezek információbiztonsági kockázatkezelésére és információbiztonsági tudatosság összefüggéseire, valamint vonatkozó intézkedési típusok hatékonyságára összpontosítottam. Az értekezés eredményeinek megállapításaihoz szükséges eszközök és igazolások tekintetében fókuszba kerültek az adatvédelmi és információbiztonsági incidensek gazdasági aspektusai, az információbiztonsági kockázatkezelésnél alkalmazott módszerek, az információs társadalom sajátosságai és az európai digitális kultúra fejleszthetőségének módjai, ugyanakkor ezen témák volumenüket tekintve kizárólag a kutatás igazolásának forrásai vagy eszközei, a háttérkutatás részét képezik.

Összegezve, az értekezés a hazai információbiztonsági tudatosság helyzetére, a hiányának sajátosságaira, azok következményeire és pótlásának lehetőségeire keresi a választ, különösen a releváns folyamatok mely tényezőiről és eredményeiről beszélhetünk az adatvédelmi és információbiztonsági, valamint az információbiztonsági tudatosítási folyamatok és kapcsolatok tekintetében. Az említett folyamatokhoz igazodva, az értekezés szerkezetét tekintve az európai és hazai adatvédelmi és az információbiztonsági történeti és szabályozásának vonulatából, valamint a biztonságtudatosság, különös tekintettel az információbiztonság és az információbiztonsági tudatosság helyzetéből kiindulva, szűkítő jelleggel jut el az adatvédelmi és információbiztonsági jogalkotás és a digitális kultúra fejlesztésének igényéig.

1.1.1. A KUTATÁS HÁTTERE ÉS A TÉMA AKTUALITÁSA

A hírközléstechnika megjelenésével és fejlődésével egy olyan technikai és kulturális forradalmi változás ment végbe, ami egészen egyedi, továbbá az információelmélet megalkotásával 1948-ban egy új korszak született az információvédelem terén. Az információ és a tudás szerepe meghatározó a gazdaság és a társadalom életében, így napjainkban a felgyorsult társadalmi, gazdasági, technológiai fejlődés folyamatai ezt a szerepet folyamatosan alakítják. Fontossá vált a gyors, biztonságos elektronikus információáramlás és a támogató folyamatok, technológiák rendelkezésre állása, az egyéni tudás megszerzése, terjesztése, fejlesztése, mind a versenyszférában, mind a közigazgatásban egyaránt. Az információs rendszerekre épült világunk oly mértékű, hogy szabályozási rendszer is társult mellé, így különösen az információbiztonsági szabványok vagy az európai általános adatvédelmi rendelet (GDPR). Az információ, valamint a digitális adat, és a köré épített technológia elválaszthatatlanok. A számítógép, az informatikai alkalmazások, rendszerek és hálózatok nemcsak a technológiai fejlődés aktuális állapotát tükrözik, hanem adataink védelmét is szolgálják. Ebben az értelemben nincs rangsor, *csak néhány,* nélkülözhetetlen, alapvető tényező, aminek a magja az információ és az adat, a lényege az adatbiztonság és az adatvédelem, amely a legfejlettebb informatikai megoldást kíván minden szinten. Kutatási témámat és gyakorlati megvalósítását a fentiekben említett adatvédelmi és információbiztonsági problémakörre építettem.

1.1.2. A KUTATÁS TÉMÁJA ÉS CÉLJA, A TÉMAVÁLASZTÁS INDOKLÁSA

Az informatika kiemelt szerepét tükrözi az elektronikus kormányzati tevékenység létrejötte, a közigazgatás-tudományhoz való kötődése. Az információs rendszereknek biztosítania kell az elektronikus információ rendelkezésre állását, biztonságos kezelésének lehetőségét és sértetlenségének megőrzését, amely napjaink információbiztonsági területének jelentős alapelve. Kutatási témaként az adatvédelmi és az információbiztonsági szabványi, jogszabályi eszközök felmérését, az információbiztonság szintjének meghatározására irányuló felmérések elemzését, és a felhasználói információbiztonsági tudatosság fejleszthetőségének vizsgálatát választottam. A rendelkezések vizsgálatának szempontjából a GDPR, Infotv. és IBtv., valamint szabvány szempontjából a ISO/IEC 27001 szabványra fókuszáltam, minden további, kevésbé releváns előírás kizárólag a háttérkutatást segítette, esetlegesen a hipotézisek igazolásához szükséges. A vonatkozó jogszabályok és a szabványok tételes vizsgálata nem része az értekezésnek. A témához szorosan kapcsolódik az információs rendszer működtetése során alkalmazandó adatvédelmi és információbiztonsági alapelvek és szabályok, az információbiztonsági kockázatkezelés, valamint a a felhasználói magatartás kihasználhatóságának elemzése. A kutatási témám érinti az információ történeti áttekintését, az információbiztonság és vonatkozó jogintézményeit és azok fejlődését, az adatvédelmi és információbiztonsági szabályozással kapcsolatos rendelkezéseket és ajánlásokat, az

információs rendszerek a felhasználói közösség számára biztosított lehetőségeit, az információs adatvagyon kezelését, különösen a személyes adatok körét, a felhasználói tevékenységet, az információs rendszerek működését befolyásoló cselekedeteket, a kártékony tevékenységeket, és az azokat előidéző tényezőket. Kutatásom során az adatvédelmi és információbiztonsági alapelvek és szabályok teljesülésén túl, mintegy kapcsolódó témakörként a felhasználói biztonságtudatos viselkedést, saját, valamint információbiztonsággal foglalkozó vállalatok, illetve intézmények által lefolytatott kockázatfelmérésből származó adatokat vizsgáltam. Kutatásom során nem foglalkoztam a kiberbiztonság és kibervédelem fogalom szerinti tényezőinek, az adatvédelmi és információbiztonsági incidenstípusok teljes vizsgálatával, ugyanakkor a kutatási témakörökhöz példaként adatvédelem és kibervédelem területéről származó eseteket és statisztikai adatokat prezentáltam annak érdekében, hogy az adatvédelmi és információbiztonsági rendelkezések jogalapját igazolhassam. Az incidensvizsgálat fókuszában a személyes adatokra vonatkozó adatvédelmi jogsértések, legfőképp adatszivárgás, adatlopás vagy adatvesztés, illetve *néhány* kártékony kódtípus által okozott incidens áll, amely során sérül különösen a titoktartás kötelezettsége, az adatok hozzáférhetősége vagy az integritás. Az információbiztonsági szabályozás (IBtv., ISO/IEC 27000) nagy területet foglal magába. Az értekezés terjedelmére vonatkozó korlát miatt nem foglalkozom különösen a belső szervezetet, a fizikai és környezeti biztonság, vagy a szállítói kapcsolatok, működésfolytonosság (BCP) biztosításának területével, és részben érintem az információbiztonsági szabályokat, az emberi erőforrás biztonságát, hozzáférés-felügyeletet (felhasználói felelősségek, rendszer és alkalmazás-felügyelet), titkosítás intézkedéseit, üzemeltetés biztonságát, kommunikáció biztonságát, rendszerek fejlesztését és karbantartását (kapcsolódó téma az interoperabilitási képesség kialakítása és fenntartása), információbiztonsági incidensek kezelését, megfelelést (vonatkozó jogszabályok, szellemi tulajdonjogok, magántitok és személyhez köthető információk védelme, titkosítási intézkedések) és információbiztonsági vizsgálatokat. A disszertációban megemlítem a kutatásom során lefolytatott információbiztonsági kockázatkezelés eredményeit, amelyhez kapcsolódik néhány, az információbiztonsági vagyonelemek kezelésére vonatkozó intézkedés. Az elmúlt öt évben folytatott információbiztonsági elemzéseim és ebből származó statisztikai adataim felhasználásával további vizsgálatokat folytattam a biztonságtudatos magatartás területén, amelynek során felhasználtam az informatikai rendszerekre és a környezetünkre gyakorolt hatástanulmányokat is. Ezáltal az értekezés tartalmaz néhány évnél régebbi, de a kutatási tevékenység szempontjából elengedhetetlen hatósági statisztikai adatokat és hivatkozásokat. A kutatási témám csak részben foglalkozik a felhasználói aktivitást kihasználó informatikai jellegű támadások körével, valamint az informatikai technikai megoldásokkal, ugyanakkor fontos megjegyezni, hogy ezek a tényezők hatással vannak az adatvédelmi szabályozásra és technikai megoldásokra, az információbiztonsági szabályozásra és kockázatkezelésre, valamint a humán faktorra egyaránt. A kockázatmenedzsment tekintetében az

