Pécsi Tudományegyetem
Állam- és Jogtudományi Kar
Doktori Iskola

Szádeczky Tamás

Szabályozott biztonság

Az informatikai biztonság szabályozásának elmélete, gyakorlata
és az alkalmazás megkönnyítésére felállított módszertan

PhD értekezés tézisei

Témavezető:
Dr. Balogh Zsolt György PhD
tanszékvezető egyetemi docens

Pécs, 2011.

Tartalom

1. A kitűzött kutatási feladat

Az előző évszázad közepétől hatalmas fejlődés volt tapasztalható a számítástechnika területén. Az első otthoni Commodore 64-esünk és az elszigetelt BBS-ek[1] használata óta eljutottunk az egész életünket átszövő informatikai eszközök és hálózatok garmadájáig: okostelefon, notebook, Internet, amelyek táptalaján egy egész virtuális világ alakult ki. Ebben a virtuális világban a való világban tapasztalható jelenségekhez többé vagy kevésbé hasonló jelenségek tapasztalhatók. Kriminológusok vitatkozhatnak azon, hogy bizonyos bűncselekmények virtuális világban történő végrehajtása eltér-e a való világban történő elkövetéstől. Ami viszont mindenképpen egyedi: a védelem technikai végrehajtásának módja és lehetőségei. Az informatikai biztonság és védelem magába olvaszt elemeket a hagyományos területekből, mint a katonai védelem vagy a vagyonvédelem, viszont azoktól merőben eltérő tulajdonságai is vannak. Az informatikai biztonság különlegességére és fontosságára való rádöbbenés időszaka hazánkban a kilencvenes évekre tehető. Ekkor még minden biztonságról szóló dokumentumban fogalommagyarázatokat kellett feltüntetni és el kellett magyarázni, hogy ez az egész terület miért fontos. Húsz év alatt a biztonsági szakma kiharcolta létjogosultságát, az informatikai biztonságot alkalmazók, azt megfizetők többé-kevésbé tudják, hogy fontos ez a terület. A kérdés a huszonegyedik század elején nem a *miért*, hanem a *hogyan* és a *mennyire*. Az üzleti szférában – a gazdasági világválság idején különösen – nem létezik elég olcsó, nincs olyan kötelező kiadás, amiből ne akarnának még egy kicsit lefaragni. A cél viszont elérendő: az állampolgárok, a shareholderek,[2] a stakeholderek[3] és az állam célja is, hogy mindenhol – úgy az üzleti, a magánéletben és az állami szférában is – megfelelő informatikai biztonsági szint kerüljön kialakításra és fenntartásra. Nap, mint nap tapasztaljuk, hogy a biztonság oltárán való áldozat értéke a költségvetés csökkenésével négyzetesen arányos mértékben csökken. Amíg egy nagy távközlési cég esetében szinte soha nem lehet komoly hiányosságot találni, addig az otthoni számítógépére a felhasználó gyakran még az

[1] Bulletin Board System, 1970-1990 között használatos terminálcsatlakozást lehetővé tévő közösségi számítógépek elsősorban fájlmegosztás céljára.
[2] tulajdonos, részvényes
[3] a szervezet működésében érdekelt illetve érintett felek összessége

ingyenes védelmi eszközöket sem telepíti fel. Nyilván ennek rendkívül sok oka lehet: például a szakmai ismeretek, tapasztalat, információ, pénz, érdeklődés hiánya, de mindemellett a figyelem felhívása sem történik meg a területre, valamint a későbbi felelősségre vonhatóságra. A felelősségre vonhatóság pedig fontos tényező, hiszen a jogalkotó szempontjából nincs teljes megfelelés, mindenen lehet még javítani, az elérendő cél a tökéletesség.

Az értekezés tárgya az informatikai biztonság jogi és nem jogi szabályozása. A nem jogi szabályozás elemzésének hangsúlya is elsősorban az állami irányítás eszközrendszerébe illeszthető elemeken van. Az informatikai biztonság a lenti levezetés szerinti fogalmat takarja.

