HADMÉRNÖK
VÉDELMI ELEKTRONIKA, INFORMATIKA, KOMMUNIKÁCIÓ

14. évfolyam (2019) 3. szám 113–128.
DOI: 10.32567/hm.2019.3.10

Nagyné Takács Veronika[1]

Hogyan írjunk informatikai biztonsági szabályzatot?

How to Write an IT Security Regulation?

A tanulmány a jogszabályi környezet áttekintésével, az előírások számbavételével és rendszerezésével, továbbá személyes tapasztalatok megosztásával kívánja segíteni azokat, akik munkájuk során informatikai biztonsági szabályzat előkészítését, megírását kapták feladatul, vagy személyes kíváncsiságból érdeklődnek a téma iránt.

Kulcsszavak: **információbiztonság, szabályozás, informatikai biztonsági szabályzat**

The study aims to help those who have been involved in the preparation and writing of the IT Security Regulation, or personally interested in it in their work, by reviewing the legal environment, listing and organising the regulations, and sharing personal experiences of the author.

Keywords: **information security, regulation, information security regulation**

Bevezetés

Bizonyára sokan emlékeznek Umberto Eco[2] *Hogyan írjunk szakdolgozatot?* című, Magyarországon 1992-ben megjelent könyvére [1], amelyben főiskolások, egyetemisták számára adott módszertani útmutatót életük első nagyobb lélegzetű tudományos munkájának megírásához.

Jelen tanulmány címe így nem titkoltan Ecótól ered, egyben utólagos köszönet az akkoriban jókor érkezett segítségért, és nagyon szerény tisztelgés a nagy tudású író emléke előtt, aki regényei, tanulmányai, publicisztikája mellett egy hasznos, ugyanakkor szórakoztató segédlet megírására is energiát fordított.

[1] Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: takacs.veronika2016@gmail.com, ORCID: https://orcid.org/0000-0002-4868-5622

[2] Umberto Eco (1932–2016) olasz író, irodalomkritikus és filozófus. *Hogyan írjunk szakdolgozatot?* című esszéjét magyarul a Gondolat Könyvkiadó adta ki 1992-ben, Budapesten, Klukon Beatrix fordításában.

Az *Informatikai biztonsági szabályzat* (a továbbiakban: IBSZ) megírásához készítendő módszertani útmutató szükségessége már saját tapasztalatokon alapuló felismerés. A cikk előzménye közel tízévnyi IBSZ-írási tapasztalat (eredmény és kudarc) és többéves tudományos kutatás, célja pedig az előzőkből származó felismerések megosztása annak érdekében, hogy mások számára az IBSZ megírásához szükséges előkészületi időszak, illetve maga a kidolgozás folyamata lerövidülhessen. A cikk – természetesen – elfogult nézőpontból közelít a kérdéshez: a szerző hisz abban, hogy a szabályozás nem felesleges adminisztrációs teher, hanem egy adott szervezet működését és az ott dolgozók munkavégzését támogató tevékenység, amit – mint minden mást – érdemes jól végezni, így eredményeit is lehet hasznosítani.

A cikk az alábbi kérdésekre adható/adandó válaszok áttekintésével és néhány gyakorlati tanáccsal – nem kizárólagosságra törekedve és nem konkrét, *egy az egyben* használható mintadokumentum átnyújtásával – kívánja segíteni az IBSZ-írás iránt önszorgalomból vagy kötelezettség alapján érdeklődőket:

- Miért van szükség az IBSZ-re?
- Milyen szabályozási környezetben szükséges elhelyezni az IBSZ-t?
- Mit tartalmazzon és hogyan az IBSZ?

Az IBSZ és szükségessége

Az IBSZ az infokommunikációs eszközöket tevékenysége során alkalmazó (azaz ma már szinte minden) szervezet egyik szabályozási alapdokumentuma. Tartalmazza – tartalmaznia kell – mindazon előírásokat, amelyek az adott szervezetnél az infokommunikációs eszközök rendeltetésszerű és biztonságos használatához szükségesek, ezért kötelezően alkalmazandók.

Az IBSZ megírásának szükségességét a szakmai konszenzust tükröző szabványok, ajánlások évtizedek óta rögzítik és hangsúlyozzák. A nemzetközi példákat követve a hazai Informatikai Tárcaközi Bizottság (ITB)[3] 8. és 12. számú ajánlásai 1994-ben és 1996-ban, majd a Közigazgatási Informatikai Bizottság (KIB)[4] 25. számú ajánlása 2008-ban alapvető dokumentumnak tekintették az IBSZ-t [2: 115.], [3: 29.], [4: 49.]. Az információbiztonsági szabványok fejlődéstörténetének bemutatása meghaladná

[3] A 3296/1991. (VII. 5.) Korm. határozat alapján a Miniszterelnöki Hivatal (MeH) közigazgatási államtitkárának irányításával létrehozott, a MeH-en belül működő Informatikai Koordinációs Iroda tevékenységére támaszkodó ITB a kormányzati informatikai (elsősorban fejlesztési) feladatok összehangolásáért volt felelős. Feladatai közé tartozott – az 1066/1999. (VI. 11.) Korm. határozat szerint – a kormányzati informatikai fejlesztések stratégiai tervezésében való közreműködés, a kiemelkedő jelentőségű kormányzati informatikai részterületek szakmai koncepcióinak kidolgozása és megvalósulásuk figyelemmel kísérése, kormányzati informatikai ajánlások kidolgozása, több tárcát érintő informatikai rendszerek létrehozásával, korszerűsítésével kapcsolatos koordináció végrehajtása.

[4] Az 1026/2007. (IV. 11.) Korm. határozattal – három korábbi tárcaközi bizottságból – létrehozott KIB koordinációs fórumként támogatta a stratégiai szintű közigazgatási informatikai programok tervezését, végrehajtását, az infokommunikációs technológiák, eszközök közigazgatáson belüli terjesztését, szabályozásokat kezdeményezett és ajánlásokat készített az informatika közigazgatáson belüli alkalmazásának támogatásához. A KIB elnöke a közigazgatási informatikáért felelős kormánybiztos volt, tagjai a központi államigazgatási és az önkormányzati igazgatási szervek delegáltjai, valamint a közigazgatási informatikai fejlesztésekben érintett szervezetek képviselői. A KIB munkáját albizottságok segítették.

jelen munka kereteit, a témában lásd például Muha Lajos és Krasznay Csaba Nemzeti Közszolgálati Egyetemen készült tananyagát [5: 26–36.].