értekezés részét képezi a releváns fenyegetések, a támadási kísérletek vagy az incidensek elemzéséhez és kezeléséhez szükséges módszerek, de ezekre vonatkozó bővebb kutatások közlése nem része az értekezésnek. Jelen értekezésben az informatikai technológiai megoldásokkal, mint például az ipari forradalmak vívmányai vagy a mesterséges intelligencia meghatározásával, illetve megoldásaival, valamint támadási formák részletesebb definiálásával és bemutatásával nem foglalkozom. Az értekezésnek nem témája az adatvédelmi, az információ-, valamint az információbiztonsági kategóriák, alapelvek, szabályok és események teljes palettájának felsorakoztatása és vizsgálata. Kutatás szempontjából fókuszba kerültek egyes felhasználói csoportok, így legfőképp az általános felhasználó, adatkezelő, adatfeldolgozó, rendszerüzemeltető, valamint az egyetemi hallgató, illetve közoktatás tanulója. Ezen csoportok meghatározása és vizsgálata az incidensek általi megközelítés révén történt, mint az incidens közvetett vagy közvetlen okozója, illetve lehetséges elszenvedője. A kor és a nem meghatározása e vizsgálat szempontjából lényegtelen. Az Információbiztonsági tudatosság gyakorlat egyetemi jegyzet (NKE) keretében megfogalmazott Információbiztonsági tudatosság program rámutat a felhasználói szintek jelentőségére, ugyanakkor a COVID-19 által kötelezően bevezetett távoktatási módszerek alkalmazása és azok tapasztalata a digitális kompetenciaigényeket teljes mértékben átírta. A gyerekek, és az átlag, nem informatikai szakterületen tanult, felsőfokú szakképesítéssel nem rendelkező felhasználók általában nem rendelkeznek azon informatikai és információbiztonsági képességekkel, amelyekkel megnyugtató módon, megfelelő szintű digitális képességgel biztosítani lehet a távoktatás háttértámogatását. A pandémia kényszerén tanulva, a gyermekeket is fel kell készíteni a virtuális világ veszélyeire, nemcsak használatának előnyeire. A rendszernek ezen hiányosságait a tapasztalatok alapján javítani szükséges, nemcsak azért, mert már az első osztályos gyermekek is okostelefont használnak, hanem mert „az adott szervezet általános felhasználóinak”, azaz az adott általános iskola felhasználóinak minősülnek. Jelentős felhasználói réteg azon nyudíjasok köre is, akik a különösen a magyarországi központi azonosító (ügyfélkapu) vagy banki rendszerhez felhasználói hozzáfésrést kapnak. Az értekezésben csak azon felhasználói szintek kerülnek vizsgálat alá, amelyek az adott esemény, adat és dokumentumvizsgálat alapján kutatásom tekintetében a statisztikai mintavétel része, ezáltal például a nyugdíjasok körének vizsgálata nem része az értekezésnek, ugyanakkor az általam megállapított általános felhasználói szint (továbbiakban ÁFSZK modell) körébe tartozik. A polgárok biztonságtudatos viselkedését a saját képességeken túl befolyásolja az információs rendszer állapota, fejlettsége, megbízhatósága, valamint a kibertér adta hacker szereplőinek aktivitása, az általuk okozott kár, a jogsértések mértéke. A támadások megelőzésétre létrehozott többféle online oktatás, útmutató, valamint adatvédelmi állásfoglalás segíti a felhasználói közösséget a biztonságtudatos magatartás erősítésében. A közszolgáltatási rendszerek fejlesztése tekintetében az egyik jelentős cél, egy olyan rendszer kialakítása, amely megvalósítja a különböző közszolgáltatási szintek kiegyenlített, hatékony és

biztonságos együttműködését. A közszolgáltatási információbiztonság témához kapcsolható a Magyary Zoltán Közigazgatás-fejlesztési Program, mivel egyes fejezeteiben az információbiztonsági vonatkozások is szerepet kaptak. Az adatvédelmi és információbiztonsági jogszabályi előírások megvalósulását belső és külső kontroll folyamatokkal ellenőrizhetjük, így a rendszerauditok, az oktatási visszacsatolás által nyújtott eredmények megmutatják a kezelendő területeket, illetve a gyenge pontokat és a javítandó állapotokat. Az emberi tényező biztonságtudatossági hiányosságait kihasználó, jól felépített pszichológiai megtévesztési, támadási módszereket és technikákat 2008. óta vizsgálom. Az értekezés kísérlet arra vonatkozóan, hogy a feltételezések igazolásához szükséges információbiztonság, a közigazgatás és a magánszféra adatvédelmének jelenlegi helyzetét bemutassam, az információbiztonsági tudatosság szempontjából elemezhessem és az információbiztonsági tudatosság és az adatvédelem, illetve az információbiztonság közti összefüggéseket feltárhassam annak érdekében, hogy az információbiztonsági tudatosság hiánya, a kockázati tényezők és fejlesztési lehetőségek megállapításra kerüljenek, és ezáltal a magyarországi digitális kompetenciafejlesztést támogassam.