Az adatbiztonság „az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere."[4] Más megfogalmazás szerint „az informatikai rendszerekben az adatok kezelésének megfelelő minőségét jellemző állapot. az adatbiztonság három összetevőre: az integritásra, a titkosságra és a pontosságra bontható."[5]

Az adatbiztonság tágabb értelmezésében az adatok (digitális vagy papíralapú) jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere. Szűkebb értelmezésében technikai adatvédelem, tehát a jogi úton történő magánszféra-védelem műszaki-technikai megvalósítása.

Az információbiztonság „az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb tulajdonságok, mint a hitelesség, a számon kérhetőség, a letagadhatatlanság és a megbízhatóság, szintén ide tartozhatnak."[6] Az információbiztonság a tágabb értelmezésben használt adatbiztonsággal egy értelmű, viszont az információ szó értelmezett adatot jelent, e szerint az információbiztonság a feldolgozatlan, nem értelmezett adatot nem védené, amely nem felel meg a valóságnak. Használható viszont a szűkebb értelmezésben használt adatbiztonságtól való tartalmi elhatárolásra.

Az informatikai biztonság „olyan előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és bizalmasságát érintik,

[4] ITB 8. sz. ajánlás, 1994, p. 132.
[5] Szabó J., 1995, adatbiztonság címszó, p. 6.
[6] MSZ ISO/IEC 27001:2006 3.4. p. 22.

és amelyeket az informatikai rendszerekben vagy komponenseikben, valamint az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző intézkedésekkel lehet elérni. […] Informatikai biztonság alatt valamely informatikai rendszer azon állapota értendő, amelyben a kockázatokat, amelyek ezen informatikai rendszer bevezetésekor a fenyegető tényezők alapján adottak, elfogadható intézkedésekkel elviselhető mértékűre csökkentettük."[7]

Ennél rövidebb és pontosabb meghatározás, hogy „az informatikai biztonság az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.[8]

Az informatikai biztonság a tágabb értelemben vett adatbiztonság (amely alapvetően független az adat hordozójától) megvalósítását jelenti az informatikai hálózatok és rendszerek tekintetében. Nem lehet viszont elvonatkoztatni a komplex biztonságfogalomtól, így az informatikai biztonság nem jelentheti kizárólagosan például a kriptográfiai biztonságot, vagy a tűzfalak konfigurációját. Az informatikai biztonság megvalósítása tehát nem korlátozódhat a kibertérre, feltétlenül figyelembe kell vennünk az anyagi világban felmerülő biztonsági igényeket is: az épület nyílászáróinak védelmétől a humánerőforrás biztonságáig.

Az IT biztonság jelentése megegyezik az informatikai biztonsággal, mindemellett az informatika helyett az információtechnológia[9] kifejezés használata jobban hangsúlyozza, hogy a technológiák védelmét tekinti fontosnak. Angolszász nyelvterületen az IT Security kifejezés kizárólagosan használt az informatikai biztonság meghatározásaként, jelentését tekintve is ugyanúgy a komplex biztonság-megközelítés alapján alkalmazzák. Tekintettel arra, hogy az IT idegen rövidítés és a szakmán kívül kevéssé ismert, az alkalmazása az IT-hez hasonlóan kerülendő, bár a szaknyelvben már elfogadott a használata.

Az információvédelem „alapvetően a bizalmasság, a sértetlenség és a hitelesség elvesztése elleni védelmet, a megbízható működés a rendelkezésre állás és a

[7] ITB 8. sz. ajánlás, 1994, p. 138.
[8] Muha, 2008, p. 145.
[9] A fogalom magyarázata a Forradalmak kora c. fejezetben található

funkcionalitás elvesztése elleni védelmet foglalja magába."[10] Tágabb értelemben tehát a szintén tág értelmében vett adatbiztonsághoz (is) kapcsolódó védelmi intézkedések összessége. Szűkebb értelemben katonai, nemzetbiztonsági használatban a titokvédelem, a minősített adatok védelme.
A lenti táblázatban összefoglalásra kerültek az alkalmazott legfontosabb fogalmak, a fogalmak tárgya, megjelenési formái és így az összefüggésük.