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) megjelenését követően a törvény hatálya alá tartozó szervezetek vezetői számára „a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályok" rögzítése és az informatikai biztonsági szabályzat kiadása jogszabály alapján előírt kötelezettséggé vált [6]. A jogalkotó maga gondoskodott arról, hogy az IBSZ kiadása a vezető megbízásából eljáró, neki felelős személy feladatkörébe kerüljön; a szabályzat kiadásának előkészítését az elektronikus információs rendszer védelméért felelős személy feladatává tette [6].

Az Ibtv. hatálya alá tartozó szervezetek IBSZ-eit az Ibtv. hatálya alá tartozó elektronikus információs rendszerek biztonságának felügyeletét ellátó, a kormány által kijelölt hatóság, a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) nyilvántartja és kezeli [6].

Az IBSZ helye a szabályozási rendszerben

A szabályozási tevékenység céljáról, tartalmáról, módszeréről (egyes szkeptikusok szerint: értelméről) való gondolkodás meghaladná jelen munka kereteit, így a szabályozás – általában vett és tudomásul vett – szükségességét a szerző alapvetésként kezeli. Kitekintésként mindössze annyi megjegyzést érdemes tenni, hogy nem az információvédelem az egyetlen terület, ahol a szabályozás jogszabályban foglalt kötelezettség. *A köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről* szóló 1995. évi LXVI. törvény (Ltv.) a hatályba lépésének napjától (1995. 06. 30.) előírta a közfeladatot ellátó szervek számára iratkezelési szabályzat kiadását [7], *a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról* szóló 1992. évi LXIII. törvény (Avtv.) 2004. január 1-jétől a belső adatvédelmi felelős feladataként határozta meg belső adatvédelmi és adatbiztonsági szabályzat készítését [8] – az előírás az Avtv.-t hatályon kívül helyező *az információs önrendelkezési jogról és az információszabadságról* szóló 2011. évi CXII. törvényben (Info tv.) is szerepel [9], *a számvitelről* szóló 2000. évi C. törvény (Számv. tv.) szintén hatályba lépésétől (2000. 09. 21.) rögzíti kötelezettségként a gazdálkodók esetében, hogy a számviteli politika keretében el kell készíteni az eszközök és a források leltárkészítési és leltározási szabályzatát, az eszközök és a források értékelési szabályzatát, az önköltségszámítás rendjére vonatkozó belső szabályzatot, a pénzkezelési szabályzatot [10]. A felsorolás nem teljes, ez nem is cél, inkább bevezető a további megállapításokhoz.

Az IBSZ tehát jogszabály által előírt szabályzat. *A szabályzat*, amennyiben az információvédelem általános tárgyköréről van szó. Az IBSZ további – információvédelmi tárgyú – szabályozóeszközök kiindulópontja is lehet (tehát *alapszabályzat*). De az IBSZ csak *egy szabályzat*, amennyiben egy szervezet jogszerű működésének szabályozásáról van szó.

Fentiekből következik, hogy fogalomhasználatában, tartalmában, szerkezetében illeszkednie kell a szervezet egyéb belső szabályozóeszközeihez, és lehetővé kell tennie, elő kell segítenie további szabályozóeszközök kidolgozását.

Ezért amikor az IBSZ megírásáról vagy újraírásáról születik döntés, alapul lehet venni a szervezet korábbi, akár az éppen hatályos IBSZ-ét vagy más szervezetek IBSZ-eit (az internet e tekintetben számos forrással szolgálhat); a lényeg az aktuális szabályozási rendszer figyelembevétele és a kidolgozandó dokumentum ehhez illesztése.

Egy szervezet szabályozási rendszerét részben a jogszabályok, de – a részletek tekintetében – leginkább saját felépítése és tevékenysége, valamint hagyományai határozzák meg. *A jogalkotásról* szóló 2010. évi CXXX. törvény (Jat.) szerint az arra jogosultak *közjogi szervezetszabályozó eszközök*ben *(normatív határozat* és a *normatív utasítás)* rögzíthetik a szervezetre és a működésre, valamint a tevékenységre vonatkozó előírásokat [11]. Az egyes – már idézett – jogszabályok a szervezet vezetője által kiadott *szabályzatok*ra hivatkoznak. A belső szabályozóeszközök körébe az egyes szervezeteknél leggyakrabban a *szabályzatok*, az *utasítások*, az *eljárásrendek*, a *munkautasítások* tartoznak, ezek pontos fogalma, hatálya, tartalma azonban szervezetenként eltérő. Ugyancsak jelentős eltérést mutat a szabályozóeszközök hierarchiája, egymáshoz való viszonya. Egyes szervezeteknél kizárólag a szervezet első számú vezetőjének van szabályozási joga, azaz ő adhat ki szabályozóeszközt. Más szervezeteknél a szabályozási jog különböző vezetői szintekre lett telepítve.

Az Ibtv. végrehajtási rendelete, *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről* szóló 41/2015. (VII. 15.) BM rendelet (a továbbiakban: 41/2015. BM rendelet) 4. melléklete – a *szabályzatok* mellett – *eljárásrendek* kialakítását és rögzítését írja elő, és elvárásként rögzíti azt is, hogy az eljárásrendeket megsértő személyekkel szemben szankciót kell alkalmazni [12]. A 41/2015. BM rendelet 2. melléklete *munkautasítást*, *belső rendelkezést*, *szabályozást, vagy más erre a célra szolgáló* dokumentumot (*együtt: szabályzat*ot) említ [12].