1.2. AZ ÉRTEKEZÉS FELÉPÍTÉSE

Az értekezés fő témája az információbiztonsági tudatosság helyzetének és fejlesztési lehetőségeinek vizsgálata, amelyhez szorosan kapcsolódik az információtörténeti és adatvédelmi jogtörténeti áttekintés, információbiztonsági események és statisztikai adatok elemzése, információbiztonsági kockázatkezelés, valamint a „*humán faktor”* és a digitális kompetencia fejlesztését befolyásoló tényezők áttekintése. Az értekezés figyelembe veszi az információtörténeti és adatvédelmi jogtörténeti szempontból a preindusztriális, indusztriális és a posztindusztriális társadalom formális jellemzőit, továbbá főirányként az információ-, és az adatvédelemmel kapcsolatos jogintézmények kialakulását, a szerzői jogtól az adatvédelemig és az információbiztonságig, továbbá az adatvédelmi és információbiztonsági szabályozás terén az emberi jogok és alapvető szabadságok védelméről szóló római Egyezményt (EJEE), a napjainkban érvényes és hatályos, a téma szempontjából releváns hazai és Európai Uniós adatvédelmi és információbiztonsági jogszabályi rendelkezéseket (1950-2021. időszakra vonatkozóan), továbbá az adatvédelmi és információbiztonsági események, felmérések statisztikai adatait (ENISA), valamint a vonatkozó hatósági határozatokat (Nemzeti Adatvédelmi és Információszabadság Hatóság, a továbbiakban NAIH) és az incidensekből és hazai statisztikai adatokból (Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet, a továbbiakban NBSz NKI) eredő következtetéseket (2000-2021. időszakra vonatkozóan), az információbiztonsági kockázatfelmérés és kockázatkezelés statisztikai adatait és következtetéseit (2015-2021. időszakra vonatkozóan), a balesetek „*humán faktorra*” vonatkozó vizsgálatok és kutatási adatait (1990-2020. időszakra vonatkozóan), a digitális kompetencia fejlesztésére vonatkozó követelményeket (2017-2021. közötti időszakra vonatkozóan). A disszertáció kutatási

dokumentumainak feldolgozását és összegzését 2022. február hónap végén, az előbírálatok szerinti módosítást 2022. augusztus hónap elején fejeztem be, a következtetéseket és hipotézis igazolásokat, valamint a tudományos eredményekre vonatkozó megállapításokat a 2022. március hónap végén rendelkezésemre álló statisztikai adatok és dokumentumok alapján fogalmaztam meg. A fentiekben megfogalmazott főirány szerint alakítottam ki a fejezeteket, igazoltam a hipotéziseket és állapítottam meg a téziseket.

1.3. A TÉMA VIZSGÁLATÁNAK HIPOTÉZISE

A kutatás során az alábbi hipotéziseket fogalmaztam meg.

- Az első hipotézisem (H1) szerint feltételezem, hogy a Magyarországon érvényes adatvédelmi és az információbiztonsági alapelvek és jogszabályi rendelkezések fejlődése a nemzetközi szabványügyi intézmények ajánlásaival és az európai szabályozással összhangban vannak.
- A második hipotézisem (H2) szerint feltételezem, hogy a felhasználói információbiztonsági tudatosság hiánya elősegíti az adatvédelmi jogsértések bekövetkezését, ezáltal kiberbűnözést.
- A harmadik hipotézisem (H3) szerint feltételezem, hogy a Magyarországon érvényes adatvédelmi és az információbiztonsági alapelvek és rendelkezések tudatosítása hatékonyan befolyásolja a felhasználói információbiztonsági tudatosság fejlődését.
- Az negyedik hipotézisem (H4) szerint feltételezem, hogy az információbiztonsági tudatosítás rendszerét nemcsak az informatikai oktatásban, hanem minden korosztály számára elérhetővé kell tenni és minden szakterületen indokolt bevezetni és működtetni.

Az értekezésem végeredményéül kapott állításokkal erősíteni szeretném azt a feltevést, hogy az adatvédelmi és információbiztonsági alapelvekre épített felhasználói biztonságtudatosság növelése nagymértékben hozzájárul az információs rendszereink – különösen a hazai közszolgálati rendszerek – megerősítéséhez, míg a hiánya vagy gyengesége növeli az információs rendszereink gyenge pontjait, ezáltal az információs rendszer sérülékenyebbé, kihasználhatóbbá válhat.

1.4. A KUTATÁS SORÁN ALKALMAZOTT MÓDSZEREK

A kutatásom során többféle módszert alkalmaztam, különösen dokumentum- és tartalomelemzést (információtörténet és jogtörténet feldolgozása, adatvédelmi és információbiztonsági jogtényezők vizsgálata, általános és összehasonlító jellegű kronologikus elemzés, nemzetközi és hazai adatvédelmi irányelvek, alapelvek és törvények, valamint nemzetközi információbiztonsági ajánlások vizsgálata során, a második fejezetben), kvalitatív és kvantitatív módszereket (ISMS vizsgálatok esetében - minőségirányítás módszerekkel, a második fejezetben), összehasonlító elemzést (nemzetközi és hazai jogszabályok vizsgálatánál a második fejezetben), statisztikai adatok elemzését, valamint adatbázis vizsgálatot (kockázatkezelésnél), empirikus kutatást (az észszerűség, a matematikai logika alkalmazásával, valamint az objektívitásra és pontosságra törekvő

megfigyeléssel), továbbá kutatás szempontjából releváns fogalommeghatározást (információbiztonság témakörében). Kutatásom konzekvens fogalomhasználatot kívánt, ezért szükségesnek tartottam bemutatni és meghatározni a kapcsolódási pontokat. Tekintettel arra, hogy kutatásom során az információbiztonsági tudatosság hiányát, kiváltó tényezőit és következményeit vizsgáltam, a digitális kompetencia állapotára irányuló eredmények megállapításához és fejlesztési igények összegzéséhez már nem volt elegendő az egyszerű, lakossági kérdőíves módszer alapú megállapítás, hanem elsősorban a hatóságok (ENISA, NAIH, NBSz NKI) által összeállított, hiteles adattartalmon alapuló saját statisztikai elemzést tartottam szükségesnek.

2. A KUTATÁS TÖMÖR ISMERTETÉSE FEJEZETENKÉNT

Az értekezés hat fejezetből áll, és az első, bevezető rész tartalmazza a kutatás hátterét, aktualitását és célját, a témaválasztás indoklását és a tudományos probléma megfogalmazását, az értekezés felépítését, a téma vizsgálatának hipotéziseit és azok bizonyításához alkalmazott módszereket. A hatodik fejezet tartalmazza az összegző megállapításokat, következtetéseket, a hipotézisek igazolását, új tudományos eredmények összefoglalását, valamint ajánlásokat a továbbfejlesztésre és hasznosításra vonatkozóan. Az értekezés kutatásra és a vizsgálatok bemutatására vonatkozó, második fejezettől az ötödik fejezetig terjedő részének tömör ismertetését az alábbiak tartalmazzák.

2.1. Az információ jelentősége, az adatvédelem és az információbiztonság jogtörténete és szabályozási rendszere (második fejezet)

A második fejezet az első hipotézisem (H1) bizonyításához szükséges adatvédelmi és információbiztonsági jogtörténet és jogszabályok vizsgálatának eredményeit tartalmazza, a hipotézist az összehasonlító elemzési módszerek figyelembe vételével igazoltam. A fejezetben bemutattam az információ fogalmával összefüggésben lévő jelentősebb adatvédelmi és információbiztonsági jogintézményeket. Az információbiztonsági tudatosság altémához kapcsolódó szakkifejezések pontosabb használatának érdekében, az értekezésben általam definiált meghatározásokat és összefüggéseket használom. A fejezethez kapcsolódó kutatásom során megvizsgáltam a nemzetközi, elsődlegesen Európai Uniós, valamint példaként a németországi és a hazai adatvédelmi (GDPR, német szövetségi adatvédelmi törvény, Infotv.) és az információbiztonsági rendelkezések (IBtv.) és szabványi ajánlások (ISO/IEC 27001), jogtényezők történeti hátterét és fejlődését, jelentőségét, összefüggéseit, valamint az adatvédelmi alapelvek és szabályok alkalmazásának szükségességét.