fogalom	**tárgya**	**formája**	**megjelenése**
adatvédelem	személyes adat	jogi	bármely megjelenés
adatbiztonság (szűk)	személyes adat	műszaki	bármely megjelenés
adatbiztonság (tág), információbiztonság	bármely adat	komplex	bármely megjelenés
információvédelem (szűk), minősített adatok védelme	minősített adat	komplex	bármely megjelenés
információvédelem (tág)	bármely adat	komplex	bármely megjelenés
informatikai biztonság, IT biztonság	bármely adat	komplex	informatikai rendszer, hálózat, adathordozó

A fentiek alapján a kutatás az informatikai biztonság tekintetében elsősorban a számítógépen tárolt és feldolgozott adatok elektronikus védelmével foglalkozik, de ahol szükséges, kitér a biztonság és a védelem más aspektusaira (a fogalom-meghatározásban található informatikai biztonság fogalmának megfelelően). A szabályozás jelen esetben nem a szűken vett jogi szabályozás, hanem a szakterületen alkalmazható bármely szabályzási módszer, így a szabványosítás és a belső szabályozás is. Másrészről viszont első sorban az állam szempontjából kerül megközelítésre a szabályozandó terület, ezért a gyakorlati részben már csak az állam által alkalmazható szabályozások kerülnek kifejtésre.

A témaválasztás aktualitását adja a szakterületre vonatkozó jogalkotási lépések szaporodása: az elektronikus közszolgáltatásokra vonatkozó jogszabályok megalkotása és az informatikai biztonságról szóló törvény tervezetének elkészítése. Közösségi szinten az adatvédelmi szabályozás újragondolási lépései:

[10] ITB 12. sz. ajánlás, 1996.

az adatmegőrzési irányelv és a hírközlési irányelv módosítása, az adatvédelmi irányelv megújításának szándékát mutató lépések a WP 29[11] részéről. Az időszerűség mellett kiemelendő a fontosság: ezzel a multidiszciplináris kérdéssel tudományos körökben rendkívül kevesen foglalkoztak, de a szabályozás mindennapi gyakorlati alkalmazása elkerülhetetlen a gazdálkodó szervezetek és az állami szféra számára.

[11] Az Európai Bizottságban működő adatvédelmi munkacsoport

2. Kutatási módszertan

Az értekezés témája tehát az informatikai biztonság szabályozása. Ebből az informatikai biztonság tekintetében elsősorban a számítógépen tárolt és feldolgozott adatok elektronikus védelmével foglalkozik, de ahol szükséges, kitér a biztonság és a védelem más aspektusaira. A szabályozás jelen esetben nem a szűken vett jogi szabályozás, hanem a szakterületen alkalmazható bármely szabályzási módszer, így a szabványosítás és a belső szabályozás is. Másrészről viszont első sorban az állam szempontjából kerül megközelítésre a szabályozandó terület, ezért a gyakorlati részben már csak az állam által alkalmazható szabályozások kerülnek kifejtésre.

A *miért* szükséges az informatikai biztonsági kontrollok bevezetése kérdés megválaszolására a bevezető első részében leírtak alapján kevéssé van szükség, de az értekezésben elemzésre kerül mind a veszélyeztetettség, mind a veszélyeztető tényezők összessége.

Fő cél a *hogyan* és a *mennyire* kérdések megválaszolása. A szabályozási módszerek gyakorlati megvalósításának elemzése mellett a kutatási eredményeket egyesítő megfeleltetés készült, amellyel az adatvédelemre vonatkozó jogszabályi követelményekből a szabványok alkalmazásával meghatározásra került az az informatikai biztonsági minimum, ami megkövetelhető, a kötelezett részéről is belátható, hogy szükséges, és csökkenti azt a jogbizonytalanságot, amely a jogalkotó esetenként nagyvonalú maximalizmusából fakad.

A tudományos problémát tehát az jelenti, hogy a heterogén informatikai biztonsági szabályozás hazánkban olyan követelményeket támaszt a kötelezettek felé, amelyeket nehéz egyértelműen meghatározni. Ezzel a szabályozás hatékonysága romlik és a jogbizonytalanság is növekszik.

A kutatás célja a jelenlegi szabályozási gyakorlat feltérképezése és az esetlegesen hiányos részek „kipótlása”, tehát a nem megfelelő mértékben szabályozott területeken az alkalmazás megkönnyítése.