A szervezeti szabályozási rendszerbe illesztés követelménye a fentieken túl azt is jelenti, hogy ha egy szervezet a szabályozás kidolgozására külső erőforrást vesz igénybe – számos vállalkozás van a piacon, amely IBSZ és egyéb szabályozóeszközök jogszabály- vagy szabványkonform elkészítését vállalja –, ügyelni kell arra, hogy a külső szakértők által elkészített (kellően absztrahált, így több szervezet felé is kiajánlható) dokumentumminta szervezetre adaptálása, testreszabása kellő mértékben megtörténjen. Ha erre a testreszabásra nem kerül sor, az IBSZ külső dokumentum marad, ennek minden következményével. Ha elmarad, későbbre halasztódik a szervezeti szabályozási rendszerbe illesztés, a szervezettől idegen fogalomhasználat, tartalom és szerkezet esetén nehezebbé válik az IBSZ értelmezése és alkalmazása, és természetesen nehezebbé válik az IBSZ alapján elkészítendő további szabályozóeszközök kidolgozása is.

Az IBSZ kiadásával az információvédelmi szabályozás jogszabályban elvárt feladata még korántsem teljesül. A 41/2015. BM rendelet 4. mellékletének 3. alcíme szerinti *Védelmi intézkedés katalógus*ban meghatározott szabályozási kötelezettségeket az 1. táblázat 1. és 2. oszlopa foglalja össze.

1. táblázat

Szabályozási kötelezettségek [a szerző saját szerkesztése]

41/2015. Korm. rendeletben nevesített vagy hivatkozott szabályozóeszköz		Az IBSZ tartalmára vonatkozó előírás
szabályzat	***eljárásrend***	
Informatikai biztonsági szabályzat (IBSZ) *3.1.1.1.*[5]		
Kockázatelemzési és kockázatkezelési szabályzat *3.1.2.1.1.1.*	Kockázatelemzési és kockázatkezelési eljárásrend *3.1.2.1.*	kockázatelemzés (amely szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz) *3.1.1.1.3.1.*
általános beszerzési szabályzat[6] *3.1.3.1.1.1.*	Beszerzési eljárásrend *3.1.3.1.*	az elektronikus információs rendszer (ideértve ezek elemeit is) és információtechnológiai szolgáltatás beszerzés (ha az érintett szervezet ilyet végez vagy végezhet) *3.1.1.1.3.3.*
Üzletmenet-folytonosságra vonatkozó szabályzat *3.1.4.1.1.1.*	Üzletmenet-folytonosságra vonatkozó eljárásrend *3.1.4.1.*	üzlet-, ügy- vagy üzemmenet-folytonosság tervezése (így különösen a rendszerleállás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása stb.) *3.1.1.1.3.9.*
	Biztonsági eseménykezelési eljárásrend *3.1.5.1.*	biztonsági helyzet- és eseményértékelés eljárási rendje *3.1.1.1.3.2.*, a biztonsági események – ideértve az adatok sérülését is – bekövetkeztekor követendő eljárás, ideértve a helyreállítást *3.1.1.1.3.15.*
	Személybiztonsági eljárásrend *3.1.6.1.* *belső szabályozás*ban rögzített eljárás a jogviszony megszűnésekor *3.1.6.4.* *belső eljárási rend* szerint fegyelmi eljárás kezdeményezése *3.1.6.7.1.1.*	az emberi erőforrásokban rejlő veszélyek megakadályozása (például személyzeti felvételi és kilépési eljárás során követendő szabályok, munkavégzésre irányuló szerződésben a személyes kötelmek rögzítése, a felelősség érvényesítése stb.) *3.1.1.1.3.6.*

[5] A könnyebb azonosíthatóság érdekében minden esetben feltüntetésre kerül az előírás *Védelmi intézkedési katalógus* szerinti sorszáma.

[6] Dőlt betűvel vannak jelezve a nem konkrét (néven nem nevezett) szabályozóeszközökre történő utalások (amelyek jellemzően egy-egy tevékenység szabályozásának előírásakor jelennek meg).

41/2015. Korm. rendeletben nevesített vagy hivatkozott szabályozóeszköz		Az IBSZ tartalmára vonatkozó előírás
szabályzat	***eljárásrend***	
*belső szabályzat*ban meghatározott, interneten megvalósuló tevékenység tiltása (például chat, fájlcsere, nem szakmai letöltések, tiltott oldalak, nem kívánt levelezőlisták stb.) *3.1.6.9.1.2*		
Képzési szabályzat *3.1.7.2.1.1.*	Képzési eljárásrend *3.1.7.2.*	az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében *3.1.1.1.3.7.*
(*elektronikus információbiztonsági vagy egyéb szabályzat* részét képező) Fizikai védelmi szabályzat *3.2.1.2.1.1*	Fizikai védelmi eljárásrend *3.2.1.2.*	fizikai és környezeti védelem szabályai, jellemzői *3.1.1.1.3.5.*
Biztonságtervezési szabályzat *3.2.2.1.*		biztonsággal kapcsolatos tervezés (például beszerzés, fejlesztés, eljárásrendek kialakítása) *3.1.1.1.3.4.*
	az elektronikus információbiztonsággal kapcsolatos (ideértve a rendszer- és felhasználói, külső és belső hozzáférési) engedélyezési folyamatok kialakítása, dokumentálása és kihirdetése *3.3.1.1.1.*	
	az elektronikus információs rendszer más elektronikus információs rendszerhez kapcsolódásának *szabályozás*a és belső engedélyhez kötése *3.3.1.3.1.1.*	szabályrendszer felállítása és alkalmazása a külső elektronikus információs rendszerekhez való kapcsolódáshoz *3.3.1.3.3.*
Biztonságértékelési szabályzat *3.3.4.1.1.1.*	Biztonságelemzési eljárásrend / Biztonságértékelési eljárásrend *3.3.4.1.*	
	elektronikus információs rendszer tesztelésével, képzésével és felügyeletével kapcsolatos eljárások megfogalmazása, dokumentálása és kihirdetése *3.3.5.1.1.*	