2.2. Az adatvédelem jelentősége, szabályozás és gyakorlat összefüggései (harmadik fejezet)

A harmadik fejezetben az alkalmazható módszerek közül elsődlegesen azokat a megelőzés típusú módszerek alkalmazását részesítem előnybe, amelyeket az adatvédelmi és információbiztonsági rendelkezések is támogatnak, valamint használhatóságukat, amelyeket kutatásom során kapott eredmények és a fejezetben összegzett adatvédelmi statisztikai adatok is alátámasztanak. Kutatásom

során elsődlegesen a NAIH nyilvános adatvédelmi határozataiban közölt esetek vizsgálata alapján általam összeállított statisztikai kimutatáson keresztül szemléltetem az adatvédelmi alapelvek és szabályok betartásának szükségességét. A vizsgált nemzetközi és hazai adatvédelmi esetek statisztikai adatai rámutatnak az adatvédelmi szabályok és a hatásvizsgálat jelentőségére.

2.3. Az információbiztonsági irányítási rendszer szabályai (negyedik fejezet)

A negyedik fejezetben az információbiztonság és információvédelem nemzetközi és hazai jelentőségét vizsgáltam. A nemzetközi és hazai információbiztonsági incidensek statisztikai adatain keresztül igazoltam az információbiztonsági szabványok és jogszabályi előírások intézményi szintű alkalmazásának szükségességét, a szabályok figyelmen kívül hagyásának károkozó jelentőségét, tehát a második hipotézisem (H2) bizonyításának kiberbűnözés vonatkozású összetevőjét. Tekintettel arra, hogy az információbiztonság megerősítésére vonatkozó előírások megfogalmazása és intézkedések végrehajtása nemcsak a magánvállalkozásokat, vagy az állami intézményeket érinti, hanem egész nemzetünk érdeke, ezért kiindulópontja nem lehet más, mint az államigazgatás és a közigazgatás. A vizsgálat során elsődlegesen az információbiztonsági incidensek statisztikai adatain, az információbiztonsági irányítási rendszer bemutatásán és alkalmazhatóságán, valamint az információbiztonsági kockázatkezelésen keresztül szemléltetem az információbiztonsági (IB) szabályok betartásának szükségességét. A kutatásom során figyelembe vettem a GDPR és az Infotv. életbe lépését, és külön vizsgáltam az ez előtti, illetve utáni időszakot, valamint időszak tekintetében figyelembe vettem a COVID-19 világjárvány, a fokozottabb távmunka és az információbiztonsági események egymásra gyakorolt hatását, következményeit. A kutatásomhoz nemzetközi és hazai tudományos publikációk, hatóságok (14. ábra, Leggyakoribb incidenstípusok statisztikai adatai NKI adatai alapján) és információbiztonságnkigal foglalkozó nagyvállalatok által nyilvánosságra hozott, hiteles statisztikai adatokat vizsgáltam, annak érdekében, hogy különösen a második (H2) és harmadik (H3) hipotézisem információbiztonsági tényezőit igazoljam, amelyeket összevetettem az általam auditált szervezet információbiztonsági adataival. A fejezetben található kutatási eredmények közléséhez és a háttérkutatáshoz dokumentum- és tartalomelemzési, kvalitatív, minőségirányítási, különösen információbiztonsági és kockázatkezelési módszereket, összehasonlító, statisztikai valamint adatelemzéseket, továbbá empirikus kutatást, a matematikai logika alkalmazásával használtam.

2.4. Az információbiztonsági tudatosság szerepe, helyzete, és hatása (ötödik fejezet)

Az ötödik fejezetben hivatkozott felmérések során kiválasztottam azokat az adatvédelmi jogsértéseket, amelyen keresztül bemutattam a statisztikai eredmények igazolását, az információbiztonsági tudatosság szintjének és a fejlesztendő területek meghatározását. Az adatvédelmi jogsértések elemzéséhez szükség volt az úgynevezett „*humán faktor*” vonatkozású, empirikus módszer alapú háttérkutatás lefolytatására, ami az információbiztonsági kockázatkezelés,

valamint az információbiztonsági tudatosítás kutatásához és a harmadik, valamint a negyedik hipotézis igazolásához szükséges. Matematikai kutatási eredményeink felhasználásával kutatói csoportban bizonyítottuk, hogy az információbiztonság kockázatainak vizsgálatakor figyelembe kell venni a védeni kívánt információs rendszeren és a kártékony tevékenységen túl a felhasználói viselkedést (értekezés 15. ábra, IT infrastruktúrát befolyásoló tényezők). A hazai vonatkozású kutatásom során egy olyan vállalkozás informatikai és információbiztonsági tevékenységét vizsgáltam, amely nemcsak információbiztonsági kutatásokat támogató szoftver fejlesztésével, hanem különböző informatikai rendszerek üzemeltetését is ellátta. A kutatásom során alkalmaztam az ISO/IEC 27001 szabvány kritériumait és javasolt intézkedéseit, amely a szabályozási rendszer felállítására, annak működtetésére, kockázatok (vagyonelem, sérülékenységek és fenyegetések) felmérésére és kezelésére (bekövetkezési valószínűség, hatáselemzés), intézkedések megvalósítására, valamint munkavállalói tudatosításra és a belső audit végrehajtására fókuszált. A kutatás során bebizonyosodott, hogy a jelentős intézkedések végrehajtásával, a kockázatok rendszeres felmérésével és a belső auditok évenkénti lefolytatásával a magas kockázatú sérülékenységek és tevékenységek száma, valamint a reális fenyegetések bekövetkezési valószínűsége is csökkenthető. (20. ábra, Fenyegetettség elemzés és lehetséges hatások felmérése saját információbiztonsági és kockázatkezelési kutatás alapján, 2020.) Kutatásom és a 2015-2020. években lefolytatott kockázatkezelési eljárások alapján megállapítottam, hogy a sebezhetőségek kezelése, az emberi hibák bekövetkezésének megelőzése és a megelőzési módszerek (legfőképp információbiztonsági tudatosítási módszerek, 54%-ban) alkalmazása 5-20%-kal csökkentheti az incidensek számát. (értekezés 21. ábra, Kockázatkezelési intézkedési tervben rögzített szükséges intézkedés típusok; 22. ábra, Kockázatkezelés, elfogadható kockázatok eloszlása, maradványkockázat – saját kutatás alapján) Különböző információbiztonsági tudatosítási módszert alkalmaztam, különösen információbiztonsági oktatást, tréninget, egyéni és interaktív kommunikációt. A kockázatkezelésnél, valamint a NAIH által vizsgált (utazási iroda) adatvédelmi incidensek is alátámasztották a biztonságtudatos viselkedésre vonatkozó kutatási eredményeimet.