Az értekezés hipotézisei a következőek:

1. Az informatikai biztonság szabályozása ma Magyarországon nem egyenszilárdságú, és a különböző mértékben szabályozott területek egymástól megkülönböztethetőek és kategorizálhatók.
2. A jogilag felületesen szabályozott területeken a jogszabályok által leírt informatikai biztonsági követelmények a szakterületen alkalmazott valamely szabvány bizonyos pontjainak megfeleltethetőek és így jól meghatározott informatikai biztonsági szabályrendszert alkotnak.

Az elméleti és gyakorlati részek alkalmazott kutatásként a szummatív értékelés és az orientációs kutatás módszereit ötvözik. A megfeleltetés kvalitatív kutatásként, objektív osztályozási (COBIT[12] területek elsődlegessége) és empirikus elemek (bevált gyakorlat) felhasználásával készült el.

A dolgozat elméleti és gyakorlati részekre tagolódik, amelyen belül a különböző szabályozási módszerek képezik az alfejezeteket. A dolgozat másik fontos része a függelékben kapott helyet, bár kerülhetett volna a törzsrészbe is. A leválasztás oka az a nem titkolt gyakorlati cél volt, hogy az egy önálló anyagként a szakma által már ismert formátumban azonnal alkalmazható legyen a gyakorlatban, lehetővé téve a kvalitatív kutatás kísérleti módszerének azonnali végrehajthatóságát.

[12] Control Objectives for Information and Related Technology, részletesen ld. az azonos című fejezetben

3. A tudományos eredmények összefoglalása

A kutatómunka során elért tudományos eredmények a következőek:

1. tézis: Az informatikai biztonság szabályozása ma Magyarországon nem egyenszilárdságú, és a különböző mértékben szabályozott területek egymástól megkülönböztethetőek és kategorizálhatók.

Igazolva látom a felállított hipotézist, tudományos eredményként értékelendő *A szabályozás gyakorlata* című fejezet *Jogi szabályozás* című alfejezetében felállított csoportosítás és annak részletes alátámasztása a hatályos magyar jogi szabályozás informatikai biztonságra vonatkozó tételes rendelkezéseinek besorolásaival.

2. tézis: A jogilag felületesen szabályozott területeken a jogszabályok által leírt informatikai biztonsági követelmények a szakterületen alkalmazott valamely szabvány bizonyos pontjainak megfeleltethetőek és így jól meghatározott informatikai biztonsági szabályrendszert alkotnak.

Tudományos eredményként értékelhető, hogy az értekezés második tézise bizonyításra került, a függelékben elhelyezett megfeleltetés biztosítja az adatvédelmi törvényben meghatározott informatikai biztonsági szabályok értelmezhetőségét. A megfeleltetés a gyakorlatban használható és annak alkalmazása javasolt. A további kutatásoknak is megfelelő kiinduló pontot adnak a jelenlegi kutatási eredmények, a folyamatos tartalmi és elméleti-módszertani fejlesztés lehetősége adott.

A robbanásszerű infokommunikációs, és az ezzel párhuzamosan bekövetkező társadalmi, gazdasági fejlődés – mely az információs társadalom, mint magasabb szintű társadalmi fejlettség felé mutat – eredményeképp egyre kiszolgáltatottabbak vagyunk az informatikának és így az informatikai bűncselekményeknek elkövetőinek is. Az információs társadalomhoz vezető utak legfontosabb ösvénye az elektronikus írásbeliség. Ezen új típusú írásbeliségnek vannak bizonyos problémái, amelyek várhatóan jelentkezni fognak. Az informatikának való kiszolgáltatottság és az elektronikus írásbeliség már most

látható problémái együttesen vezetnek olyan biztonsági kockázathoz, amelyben a véletlen események mellett jelentős szerepe van az informatikai bűncselekményeknek elkövetőinek is. Ezek az elkövetők és cselekményeik is jól kategorizálhatók. Ezen informatikai bűncselekmények a cyberterrorizmus építőkövei. A cyberterrorizmus elleni védekezés a terrorizmus és az informatikai bűncselekmények oldaláról is megközelíthető. A cyberterrorizmus a támadás bekövetkezésének valószínűségétől függetlenül – amennyiben az nullától különböző – valós veszélyforrásnak tekintendő, ugyanúgy, mint például egy, a Magyar Köztársaság elleni fegyveres támadás. Ebből következően az ellene való védekezés legalább tervezési, szervezési szinten szükséges és állami feladat. Az egyedi informatikai támadások oldaláról tekintve a védelem minden üzemeltetőnek és felhasználónak érdeke és kötelessége.