41/2015. Korm. rendeletben nevesített vagy hivatkozott szabályozóeszköz		Az IBSZ tartalmára vonatkozó előírás
szabályzat	*eljárásrend*	
Konfigurációkezelési szabályzat *3.3.6.1.1.1.*	Konfigurációkezelési eljárásrend *3.3.6.1.*	
a szoftver használatra meghatározott *szabályzatok* *3.3.6.7.2.2.*		
szoftvertelepítésre vonatkozó *szabályok* érvényesítése 3.3.6.11.1.2.		
Rendszer karbantartási kezelési szabályzat *3.3.7.1.1.1.*	Rendszer karbantartási eljárásrend *3.3.7.1.* *folyamat* kialakítása a karbantartók munkavégzési engedélyének kezelésére *3.2.1.19.1.1.*	az elektronikus információs rendszerek karbantartásának rendje *3.1.1.1.3.10.*
Adathordozókra vonatkozó védelmi szabályzat *3.3.8.1.1.1.*	Adathordozók védelmére vonatkozó eljárásrend *3.3.8.1.*	az adathordozók fizikai és logikai védelmének szabályozása *3.1.1.1.3.11.*
Azonosítási és hitelesítési szabályzat *3.3.9.1.1.1.*	Azonosítási és hitelesítési eljárásrend *3.3.9.1.*	az elektronikus információs rendszerhez való hozzáférés során követendő azonosítási és hitelesítési eljárás, és a hozzáférési szabályok betartásának ellenőrzése *3.1.1.1.3.12.*
Hozzáférés ellenőrzési szabályzat *3.3.10.1.1.1.*	Hozzáférés ellenőrzési eljárásrend *3.3.10.1.*	
minden engedélyezett távoli hozzáféréstípusra a felhasználásra vonatkozó korlátozások, a konfigurálási vagy a kapcsolódási követelmények és a megvalósítási útmutatók kidolgozása ás dokumentálása *3.3.10.13.1.1.*		
*belső szabályozás*ban felhasználási korlátozások, konfigurálásra és kapcsolódásra vonatkozó követelmények, valamint technikai útmutató kiadása a vezeték nélküli technológiák kapcsán *3.3.10.14.1.1.*		
*belső szabályozás*ban felhasználási korlátozások, konfigurálásra és kapcsolódásra vonatkozó követelmények, valamint technikai útmutató kiadása az ellenőrzött mobil eszközökre *3.3.10.15.1.1.*		

41/2015. Korm. rendeletben nevesített vagy hivatkozott szabályozóeszköz		Az IBSZ tartalmára vonatkozó előírás
szabályzat	***eljárásrend***	
(az IBSZ részét képező) Rendszer- és információsértetlenségre vonatkozó szabályzat *3.3.11.2.1.1.*	Rendszer- és információsértetlenségre vonatkozó eljárásrend *3.3.11.2.*	
	az elektronikus információs rendszer hibáinak azonosítása, *belső eljárásrend* alapján jelentése és kijavítása vagy kijavíttatása *3.3.11.3.1.1.*	
Naplózásra és elszámoltathatóságra vonatkozó szabályzat *3.3.12.1.1.1.*	Naplózási eljárásrend *3.3.12.1.*	ha az érintett szervezetnek erre lehetősége van, a rendszerek használatáról szóló rendszerbejegyzések értékelése, az értékelés eredményétől függő eljárások meghatározása *3.1.1.1.3.13.*
Rendszer- és kommunikációvédelmi szabályzat *3.3.13.1.1.1.*	Rendszer- és kommunikációvédelmi eljárásrend *3.3.13.1.*	
		az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatok, elvárások, jogok (ha az érintett szervezetnél ez értelmezhető) *3.1.1.1.3.8.*
		az adatok mentésének, archiválásának rendje *3.1.1.1.3.14.*
		az elektronikus információs rendszerhez jogosultsággal (vagy jogosultság nélkül fizikailag) hozzáférő, nem az érintett szervezet tagjainak tevékenységét szabályozó (karbantartók, magán- vagy polgári jogi szerződés alapján az érintett szervezet számára feladatokat végrehajtók), az elektronikus információbiztonságot érintő, szerződéskötés során érvényesítendő követelmények *3.1.1.1.3.16.*

Az IBSZ-en túl konkrét megnevezéssel 14 szabályzat szerepel, ugyanezen címekkel – egy kivétellel – eljárásrend készítését is előírja a jogszabály, további 3 esetben konkrét

megnevezéssel szerepel elkészítendő eljárásrend. Az előzőkön kívül 7(8) esetben[7] szabályzat/szabályozás kialakítását, 5 esetben eljárás, folyamat kialakítását és dokumentálását írja elő a *Védelmi intézkedési katalógus*.[8] Ebből következően az IBSZ mellett a szabályozási rendszer részeit kell, hogy képezzék az említett „tematikus" szabályzatok, eljárásrendek is.[9]

Az *1. táblázat* rögzíti az IBSZ előírt tartalmával (lásd következő fejezet) történt összevetés eredményét is (3. oszlop). Eszerint az IBSZ-ben 17 elektronikus információs rendszerbiztonsággal kapcsolatos területet, tevékenységet kell szabályozni, ezekből 14 esetében szabályzat vagy eljárásrend kiadása is kötelező.

Az IBSZ tartalma

Az Ibtv. és a 41/2015. BM rendelet az IBSZ tartalmára vonatkozó (konkrét és kevésbé konkrét) előírásokat is tartalmaz.

Az Ibtv. alapján az IBSZ-ben a szervezet, valamint – a szervezeten belüli eltérések esetén – a szervezeti egységek biztonsági szintbe sorolásának eredményét és az elektronikus információs rendszerek biztonsági osztályba sorolását rögzíteni kell [6]. A *Védelmi intézkedés katalógus* e tekintetben némileg eltérően fogalmaz: az IBSZ-nek tartalmaznia kell a szervezet elvárt biztonsági szintjét és egyes elektronikus információs rendszereinek elvárt biztonsági osztályát [12]. A két rendelkezés összeolvasásának eredménye: a tényleges és az elvárt biztonsági szintet és osztályokat is rögzíteni kell az IBSZ-ben.