3. ÖSSZEGZŐ MEGÁLLAPÍTÁSOK ÉS KÖVETKEZTETÉSEK, ÚJ TUDOMÁNYOS EREDMÉNYEK

A kibertér nehézségei, a sérülékenységek, biztonsági rések, és az azokat kihasználó incidensek következménye már nemcsak a szervezetek, az állami intézmények, de a háztartások, ezáltal gyermekeink életét is veszélyezteti, ezen kívül komoly gazdaságot érintő károkat okoz. Az adatvédelmi és információbiztonsági rendelkezések nem hagyhatók figyelmen kívül. A folyamatos támadások miatti megelőzési és védekezési, adatvédelmi és információbiztonsági intézkedések sem biztosítanak teljes körű védelmet, de a kockázatok ismerete és a megfelelő akciók végrehajtása csökkentheti az esetleges incidensek számát.

3.1 Hipotézisek igazolása

A H1 hipotézis igazolásának tekintetében a vonatkozó jogtörténet, történeti áttekintés, adatvédelmi és információbiztonsági szabályok, és szabványok vizsgálata (második fejezet) nélkülözhetetlen. A kutatási terület szempontjából elsősorban a téma pozícionálása, a releváns adatvédelmi és információbiztonsági szabályozás folyamatainak vizsgálata és kapcsolatok elemzése szükséges abból a célból, hogy az információbiztonsági tudatosság helyzetét a törvényi előírásokhoz mérten vizsgálhassam. A történeti, technikai, jogtényezői kapcsolati viszony feltárása és bemutatása lényeges, hiszen egy korban egészen fiatal tudományterületből kifejlődött jogintézmények és technológiák egészen egyedi szimbiózisa. Tekintettel arra, hogy Hazánk az Európai Unió tagállama, számos Uniós jogszabálynak, így az általános adatvédelmi rendelet előírásainak is meg kell felelni, ezáltal a vizsgálat fókuszát ki kellett terjeszteni a nemzetközi, de legfőképp az Uniós jogrendre, a tekintetben, hogy Hazánk a szabályozási kötelezettséget milyen szinten teljesíti és szabályozásunk mennyire illeszkedik a nemzetközi gyakorlatba, illetve figyelembe kell venni, hogy más tagállam, például Németország hogyan valósította meg ezen feladatait. Kutatásom során megállapítottam, hogy az információbiztonsági szabályozás (IBtv.) nem terjed ki minden jogi személyre, csak az állami és önkormányzati szervekre. Ugynakkor H1 bizonyítása és a megfogalmazott következtetéseim rámutatnak arra, hogy a vonatkozó alapelvek és rendelkezések megalkotása és alkalmazása indokolt a személyes adatok védelmének biztosításához. A fogalomrendszer vizsgálata során megállapítottam, hogy az IBtv. által definiált fogalmi kör lényegesen szélesebb spektrumú, mivel nemcsak információvédelmi és információbiztonsági szakkifejezéseket, hanem adatvédelemre vonatkozó megállapításokat is tartalmaz. A két jogszabály (Infotv., IBtv.) értelmező rendelkezései között redundancia és némi eltérés tapasztalható. Az Infotv. tekintetében a magatartási kódex magyar jellegzetességeinek és szükségességének hangsúlyozása hasznos volna az adatkezelők számára. A tananyagok és szakirodalom tekintetében már sokkal színesebb meghatározásokkal találkozhatunk, akár az információbiztonsági tudatosság, mint fogalom vonatkozásában sincs egységes álláspont. Egységes magyar adatvédelmi és információbiztonsági szakkifejezések kiadása és rendszeres időszakonkénti felülvizsgálata, a technológiai fejlődéshez igazított fejlesztése szükséges. Az adatvédelmi, információbiztonsági rendelkezések és szabványi ajánlások elősegítik intézményi szintű alkalmazásukat, de a tisztázatlan fogalmak a jogszabályok téves értelmezését eredményezik. A kutatás során megállapítottam, hogy a Magyarországon érvényes adatvédelmi és információbiztonsági vonatkozású jogszabályok alkalmazása hatékonyan befolyásolja az információs társadalom fejlődését. A szabványok alkalmazásával pedig az információs rendszerre vonatkozó bizalmasság, sértetlenség, rendelkezésre állás, valamint az adatvédelmi alapelvek teljesülnek, aminek következménye a tudásra, az információra, az intellektuális technológiára épített bizalmasság növelése, továbbá a posztindusztriális társadalom fejlődése. Az érvényben és hatályban lévő adatvédelmi és információbiztonsági szabályok

alkalmazása korlátozza az adatgyűjtést, csökkenti az adatvédelmi incidensek számát, növeli az információs rendszerek információbiztonsági szintjét. Az adatvédelmi és információbiztonsági szabályozás egyik jogalapja az adatvédelmi jogsértés. A komplex szabályozási rendszer egyrészt útmutatóul szolgál az információs rendszerek tervezéséhez, fenntartásához és védelméhez, a jogszerű adatkezelés, adatfeldolgozás és adattovábbítás megvalósításához, másrészt a jogellenes tevékenységek szankcionálásával elősegíti az állampolgári bizalom kialakulását. Tehát, az adatvédelmi és információbiztonsági szabályok az informatikai technológiai folyamatokkal koherens fejlesztése és konzekvens alkalmazása, állampolgárok tekintetben bizalomerősítő tényező. A megalkotott magyarországi szabályok az EU jogalkotói elvárásoknak megfelelően, védelmet nyújtanak az állampolgárok adatai számára, biztosítják az adatvédelmi és információbiztonsági jogokat, egyértelműen rögzítik az adatkezelők és adatfeldolgozók feladatait, jogait és kötelezettségeit, ugyanakkor további fejlesztésre szorul. Az incidensek jelentős tényezője a technológiai megoldásokon túl, a „*humán faktor*”, amely az információs rendszer kulcsfontosságú összetevője. A megállapítások a H1 és H2, valamint a H1 és H3 hipotézisek összefüggéseit indirekt és inverz módon is igazolják.

A H2 hipotézis szerint a felhasználói információbiztonsági tudatosság hiányának hatása esetlegesen az adatvédelmi jogsértés. A vizsgálat tárgya elsődlegesen a H1 és H2 hipotézis ok-okozati összefüggése, a H1 és H2 hipotézis során vizsgált folyamatok és hiányosság eredményei, úgymint a szabályok be nem tartásának következményei, valamint az információbiztonsági tudatos, szabálykövető és a szabályszegő magatartás összefüggéseinek tanulmányozása, beleértve az információbiztonsági tudatosság hiányainak és a kiberbűnözés lehetőségeinek korrelációját (H2). Az általam vizsgált adatvédelmi és információbiztonsági statisztikai adatok elemzésének eredménye alátámasztja a „*humán faktor*” jelentőségét, amely szerint az információs rendszerek információbiztonsági szintjének egyik befolyásoló tényezője. Ezen terület fejlesztése növekvő információbiztonsági szintet, míg elhanyagolása csökkenő tendenciát mutat. Az adatkezeléskor alkalmazott technikai intézkedéseket meg kell feleltetni az adatvédelmi elveknek, különösen az adattakarékosság hatékony megvalósítása, vagy az érintettek jogainak védelméhez szükséges garanciák beépítésére vonatkozó előírások betartása érdekében. Vizsgálat során fókuszba került a felhasználói információbiztonsági tudatosság azon hiánya, amely emberi tévedést és szándékos kárt eredményezhet, elősegíti az incidensek bekövetkezését, és támogatja a kiberbűnözést. Megállapítottam továbbá, hogy a kiberbűnözés legfőképp a nem megfelelő adatkezelést használja ki, különösen az adathalászat és a káros szoftverek tekintetében jelentős mértékű, és számottevő károkat okozott, az egészségügyi, oktatási, igazgatási, banki, ipari és egyéb szolgáltatóipari ágazatnak. A károk helyreállítása és a védelmi szint megerősítése jelentős anyagi ráfordítással jár, tehát gazdaságkárosító tényező. A vizsgálat során igazoltam, hogy a szabály alapú (ISO 27001,