A fenti összetett veszélyforrások elleni védekezés eszközei között kiemelt szerepet foglal el a szabályozás. A jogi szabályozás a támadások tiltásának, az ellenőrzések végrehajtásának és a biztonsági irányelvek meghatározásának elsődleges eszköze, de hatással van a tervezett biztonság, az elrettentés, a rendszer megerősítése, a biztonsági mentés és a reagálás kialakítására is. A szabványosítás a megelőzés vagy elfogás, a jelzések és figyelmeztetések, a rendszer megerősítése, a csoportokba osztás és feltartóztatás, a leállítás és újraengedélyezés, a biztonsági mentés, az ellenőrzések végrehajtása, a biztonsági irányelvek meghatározása és a helyreállítás területén határozza meg a követendő technikai szabályokat. Önmagában persze a szabályozás nem nyújt megfelelő védelmet, de a védelem alapjainak meghatározásához alkalmazása elengedhetetlen.

A kutatás feltárta a szabályozás lehetséges formáit, valamint a létező szabályozás eseteit. A hatályos magyar jogi szabályozást kategorizálta, az alkalmazás mértékét, a konkrét jogszabályok vonatkozó részeit elemezte.

Az informatikai biztonság jelenlegi magyar szabályozása négy csoportra bontható. Az indirekt szabályozásba sorolhatóak azok a jogszabályok, amelyek csak közvetve írnak elő követelményt a szakterületre, a szabályok megsértését szankcionálják. Az önkéntes –önszabályozott területeken a biztonsági kontrollokat a piaci igények teszik szükségessé. A felületesen szabályozott csoportban kötelezően betartandó előírások vannak, szankciók kilátásba helyezésével, viszont a szabályok a kötelezettek számára pontosan nem ismertek. Ebbe a kategóriába

tartozik az adatvédelmi törvény, amely a szankciórendszer miatt különleges figyelmet igényel. A részletesen szabályozott kategóriában a biztonsági előírások megfelelő mélységben kifejtésre kerültek, függetlenül attól, hogy azok betartása ellenőrzésre került-e.

Jelenleg az informatikai biztonság jogi szabályozása kapcsán szakadék tapasztalható a jogalkotás és jogalkalmazás (jogászok) valamint az intézkedések végrehajtói (informatikusok) között. Ennek oka, hogy a jogi követelmények mögötti technikai tartalom nem ismerhető fel könnyen. A követelmények felületesek, amelynek fő oka a technológiafüggetlenség, de a felületesség a jogalkalmazást rendkívüli módon megnehezíti. Például kérdéses, hogy „az adatkezelő [...] köteles gondoskodni az adatok biztonságáról”[13] kitétel pontosan mit takar, víruskeresőt, biztonsági mentést DVD-re, offsite backupot, vagy komplex külső auditot az ISO/IEC 27001-nek való megfelelésről? Lehetne erre azt válaszolni, hogy a vonatkozó szabványoknak való megfelelést, no de milyen mértékben? Az informatikus erre józan ésszel próbálja felmérni, hogy mit érdemes bevezetni, de hol van a gondatlanság határa? Egy esetleges káresemény kapcsán hogyan lehet jogi úton kártérítést követelni?