A *Védelmi intézkedési katalógus*ban az adminisztratív intézkedések között első helyen az IBSZ tartalmára vonatkozó előírások szerepelnek. Eszerint az IBSZ-ben rögzíteni kell:

1. a célokat, a szabályzat tárgyi és személyi (a szervezet jellegétől függően területi) hatályát,
2. az elektronikus információbiztonsággal kapcsolatos szerepköröket, a szerepkörhöz rendelt tevékenységet és a tevékenységhez kapcsolódó felelősséget, valamint az információbiztonság szervezetrendszerének belső együttműködését,
3. az elektronikus információs rendszerbiztonsággal kapcsolatos alábbi területekre, tevékenységekre vonatkozó előírásokat:
   a) kockázatelemzés (amely szorosan kapcsolódik a biztonsági osztályba és biztonsági szintbe soroláshoz),
   b) biztonsági helyzet- és eseményértékelés eljárási rendje,

[7] A 3.3.10.13.1.1., 3.3.10.14.1.1., 3.3.10.15.1.1. pontban előírtak tartalmukat tekintve eltérők, logikailag és szerkezetileg szinte teljesen azonosak, azonban az első esetben nem szerepel a *belső szabályozásban* történő kiadásra utalás.

[8] A tanulmánynak nem célja a jogszabályokban foglalt szabályozási követelményrendszer értékelése; az előírások tényszerű ismertetésére szorítkozik. Annyit azonban szükséges megjegyezni, hogy a szabályozási koncepció, a fogalomhasználat és szerkesztésmód egyszerűsítése, pontosítása, következetesebbé tétele, illetve a szabályzat – eljárásrend fogalmi tisztázása megkönnyítené az alkalmazást.

[9] A nevesített szabályozóeszközökön kívül a *Védelmi intézkedési katalógus* számos további dokumentum előállítását, kezelését és nyilvántartások felállítását is előírja (például üzletmenet-folytonossági terv – 3.1.4.2.1.1. pont, információbiztonsági architektúraleírás – 3.3.2.5. pont, rendszerbiztonsági terv – 3.3.2.2. pont, adminisztrátori dokumentáció – 3.1.3.4.1.1. pont, karbantartási nyilvántartás – 3.3.7.2.1.6. pont stb.). Tételes felsorolásukat a szerző mellőzi, tekintettel arra, hogy bár a kidolgozásukra, felállításukra vonatkozó kötelezettségeket célszerű a szabályozóeszközökben rögzíteni, ezek nem szabályozóeszközök.

c) az elektronikus információs rendszer (ideértve ezek elemeit is) és információtechnológiai szolgáltatás-beszerzés (ha az érintett szervezet ilyet végez vagy végezhet),
d) biztonsággal kapcsolatos tervezés (például beszerzés, fejlesztés, eljárásrendek kialakítása),
e) fizikai és környezeti védelem szabályai, jellemzői,
f) az emberi erőforrásokban rejlő veszélyek megakadályozása (például személyzeti felvételi és kilépési eljárás során követendő szabályok, munkavégzésre irányuló szerződésben a személyes kötelmek rögzítése, a felelősség érvényesítése stb.),
g) az informatikai biztonság tudatosítására irányuló tevékenység és képzés az érintett szervezet összes közszolgálati vagy munkavégzésre irányuló egyéb jogviszonyban álló alkalmazottainak, munkavállalóinak, megbízottjainak tekintetében,
h) az érintett szervezetnél alkalmazott elektronikus információs rendszerek biztonsági beállításával kapcsolatos feladatok, elvárások, jogok (ha az érintett szervezetnél ez értelmezhető),
i) üzlet-, ügy- vagy üzemmenet-folytonosság tervezése (így különösen a rendszerleállás során a kézi eljárásokra történő átállás, visszaállás az elektronikus rendszerre, adatok pótlása stb.),
j) az elektronikus információs rendszerek karbantartásának rendje,
k) az adathordozók fizikai és logikai védelmének szabályozása,
l) az elektronikus információs rendszerhez való hozzáférés során követendő azonosítási és hitelesítési eljárás, és a hozzáférési szabályok betartásának ellenőrzése,
m) ha az érintett szervezetnek erre lehetősége van, a rendszerek használatáról szóló rendszerbejegyzések értékelése, az értékelés eredményétől függő eljárások meghatározása,
n) az adatok mentésének, archiválásának rendje,
o) a biztonsági események – ideértve az adatok sérülését is – bekövetkeztekor követendő eljárás, ideértve a helyreállítást,
p) az elektronikus információs rendszerhez jogosultsággal (vagy jogosultság nélkül fizikailag) hozzáférő, nem az érintett szervezet tagjainak tevékenységét szabályozó (karbantartók, magán- vagy polgári jogi szerződés alapján az érintett szervezet számára feladatokat végrehajtók), az elektronikus információbiztonságot érintő, szerződéskötés során érvényesítendő követelmények [12],
q) szabályrendszer felállítása és alkalmazása a külső elektronikus információs rendszerekhez való kapcsolódáshoz [12].[10]

A fenti felsorolás 1. pontjában foglaltak rögzítése szabályozási evidencia. A 3. pont az információbiztonsági szabályozás tárgyát rögzíti, ami szervezetenként értelemszerűen eltérő mélységű szabályozást igényel; a lényeg, hogy a felsoroltakból minden

[10] Ez a követelmény nem az IBSZ tartalmi elemeinek felsorolásánál, hanem a logikai védelmi intézkedések között szerepel.

elemre ki kell térni, hiszen az elvárás az információvédelmi tevékenységek teljes körének szabályozása. A *Védelmi intézkedési katalógus* komplexitását, a teljes szervezetre kiterjedő hatókörét – divatos szóval a holisztikus megközelítést – leginkább a fenti felsorolás 2. pontjában előírt kötelező tartalom kapcsán érdemes bemutatni. Az elektronikus információbiztonsággal kapcsolatos szerepkörök, feladatok és felelősségek meghatározása és telepítése a szervezet egészét érinti vertikális és horizontális szempontból is, ezek összefoglalását tartalmazza a 2. táblázat.