GDPR, Infotv, IBtv. együttesen) informatikai és információbiztonsági fejlesztések, az interoperabilitási lehetőségek, a fejlettebb technológiák (például mesterséges intelligencia) együttes alkalmazása nagyobb védelmet nyújt adatainknak és rendszereinknek egyaránt, az egyre növekvő, kifinomult támadások kivédése ellen, továbbá gyengíti az incidensek hatását. Az adatvédelmi jogsértések jelentős része kiberbűnözői tevékenység. A H2 hipotézis kapcsolatban igazolt inverz és közvetett megállapítás szerint az információbiztonsági tudatosság fejlesztése egyben kiberbűnözői tevékenység csökkentő tényező. Következtetésként megállapítottam, hogy tekintettel az incidensek „*humán error*" tényezőire a preventív információbiztonsági folyamatok erősítésének érdekében komplexebb adatvédelmi és információbiztonsági tudatosítás szükséges. A fenti megállapításokkal a H2 és H3 valamint a H2 és H4 hipotézisek ok-okozati összefüggéseit igazoltam.

A H3 hipotézis igazolásának tekintetében a kutatás tárgya egyrészt a H2 hipotézis vizsgálata során kapott eredmények összevetése az információbiztonsági kockázatkezeléssel és a tudatosításra fókuszált intézkedések eredményességével, valamint a „*humán faktor*" és az információbiztonsági kockázatkezelés összefüggéseinek vizsgálata. A H2 és H3 hipotézis igazolása átfedéseket eredményez a „*humán faktor*" hatás vizsgálatának tekintetében. A harmadik hipotézist (H3) saját kockázatkezelési kutatási eredményeimmel, az ENISA által feldolgozott statisztikai adatokkal és a szervezet által hivatkozott tanulmányokkal, valamint a NAIH esetvizsgálatának eredményeivel igazoltam. Igazoltam tehát azt a felvetést, miszerint az adatvédelem jelentőségének tudatosítása és az információbiztonsági tudatosság fejlesztése csökkenti az emberi hiszékenység kihasználását, a tévedések, mulasztások és szándékos károkozás számát, ezáltal erősíthető a szervezet információbiztonsági szintje. A tudatosítás iránti igényt erősíti az a tény, hogy a felsőoktatási intézmények által szervezett informatikai alapképzéseken és szakirányú továbbképzéseken elsődlegesen adatvédelmi, biztonságtechnikai, kiberbiztonsági alapelveket és megoldásokat tanulhatnak, amelyeket gyakorlatban is felhasználhatnak. A irány megfelelő és a jövőben tartani szükséges, ugyanakkor az értekezésben bemutatott kutatásom statisztikai adatai és tanulmányaim rámutatnak arra, hogy az információbiztonsági tudatosításra fordított idő és tevékenység nem elegendő.

A H4 hipotézis vonatkozásában a H2 és H3 hipotézis igazolása során kapott eredmények alapján a vizsgálat tárgya a digitális kultúra állapota, az információbiztonság-tudatosságnövelési program, annak hatékonysága, a program alapján további információbiztonsági tudatossági szintek meghatározása, és a témákban érintett korosztályok vizsgálata. A H4 hipotézis igazolásánál az Európai Unió digitális kompetencia javaslatait is figyelembe vettem. A „*humán faktor"* tényezőre fokuszáló vizsgálat során megállapítottam, hogy a digitális kompetencia információbiztonsági készsége gyermekkortól az időskorig kialakítható, de rendkívül időigényes folyamat. A diákok képzésébe minden képzési szinten és minden korosztály számára elérhetővé kell tenni az

információbiztonsági képzéseket, ezzel elősegítve a digitális kompetencia és a „*kiberhigiénia*” megteremtését és fejlesztését. Folyamatosan javítani kell a vállalati és a közszférában dolgozó állampolgárok biztonságtudatossági állapotán, és a mindennapi munkavégzés folyamataiba be kell építeni a személyes és online, vállalati csoportos vagy egyénre szabott konzultációkat, továbbképzéseket és tréningeket. A végrehajtott, információbiztonsági és minőségirányítási auditok, az emberi tényező biztonságtudatosságának felmérésére, és incidensekre irányuló vizsgálatok és statisztikai adatok, valamint az informatikai oktatások során azt tapasztaltam, hogy annak ellenére, hogy az adott intézmény vagy vállalkozás rendelkezik a felhasználókra vonatkozó IT biztonsági szabályzatokkal, vezetői utasításokkal, eljárásokkal, a hiányzó vagy a nem megfelelő aktivitás hozzájárul a biztonságtudatosság csökkenéséhez.

1. ábra, az adatvédelmi és információbiztonsági tudatosság fejlesztésére vonatkozó általános felhasználói szint kapcsolati modell (ÁFSZK), saját szerkesztés (az értekezés 23. ábrája)

Megállapítottam, hogy a gyerekek, és az átlag, nem informatikai szakterületen tanult, felsőfokú szakképesítéssel nem rendelkező felhasználók (5+1 szint: Általános felhasználói szint) számára is biztosítani kell a megfelelő szintű és óraszámú digitális, adatvédelmi és információbiztonsági képzéseket. A hipotézisek igazolása alapján meghatároztam az adatvédelmi és információbiztonsági tudatosság fejlesztésére vonatkozó modellt (az értekezés 23. ábrája), amely alapján 5 szintet különítettem el. Mindenkinek rendelkezni kell az alapvető adatvédelmi kompetenciával, csak így biztosítható a felhasználói információbiztonsági tudatosság hatékonyan fejlődése.

3.2 Az új tudományos eredmények összegzése

Az értekezés, és különösen a hipotézisek igazolása alapján az alábbi téziseket fogalmaztam meg.

T1a A hazai adatvédelmi és információbiztonsági jogszabályi rendelkezések összhangban vannak a nemzetközi információbiztonsági standardokkal és az általános adatvédelmi rendelettel, ugyanakkor az értelmező rendelkezések korrelációja fejlesztendő terület.

A H1 hipotézis összefüggésében megállapítottam, hogy a vonatkozó alapelvek és rendelkezések megalkotása és alkalmazása indokolt a személyes adatok védelmének biztosításához, továbbá a hazai adatvédelmi és információbiztonsági rendelkezések összhangban vannak a nemzetközi adatvédelmi rendelkezésekkel, az általános adatvédelmi rendelettel, a német szövetségi adatvédelmi törvény vonatkozó meghatározásaival, valamint a nemzetközi információbiztonsági irányítási rendszer (ISMS) ajánlásaival, ugyanakkor a törvények értelmező rendelkezései helyenként nincsenek összhangban, meghatározó szakkifejezések deklarálása hiányzik és a meglévők erőteljes pontosításra szorulnak, továbbá a következetesség tekintetében a redundáns fogalommeghatározás javítása szükséges. Az adatvédelmi fogalomkörébe tartozó értelmezések az Infotv., az információbiztonsági és kibervédelmi meghatározások az IBtv. hatásköre legyen. Összegezve, a tudomány mai álláspontja szerint lekövetett, és egységes magyar adatvédelmi és információbiztonsági értelmező rendelkezések beiktatása szükséges, a vonatkozó szakkifejezések korrelációjának definiálásával.