A problémát felismerve és elemezve a kutatás célja volt olyan megoldást találni, amely mindkét fél számára támpontot nyújthat. A szabványoknál bemutatott COBIT megfelelőnek tűnik arra, hogy egységes keretrendszerként alkalmazzuk, amikor az IT biztonság és vezetés kérdéskörében valamely átfogó szabályrendszert alkalmazunk. A COBIT-ot már sok más szabályrendszernek is megfeleltették korábban, többek között az ISO/IEC 17799, PMBOK, ITIL, PRINCE2, COSO ERM, NIST FISMA szabványoknak, valamint a Sarbanes-Oxley törvénynek is. A második tézis az volt, hogy a COBIT követelményeit valamely IT biztonságra vonatkozó anyagi jogi jogszabállyal összerendelve, azokat kölcsönösen megfeleltetve, a COBIT részletesebb leírása alapján implementálni lehet a jogszabályban foglalt követelményeket, mintegy lefordítva az informatika nyelvére. Választásunk az adatvédelmi törvényre esett, mert az kellően kisszámú IT biztonsági követelményt fogalmaz meg. Továbblépve, ha több jogszabály kerül megfeleltetésre, akkor ha egy jogalkalmazóra több megfeleltetett jogszabály vonatkozik, egyszerűen veszi az összes

[13] 1992. évi LXIII. tv. 10. §.

követelményhalmaz unióját, és ha megfelel az ebben foglalt közös szabályoknak, akkor teljesítette az összes jogszabály által rá rótt kötelezettséget az IT biztonság területén.

Az idea megvalósításaként a fenti megfeleltetésekkel azonos formátumban készült az adatvédelmi törvény COBIT-nak való megfeleltetése is, amelynek nem rejtett célja az, hogy szakmai körökben használható és az ISACA magyar és nemzetközi vezetősége által is elfogadható, könyv formátumában kiadható dokumentum készülhessen. Ez a megfeleltetés a mű 1. sz. függelékét képezi. A megfeleltetés oly módon történt, hogy a COBIT minden egyes kontroll célkitűzéséhez[14] – ha az lehetséges volt – párosításra került az adatvédelmi törvény egy bekezdése. A lefedettség (megfeleltethetőség) mértéke négy szinten került meghatározásra:

- (F) Felülmúlt: az adott kontroll célkitűzést az Avtv. informatikai biztonsági tartalmi szempontból felülmúlja
- (T) Teljes lefedettség: az adott kontroll célkitűzésnek az Avtv. informatikai biztonsági szempontból teljes mértékben megfelel
- (R) Részleges, valamely szempont(ok) lefedve: az adott kontroll célkitűzésnek az Avtv. informatikai biztonsági szempontból részlegesen megfelel, tehát nem a teljes kontroll célkitűzést írja elő a jogszabály
- (N) Nincs lefedve: az adott kontroll célkitűzés teljesülését az Avtv. nem írja elő

A törvényi követelmények alapvetően a bizalmasság, sértetlenség és rendelkezésre állás információ-kritériumok köré csoportosulnak. Ez nem meglepő, hiszen a jogi követelmények alkalmazásáról szóló fejezetben is látszik, hogy mind az Avtv., mind az adatvédelmi irányelv, mind pedig a külföldi nemzeti jogszabályok is ezeket tekintik a legfontosabbnak. Ebből következően ahol a COBIT maga ezeket az információ-kritériumokat valamely kontroll célkitűzése tekintetében elsődleges jelentőségűnek tartotta,[15] ott az Avtv. 10. § (1) bekezdése ezen objektív okok miatt megfeleltetésre került. Az Avtv.-ben meghatározott általános követelmények emellett is igen sok kontrollnak megfeleltethetőek voltak, bár kevésbé meghatározott módon. Ezek a megfeleltetések szakmai

[14] A kontroll célkitűzés (control objective) a COBIT-ban alkalmazott legkisebb követel ményegység.

[15] ld. COBIT 4.1 II. Melléklet - Az informatikai folyamatok leképezése az informatikai irányítás I központi
területekre, A COSO-ra, COBIT informatikai erőforrásokra. p. 200

mérlegelés és egyeztetés útján alakultak ki, tehát tartalmaznak szubjektív elemeket. A széleskörű szakmai vita és a többkörös egyeztetés jelentősége éppen ezeknek a szubjektív elemeknek a bevált gyakorlattá való átformálását szolgálják. Az ilyen jellegű anyagoknak nincs végleges állapota. Ha elfogytak a jelenlegi állapottal kapcsolatos jobbító javaslatok, akkor a jogszabályi és a szabványváltozatok lekövetése miatt szükséges változtatni. Előre látható változás például a COBIT 5 megjelenése,[16] amely szintén szükségessé teszi a követő felülvizsgálatot.