2. táblázat

Információbiztonságot érintő szerepkörök, feladatok, felelősségek [a szerző saját szerkesztése]

<table>
<tr><th>Általános</th><th>Informatikai szakmai</th><th>Információbiztonsági, szakmai</th><th>Funkcionális szakterületi</th></tr>
<tr><td>szervezet vezetője
Ibtv.-ben meghatározott feladatok, felelősségek</td><td>informatikai fejlesztési szakterület/szervezeti egység vezetői
speciális, tevékenységhez kötődő vezetői feladatok és felelősség</td><td>információbiztonsági szervezeti egység vezetője/elektronikus információs rendszer biztonságáért felelős személy (IBF)
Ibtv.-ben meghatározott feladatok, felelősségek</td><td>humánpolitikai és képzési szakterület vezetői és munkatársai
jogviszony létesítésével, megszűnésével kapcsolatos, illetve képzési feladatok</td></tr>
<tr><td>minden szervezeti egység vezetője
általános vezetői feladatok és felelősség, idézett jogszabályokban nincs részletezve (például utasítás adása, munka ellenőrzése stb.)</td><td>informatikai üzemeltetési szakterület/szervezeti egység vezetői
speciális, tevékenységhez kötődő vezetői feladatok és felelősség</td><td>információbiztonsági szervezeti egység munkatársai (esetenként privilegizált felhasználók)
IBF támogatása, közreműködés a feladatai ellátásában</td><td>személybiztonsági szakterület vezetői és munkatársai
speciális követelmények érvényesítése, például nemzetbiztonsági ellenőrzéssel, vagyonnyilatkozat-tétellel kapcsolatos ügyintézés stb.</td></tr>
<tr><td rowspan="3">adatgazda (szakmai területek vezetői; az Ibtv. alapján annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik)
az elektronikus információs rendszerek osztályba sorolásánál a szakmai értékelésért felelős (milyen adatokat kezel a rendszer, ezek értéke, meddig szükséges megőrzésük stb.)</td><td rowspan="2">munkatársak (jellemzően privilegizált felhasználók)
az infokommunikációs eszközök üzemeltetésével, fejlesztésével, használatával kapcsolatos jogok és kötelességek, felelősségek, tekintettel arra is, hogy jogosítványaik és így felelősségük is jellemzően meghaladják az átlagos felhasználóét</td><td rowspan="3"></td><td>objektumvédelmi szakterület vezetői és munkatársai
fizikai biztonsági feladatok és felelősségek</td></tr>
<tr><td>jogi szakterület vezetői és munkatársai
szerződésekben érvényesítendő információbiztonsági követelmények rögzítéséről gondoskodás</td></tr>
<tr><td>gazdasági szakterület vezetői és munkatársai
beszerzések, illetve eszköznyilvántartás során érvényesítendő információbiztonsági követelmények teljesítése</td></tr>
</table>

Általános	*Informatikai szakmai*	*Információbiztonsági, szakmai*	*Funkcionális szakterületi*
munkatársak (jellemzően felhasználók) *az infokommunikációs eszközök használatával kapcsolatos jogok és kötelességek, felelősségek*			**ügyvitelszervezési /iratkezelési szakterület vezetői és munkatársai** *iratkezelési, dokumentálási követelmények teljesítése*

Gyakorlati javaslatok

A szabályozási kötelezettségek elméleti áttekintése után következzék néhány megszívlelendő gyakorlati – már az IBSZ konkrét felépítésére, megszövegezésére vonatkozó – javaslat. Az alább megfogalmazottak a szerző IBSZ-írással és már elkészült IBSZ-ek olvasásával, értelmezésével és végrehajtásával, valamint az idézett jogszabályok szabályozásra vonatkozó előírásainak teljesítésével kapcsolatos, közigazgatási, közfeladatot ellátó szerveknél szerzett személyes tapasztalatain alapulnak.

1. Az IBSZ-ben legyen egy nagyon jó fogalomtár, aminek kiindulópontjai legyenek az Ibtv. értelmező rendelkezései, de az egyes fogalmak meghatározása, elkülönítése más fogalmaktól a szervezet egyéb szabályozóeszközeiben szereplő fogalmakra tekintettel történjen. Nem elég, ha a fogalmak meghatározását kimásoljuk jogszabályból, szabványból, internetes forrásból (e tekintetben a Wikipédia segítségül hívása – bár nagyon elterjedt – veszélyes: lehet, hogy a szerző – mindössze egy ember – elfogult vagy akaratlanul pontatlan álláspontját, nem ellenőrzött tudását, ismereteit tükrözi); a fogalmakat értelmezni is kell.

   Klasszikus példa az *esemény, biztonsági esemény* fogalomköre. Az *esemény* szó az ISO/IEC 27000:2018 szabvány szerint: „occurrence or change of a particular set of circumstances" [13], az *ITIL v3 Hungarian Glossary* bővebb magyarázata szerint szolgáltatásüzemeltetési fogalom: „olyan állapotváltozás, amelynek jelentősége van egy konfigurációelem vagy IT-szolgáltatás kezelésében. Az »esemény« kifejezést bármilyen IT-szolgáltatás konfigurációelem vagy megfigyelőeszköz által keltett riasztásra vagy értesítésre használják. Az események általában az IT-üzemeltető személyzet beavatkozását igénylik, és gyakran vezetnek naplózandó incidensekre" [14]. Az Ibtv. szerint a *biztonsági esemény*: „nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül" [6]. Az *esemény* informatikai szakmai (jellemzően üzemeltetői), illetve egyes esetekben a rendszer szakmai (nem informatikai) felügyeletét ellátó szervezeti egység részéről megteendő intézkedést igényel a szervezeten belül. Amennyiben egy esemény az Ibtv. szerinti *biztonsági eseménynek*

is minősül, arról a jogszabály alapján az elektronikus információs rendszer biztonságáért felelős személy köteles tájékoztatni a Nemzeti Elektronikus Információbiztonsági Hatóságot. Amennyiben *súlyos biztonsági esemény* („olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek" [6]) következik vagy következhet be, „amely a rendszert működtető szervezet működéséhez szükséges alapvető információk vagy személyes adatok sérülésével jár, az eseménykezelő központ a védelmi feladatainak ellátása érdekében kötelezheti a szervezetet, hogy a súlyos biztonsági esemény megszüntetése vagy a fenyegetettség elhárítása érdekében szükséges intézkedéseket tegye meg" [6]. Az előírások teljesítése érdekében pontosan tudni – szabályozásban rögzíteni – kell, hogy az *események* közül melyek minősülnek *biztonsági eseménynek* és *súlyos biztonsági eseménynek*.