T1b. A magyarországi információbiztonsági szabályozás hatályossága terén jelentős hiányosság tapasztalható.

Tekintettel arra, hogy az IBtv. nem terjed ki minden jogi személyre, ezért az információbiztonsági jogszabályi előírások kiterjesztése legalább 250 fő munkavállalót és egyéni vállalkozót foglalkoztató vállalkozásokra szükséges.

T1c. Az állampolgárok adatvédelmi és információbiztonsági előírások általi támogatása és tudatosítása állampolgári bizalomerősítő, valamint humán faktor befolyásoló, közvetett módon kockázatcsökkentő tényező.

A T1c tézist a H1 és H2, valamint H1 és H3 hipotézis igazolások összefüggései alapján fogalmaztam meg.

T2a. Az adatvédelmi eseménybekövetkezési valószínűség függvényében, a „*humán faktor*”, különösen a „*humán error*” részarány vonatkozásában a felhasználói információbiztonsági tudatosság hiánya közvetett módon adatvédelmi jogsértéseket eredményezhet.

T2b. Az adatvédelmi jogsértések jelentős hányada kiberbűnözői tevékenységből ered.

T2c. Az információbiztonsági tudatosság fejlesztése kiberbűnözői tevékenység mértéket csökkentő tényező.

T2d. A preventív információbiztonsági folyamatok hatékonysága érdekében a komplex adatvédelmi és információbiztonsági tudatosítási képzés elengedhetetlen.

A T2 téziseket a H2 hipotézis igazolásának következtében állapítottam meg, amelyhez a H2 és H3 hipotézis igazolások összefüggéseit használtam fel, és eredményeként az ÁFSZK modellt alkottam meg (disszertáció 23. ábra).

T3a. A Magyarországon érvényes adatvédelmi és az információbiztonsági alapelvek és rendelkezések tudatosítása hatékonyan befolyásolja a felhasználói információbiztonsági tudatosság fejlődését.

T3b. Az adatvédelmi és információbiztonsági tudatosság fejlesztésére vonatkozó általános felhasználói szint kapcsolati modell összefüggésében a magyarországi tudatosítási és visszacsatolási folyamatok kiforratlanok.

A H3 hipotézis igazolásának összefüggésében megállapítottam a T3 téziseket, amelyek szerint az adatvédelmi és információbiztonsági alapelvek stabil kiindulópontjaira épített tudatosítási folyamatok erősítése és fejlesztése szükséges.

T4a. Az adatvédelmi és információbiztonsági tudatosítás rendszerét nemcsak az informatikai oktatásban, hanem minden korosztály számára elérhetővé kell tenni és minden szakterületen indokolt bevezetni és működtetni.

T4b. Megfelelő szintű adatvédelmi és információbiztonsági képzések hiányában az érintettek elvárt digitális kompetenciát nem szerezhetnek, ami számottevő információbiztonsági tudatossági hiányt okoz.

A T4 tézisek megfogalmazása a H2-H4 hipotézisigazolás összefüggési vizsgálatának eredménye.

T4c. Az adatvédelmi és információbiztonsági alapelveket minden korosztály számára elérhetővé kell tenni, ezáltal biztosítható a felhasználói információbiztonsági tudatosság hatékonyan fejlődése, valamint a digitális kompetencia technikai haladást követő, megfelelő ütemű fejlődése.

A H4 hipotézis összefüggésében megállapítottam az információbiztonsági tudatosítás rendszerét szükséges bevezetni és működtetni, amely érinti az oktatás különböző korosztályait, valamint a szakterületeket.

T4d. A visszacsatolás hiánya vitatható végeredményt és *pontatlan tényeken alapuló döntéshozatalt* eredményez, ami jelentős kockázati tényező.

Kutatási eredményemként bemutatott ÁFSZK modell támogatja a visszacsatolás jelentőségét, amelyet a H1-H4 hipotézisek igazolásának következtében állapítottam meg.

4. JAVASLATOK AZ ÚJ TUDOMÁNYOS EREDMÉNYEK GYAKORLATI HASZNOSÍTÁSÁRA

A dolgozat lehetőséget teremt az információbiztonsági tudatosság fejlesztésére irányuló képességfejlesztések alkalmazására minden korosztály számára. A megállapítások alapján az általános és a középiskolákban digitális kultúra (informatika) oktatás keretében, az óraszámelosztást igazítva az aktuális igényekhez, a tematikákat a tudatosításra vonatkozó módszerekkel és tananyagokkal (adatbiztonság, adatvédelem, információbiztonság alapelvek, magatartási kódex) lehetne kibővíteni. Az igény vagy szükség szerinti IB képzés meghatározója lehet a felvételi alkalmával a leendő hallgatók által kitöltött IB tesztek eredményei. Ezáltal akár helyi szinten, kompetenciának megfelelően biztosítható a képzés.

4.1. Információbiztonsági tudatosítási javaslatok óvodás korú gyermekek számára

Napjainkban egyre nagyobb figyelmet kap a gyermekek kiberbiztonsága, a gyermekek különböző online fenyegetéseknek való kiszolgáltatottsága és kockázatok vizsgálata. Szakemberek körében is vitatott az információbiztonsági tudatosítás módszereinek alkalmazása 10 éves kor alatt, ugyanakkor a négy-hét éves gyermekeket, akik már értik a mesék tanításait, őket már be lehet avatni a biztonság, a csúnya-szép, a rossz-jó világába, legyen az internet, egy alkalmazás, vagy egy kedvenc mese. Amennyiben elfogadjuk, hogy a gyermek ösztönösen különbséget tud tenni jó és rossz között, és a mesék által tanítható, úgy a digitális képességek játékossággal és tanmesékkel, gyermeki szinten is fejleszthetők. Az értekezésben javaslat szintjén foglakoztam néhány készségfejlesztési terület digitális eszközökkel támogatott megerősítésével és információbiztonsági szakkifejezés elsajátítást támogató megoldással (CIA alapelvek tanítása kulcsszavakkal, szimbólumokkal, rajzfilmekkel). Információbiztonsági koncepció iskolakezdők részére is kialakítható, különösen az identitásvédelem, a mentés, segítség kérés és elfogadás képesség kialakítása, kiberfenyegetések – akár a közlekedésben, nem hiteles tartalom felismerése, a digitális világ iránti kíváncsiság fejlesztése, jó gazda szemlélet kialakítása a digitális térben, kiberlábnyom tudatosítása. A javaslatok alkalmazása óvodai környezetben jobban érvényesül szakemberek, óvodapedagógus támogatásával. A szülők bevonása is feltétlen szükséges, mivel ők azok, akik okostelefont adnak az elsős, másodikos kisiskolásnak, a folyamatos kapcsolattartás érdekében.