Megfontolandó elméleti-módszertani bővítés lehetne továbbá a Rátai Balázs által kitalált funkcionális köztes modell[17] alkalmazása, amellyel funkcionális szempontból megközelítve a jogi szabályozás és a szabványosítás, valamint a tényleges gyakorlat követelményeit, egy köztes összerendelő modellt lehetne kiépíteni. A rendkívül jó megközelítés hátránya, hogy jelentős energia-befektetést és egy kutatócsoport munkáját igényelte volna a vizsgálat, így jelen disszertációban nem tudtam ilyen köztes modellt kialakítani, viszont a későbbiekben ez ígéretes kutatási feladat lehet.

Összességében a szerző véleménye szerint a disszertáció, és annak fő újdonsága, a megfeleltetés a gyakorlatban használható és annak alkalmazását javasolja is. A további kutatásoknak is megfelelő kiinduló pontja a mű, a folyamatos tartalmi és elméleti-módszertani fejlesztés lehetősége adott.

[16] ISACA: COBIT 5 Initiative – Status Update. http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-5-Initiative-Status-Update.aspx [2010. 08.24.]

[17] Rátai Balázs: Legal compliance audit based on an intermediate model. http://www.carneades.hu/index.php?option=com_content&view=article&id=3&Itemid=6 [2010. 05. 12.]

4. Kapcsolódó publikációk

4.1. Idegen nyelvű tanulmányok

Szádeczky Tamás: *Problems of Digital Sustainability,* Acta Polytechnica Hungarica, Journal of Applied Sciences, 2010. VII. évf. 3. sz. ISSN 1785-8860 pp. 123-136.

Szádeczky Tamás: *IT Security Regulation and Practice in Hungary*, New challenges in the field of military sciences 2010 konferencia kiadványa ISBN 978-963-87706-6-0

Szádeczky Tamás: *Pillars of IT Security*, Studia Iuridica Auctoritate Universitatis Pécs Publicata, 2010. 147. sz. pp. 247-268 ISSN 0324-5934

Szádeczky Tamás: *Terrorism in cyberspace*, XXIV. Nemzetközi Kandó Konferencia 2008 konferencia kiadvány, BMF, 2008. ISBN 978-963-7154-74-4

Szádeczky Tamás: *IT security standards in the field of military*, Bolyai Szemle, 2007. XVI. évf. 1. sz. p. 160-171. ISSN 1416-1443

Szádeczky Tamás: *IT security standards in the field of military*, Hadmérnök különszám, 2006. ISSN 1788-1919

4.2. Magyar nyelvű tanulmányok

Bíró János – Szádeczky Tamás – Szőke Gergely László: A hírközlési szolgáltatók értesítési kötelezettsége a személyes adatok megsértése esetén (Data Breach Notification) Infokommunikáció és jog, 2011. VIII. évf. 43. sz. ISSN 1786-0776

Szádeczky Tamás: *Komplexen az informatikai központok biztonságáról*, Detektor Plusz, 2009. XVI. évf. 10-11. sz. pp. 34-35. ISSN 1217-9175

Szádeczky Tamás: *Térfigyelés és adatvédelem,* Detektor Plusz, 2009. XVI. évf. 8-9. sz. pp. 31-32. ISSN 1217-9175

Szádeczky Tamás: *Az elektronikus írásbeliség és problémái*, Infokommunikáció és jog, 2009. VI. évf. 3. sz. pp. 67-72. ISSN 1786-0776

Szádeczky Tamás: *Terrorizmus a kibertérben*, Infokommunikáció és jog, 2008. V. évf. 6. sz. pp. 200-205. ISSN 1786-0776

4.3. Tansegédletek

Információbiztonsági kontrollok, Budapesti Műszaki Főiskola, Kritikus infrastruktúrák védelme, információbiztonság tárgy, 2009.

Jogi védelem formái és elemei, Budapesti Műszaki Főiskola, Kritikus infrastruktúrák védelme, információbiztonság tárgy, 2009.

Tansegédlet: *Electronic documents, signature and archiving*, Summer School on European Information Law, Wroclaw, Lengyelország, 2008.