2. Az IBSZ-ben a fogalomhasználat legyen következetes és puritán. A szabályzat ne legyen stilisztikai gyakorlat, ahol ugyanazon fogalomra szinonimákat használunk. Jobb megszokni egy szót és mindig azt alkalmazni; egy idő után már nemcsak a szabályzat írója, hanem olvasója/alkalmazója is ugyanarra a tartalomra fog gondolni a szó elolvasásakor.
3. Az IBSZ ne ismételje meg a jogszabályok rendelkezéseit (csak akkor, ha kifejezetten szükséges – erre a fogalomtár kivételével kevés esetben kerülhet sor). Az IBSZ-nek azt kell rögzítenie, hogy a jogszabályi előírásokat a szervezet az adott esetben hogyan teljesíti.

   Egy példa a *Védelmi intézkedés katalógus*ból: „Független értékelők. Az érintett szervezet független értékelőket vagy értékelő csoportokat alkalmaz a védelmi intézkedések értékelésére" [12]. Az IBSZ-ben nem azt kell rögzíteni, hogy a szervezet külső auditokon győződik meg az intézkedések megfelelőségéről, hanem azt, hogy ki/mely szervezeti egység tervezi meg és készíti elő, támogatja a külső auditokat, ki hagyja jóvá az auditok végrehajtását, azokra milyen gyakorisággal, milyen hatókörben kerül sor, hogyan hasznosulnak az auditok eredményei stb.
4. Az IBSZ ne legyen hosszú. Egy 20–25 A4-es oldal terjedelmet meghaladó dokumentumot már csak a legelszántabbak *kezdenek el* olvasni.
5. Az IBSZ tartalmazzon utalást mindazon szabályozóeszközökre, amelyeket az IBSZ mellett az információbiztonsági szempontból releváns tevékenység során alkalmazni kell. Amennyiben az IBSZ – kézikönyv jelleggel – utal a környező szabályozóeszközökre, megkönnyíti az alkalmazók dolgát, hiszen tudni fogják, milyen témában hol találhatják meg a további előírásokat. Ez a megoldás segíti a szabályozás előkészítőjét is: nem kell megismételnie (módosításkor frissítenie) a máshol már szereplő rendelkezéseket. A hivatkozások elhelyezhetők a szövegben (például „A mentésre, archiválásra vonatkozó részletes előírásokat a Mentési szabályzat tartalmazza."), de célszerű egy szabályozástérképet vagy

szabályozáskatalógust mellékletként csatolni; ez utóbbi a gyors áttekintést teszi lehetővé. A hivatkozások átlátható rendszerének mellékletben történő elhelyezése az IBSZ törzsszövegének terjedelmére is jótékony mérséklő hatással lehet. A korábban leírtak alapján magának a szabályozástérképnek vagy -katalógusnak a tartalma is meglehetősen összetett lesz.

6. Az IBSZ a valóságot rögzítse. A szabályzat létező és azonosítható személyekre, szerepkörökre, szervezeti egységekre telepítse a feladatokat és a felelősségeket. Gyakori megoldás, hogy „a vezető által kijelölt személy" lesz a felelőse egy-egy nehezebb, összetettebb, még nem teljesen pontosan körülhatárolt feladatnak – ez a nyelvi fordulat csak akkor támogatható, ha tudni lehet, ki, mikor, hogyan lett/lesz megbízva a feladattal és erről, illetve az esetleges módosulásról az érintettek hogyan szereznek tudomást. Amennyiben egy még nem létező eljárást, műszaki megoldást kívánunk rögzíteni, ami például egy projekt, fejlesztés eredményeként lép majd életbe, a szabályzat végén – az *Átmeneti és záró rendelkezések*ben – történjen utalás a későbbi bevezetésre és alkalmazásra. A várt/vágyott állapotok szabályzatban rögzítésével nehéz feladatra vállalkozna a szerző: folyamatosan figyelemmel kellene kísérnie és dokumentálnia, mi az, ami már igaz és mi az, ami csak *lesz* igaz.
7. Az IBSZ átlátható, teljességre törekvő, de nem túl részletes legyen. Adjon általános és teljes képet az információvédelem szervezeten belüli megvalósításáról, de ne vesszen el a részletekben. A törzsszöveg tartalmazza az információbiztonsági szempontból releváns beosztásokat, szerepköröket, tevékenységeket, az ezeket betöltő személyek együttműködési formáit, az ellenőrzés, a dokumentálás stb. rendjét. Hangsúlyozandó, hogy e tekintetben nemcsak a vezetői vagy az informatikusi, hanem a felhasználói szerepkör is releváns, azaz az IBSZ-nek az *egyszerű felhasználók* információbiztonsági szempontból jelentőséggel bíró jogait és kötelezettségeit is tartalmaznia kell. A módszertani leírásokat (például egy kockázatelemzési módszertant) nem a törzsszövegben, hanem a mellékletben célszerű elhelyezni. A részletező eljárásrendeket (például egy elektronikus információs rendszer jogosultságkezelését vagy mentési rendjét) önálló (esetleg alacsonyabb szintű vagy kisebb hatókörű, csak az adott tevékenységre vagy rendszerre vonatkozó) szabályozóeszközben lehet rögzíteni. Az IBSZ *szabályozzon*. Ne tartalmazza a nem normatív dokumentumok elemeit (politika, stratégia stb.).
8. Az IBSZ segítse, orientálja a gyakran ismétlődő tevékenységeket (akár elektronikus) nyomtatványok, űrlapok rendszeresítésével (nyilatkozat-minta, bejelentés-minta stb.).