4.2. Információbiztonsági tudatosítási javaslatok szülők számára

Tekintettel arra, hogy a szülők figyelemmel kísérik gyermekük tanulmányait, célszerű csoportos, szülői értekezletek alkalmait felhasználni az információbiztonsági tudatosítási eszközök

alkalmazására. Témák lehetnek, különösen az adatvédelmi és CIA alapelvek áttekintése iskolai példákkal, esettanulmányok, valamint a tanulás támogatása okoseszközökkel.

4.3. Ajánlás kutatási tevékenység és a jogszabályok fejlesztésére

Az értekezésben kapott eredmények alkalmasak a kutatás továbbfejlesztésére, úgymint az információbiztonsághoz kapcsolódó BSC stratégiai térkép megalkotására, a gyermekek biztonságtudatos gondolkodásának fejlesztésére irányuló módszerek kidolgozására, az IBtv. kiterjesztésére legalább 250 fő munkavállalót foglalkoztató vállalatokra, valamint a magatartási kódex megalkotására a közigazgatásban.

A DOKTORJELŐLT PUBLIKÁCIÓS JEGYZÉKE

[1.] Eszter OROSZI , Krisztina GYŐRFFY: Information security for egovernment social media marketing and citizen interaction, Central and Eastern European eIDem and eIGov Days 2016: Multi-Level (e)Governance: Is ICT a means to enhance transparency and democracy?, Budapest, 2016.

[2.] Ferenc, LEITOLD, Kálmán HADARICS , Eszter OROSZI , Krisztina GYŐRFFY: Measuring the information security risk in an infrastructure, MALWARE 2015 10th International Conference on Malicious and Unwanted Software, Puerto Rico, 2015

[3.] Ferenc LEITOLD, Krisztina GYŐRFFYNÉ HOLLÓ, Zoltán KIRÁLY, Quantitative metrics characterizing malicious samples, In: Cyril, Onwubiko; Pierangelo, Rosati; Aunshul, Rege; Arnau, Erola; Xavier, Bellekens; Hanan, Hindy; Martin Gilje, Jaatun (szerk.) Cyber Science, CyberSA for Trustworthy and Transparent Artificial Intelligence (AI), Dublin, Írország: Center for Multidisciplinary Research, Innovation and Collaboration 2021. pp. 82-83., 2 p.

[4.] GYŐRFFYNÉ HOLLÓ Krisztina: Az információbiztonság jelentősége és története, GRADUS Vol 8, No 2 (2021), John von Neumann University, Hungary, Kecskemét

[5.] GYŐRFFYNÉ HOLLÓ Krisztina, Információbiztonság, avagy incidens kontra biztonságtudatos viselkedés, INFOKOMMUNIKÁCIÓ ÉS JOG 18., 76 pp. 17-23. 7 p., 2021.

[6.] GYŐRFFYNÉ HOLLÓ Krisztina, Az érintés nélküli adatgyűjtés kockázatai és a kockázatszámítás módszerei, DUNAKAVICS 9 : 8 pp. 77-97. , 21 p., 2021.

[7.] GYŐRFFYNÉ HOLLÓ Krisztina, Közszolgálati információs rendszerek interoperabilitási nehézségeinek megoldása, DUNAKAVICS 2021. IX. évfolyam II. szám pp. 21-40. , 19 p., 2021.

[8.] GYŐRFFYNÉ HOLLÓ Krisztina, LEITOLD Ferenc: Felhasználókkal kapcsolatos információbiztonsági intézkedések kezelése a GDPR tükrében, Hétpecsétes történetek 2,5 - a GDPR antológia, Budapest, 2018.

[9.] GYŐRFFYNÉ HOLLÓ Krisztina, Az információbiztonsági sebezhetőségek tényezőinek vizsgálata: A „humán faktor”, In: Váraljai, Mariann (szerk.) INFORMATIKA KORSZERŰ

TECHNIKÁI KONFERENCIA 2021 „Jövőformáló tudomány” „Fenntarthatóság és digitalizáció” Dunaújváros 2021. november 9.: DUE Press (2021) 80 p. p. 40
[10.] GYŐRFFYNÉ HOLLÓ Krisztina, Információbiztonság, avagy megéri kockáztatni? In: Nagy, Bálint; Katona, József AZ INFORMATIKA KORSZERŰ TECHNIKÁI KONFERENCIA 2020 : Jövőformáló tudomány programfüzet és absztraktkötet Dunaújváros, 2020. november 9-10., Dunaújváros, DUE Press 2020. 48 p.p. 22
[11.] GYŐRFFYNÉ HOLLÓ Krisztina, Az információbiztonsági tudatos viselkedés az incidensek elkerülésének egyik tényezője, DUNAKAVICS 8 : 12 pp. 5-18. , 14 p. 2020.
[12.] HADARICS, K., GYORFFY, K., Nagy, B., BOGNAR, L., ARROTT, A., LEITOLD, F., Mathematical Model of Distributed Vulnerability Assessement, Security and Protection of Information 2017, University of Defence, IDET BRNO, Czech Republic, 2017
[13.] Krisztina GYŐRFFY, Ferenc LEITOLD , Anthony ARROTT: Individual awareness of cyber-security vulnerability – Citizen and public servant, CEE eDem and eGov Days 2017: Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment?, Budapest
[14.] Krisztina GYŐRFFYNÉ HOLLÓ: The Human Factors of the IT Risk Management, DUNAKAVICS, Dunaújvárosi Egyetem online folyóirata 2021. IX. évfolyam VII. szám, 47-61pp
[15.] Krisztina GYŐRFFYNÉ HOLLÓ, Adam KARISZTL: Domino effect and other models in the it process, GRADUS Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.

A DOKTORJELŐLT KUTATÓI ÉLETRAJZA

Holló Krisztina 2001-ben főiskolai informatikus mérnök (BSc) végzettséget szerzett, majd 2008-ban a Pannon Egyetem Műszaki Informatikai Karán kiváló minősítésű, mérnök-informatikus egyetemi diplomát. 2014-ben a Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Kar, Jogi szakokleveles gazdasági szakember szakirányú továbbképzésén, Jogi szakokleveles mérnök-informatikus diplomát szerzett. A tanulmányait több egyetemen és informatikai cégnél is hasznosította, 2001-től 2008-ig program- és SAP fejlesztőként dolgozott a Semmelweis Egyetemen. 2008-tól a Pannon Egyetemen IT biztonsági szakértőként és minőségirányítási megbízottként, jelenleg oktatóként és mentorként dolgozik. Kutatásait különösen információbiztonsági szakértőként és ISMS vezető auditorként végezte, 2015-től 2021-ig Veszprémben. 2015-2018 között a Nemzeti Közszolgálati Egyetemen óraadóként és e-szeminárium vezetőként részt vett az Elektronikus információbiztonsági vezető szak Szakirányú továbbképzésben, valamint 2018 és 2020 között a Dunaújvárosi Egyetem meghívott óraadó oktatója volt. 2016-tól 2021-ig PhD tanulmányokat folytatott a Nemzeti Közszolgálati Egyetem, Államtudományi és Nemzetközi Tanulmányok Kar, Közigazgatás-tudományi Doktori Iskolájában, 2021-ben szerzett abszolutóriumot.