Az *irodalmi felütés* után – zárásként – álljon itt két, történelmi példán alapuló módszertani javaslat:

„Egy nap, miután a szenátus bejelenti, hogy most már minden egyes orosz városnak megvan a maga katonai kormányzója, Katalin (Nagy Katalin cárnő, uralkodott: 1762–1796) hirtelen megkérdi: hány város van Oroszországban? Döbbent csend a válasz. Senki nem tudja. Ezen aztán ne múljék, majd megszámoljuk a térképen,

mondja Katalin. De a szenátus archívumában nincs térkép. Katalin mosolyogva ad öt rubelt egy fiatal tisztviselőnek azzal, hogy vásároljon térképet a Tudományos Akadémián. Kirilov Atlaszáról van szó. A szenátorok bűntudattal hétrét görnyednek az alázattól." [15: 186.]

Azaz: nem árt, ha mindenki tudja, miről beszél, miről beszélünk; a szabályozás rögzítése előtt nyugodtan nézzünk utána mindennek, ami nem ismert, nem világos.

Amikor Albert herceg, Viktória angol királynő férje (1819–1861) az 1840-es évek közepén megkezdte a királyi háztartás átszervezését, több ízben érthetetlen, indokolhatatlan hagyományokra bukkant. „Albert, miközben a számadásokat vizsgálta, megakadt egy 35 shillinges tételen, mely minden héten szerepelt: »Borköltség a vörös szoba részére.« Utánajárt a dolognak, és kisütötte, hogy III. György idejében (uralkodott: 1760–1820) a windsori kastély egyik vörös tapétás helyisége őrszoba volt, az őrségparancsnok napi öt shillinget kapott borra. Az őrszobát már régóta megszüntették, a vörös szobából lomtár lett, de a harmincöt shillinget a hagyomány szent nevében minden héten kiutalták. Egy félzsoldon levő tiszt vette fel, aki egyébként komornyik is volt a palotában. [16: 144.]"

Azaz: nem biztos, hogy az „így szoktuk" gyakorlata még az aktuális helyzetben is célszerű, hasznos, előremutató. Legyen a szabályozás rögzítésének szükséges velejárója a felülvizsgálat, újragondolás, korrekció.

Következtetések

Az IBSZ-írás – ahogyan arra a fentiek is utaltak – a jelenlegi jogszabályi környezetben összetett feladat. Meg kell felelni a jogalkotó által meghatározott számos – néha első ránézésre egyszerűnek nem tűnő – tartalmi és formai elvárásnak. Ismerni kell – átfogóan és részletekbe menően is – az érintett szervezet tevékenységét, nemcsak az információbiztonsági feladatokat, hanem az általános felépítést és működést is, hiszen az információbiztonsági szabályozás a szervezet egészére kiterjedő (speciális) funkcionális tevékenység. Együtt kell működni más szakterületekkel, egyrészt az informatikai, másrészt különösen a jogi-szabályozási, adatvédelmi stb. feladatokat ellátó szervezeti egységekkel, munkatársakkal.

Az IBSZ-írást fel lehet fogni kötelező adminisztratív feladatnak, ahol az elsődleges cél a készre jelentés. Ennél szerencsésebb megközelítés, ha az IBSZ-írást a szervezeti működést támogató, érdemi alkotótevékenységnek fogjuk fel, amelynek megvalósítása során nemcsak az előírások mechanikus rögzítése, hanem azok szervezetre adaptálása, a szervezeti működés és az előírások összhangba hozása is megtörténik.

Az IBSZ a szervezet munkatársai által akkor lesz hasznosítható, ha „felhasználóbarát" formában érdemi, konkrét ismereteket, szabályokat ad. Ez rendkívül fontos szempont, hiszen az információbiztonsági szabályozás célja a jogalkotó és az érintett szakemberek által szükségesnek ítélt előírások rögzítése annak érdekében, hogy azok megismerhetők és alkalmazhatók, sőt alkalmazandók (kikényszeríthetők, számonkérhetők) legyenek.

A jó IBSZ megírására nincsen kész recept, de az érintett szervezeteknél, a szervezetek munkatársainál az elmúlt évtizedekben felhalmozódott tapasztalatok alapján

azonosíthatók a jó gyakorlatok, ezek alapján segédletek készíthetők, amelyek megosztásából már többen profitálhatnak.

A tanulmányban közzétett áttekintéseket, összefoglalókat, illetve a szerző által megfogalmazott javaslatokat gyakorlati szempontok alapján és gyakorlati céllal rögzítettük – elősegítendő, hogy az IBSZ-írás hatékony és eredményes tevékenység lehessen. Ajánlás, amelynek követése, szükség szerinti felülvizsgálata vagy kiegészítése nem kötelező – de hasznos lehet.

Hivatkozások

[1] U. Eco, *Hogyan írjunk szakdolgozatot?* Budapest: Gondolat Könyvkiadó, 1992.
[2] Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, *Informatikai biztonsági módszertani kézikönyv*. Informatikai Tárcaközi Bizottság ajánlása, 8. sz. ajánlás, Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, 1994.
[3] Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, *Informatikai rendszerek biztonsági követelményei. Informatikai Tárcaközi Bizottság, 12. ajánlás,* Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, 1996.
[4] Közigazgatási Informatikai Bizottság, *A Közigazgatási Informatikai Bizottság 25. számú ajánlása: 25/1-1. kötet: Informatikai Biztonsági Irányítási Rendszer (IBIR) 1.0 verzió.,* Közigazgatási Informatikai Bizottság, 2008.
[5] Cs. Krasznai és L. Muha, *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem, 2014.
[6] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
[7] 1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről
[8] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról
[9] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
[10] 2000. évi C. törvény a számvitelről
[11] 2010. évi CXXX. törvény a jogalkotásról
[12] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
[13] ISO/IEC 27000:2018 (en) Information technology – Security techniques – Information security management systems – Overview and vocabulary
[14] ITIL® V3 Glossary of Terms, Definitions and Acronyms in Hungarian, Hungarian Glossary
[15] H. Troyat, *Nagy Katalin.* Budapest: Pesti Szalon Könyvkiadó, 1996.
[16] L. Strachey, *Viktória királynő. Történelmi életrajz.* Budapest: Szépirodalmi Könyvkiadó, 1984.