HADMÉRNÖK

XII. Évfolyam 4. szám – 2017. december

AZ INFORMÁCIÓBIZTONSÁG ALAPKÉRDÉSEI

THOUGHTS ON INFORMATION SECURITY

GÉMES Csaba

(ORCID: 0000-0003-3012-2175)

gemes.csaba@uni-nke.hu

Absztrakt

A hírekben mind sűrűbben megjelenő hacker-támadások, vagy a médiában szereplő külföldi és hazai kibervédelmi feladatok hallatán, tudományos munkákban, munkahelyi tájékoztatókon, de még iskolai tananyag-tervezetként is egyre gyakrabban találkozhatunk az elektronikusan kezelt adatok biztonsági kérdéseivel, egy szóval az információbiztonsággal.
De mi is az az információbiztonság? Múló divat, vagy valóban fontos kérdés, amellyel foglalkozni kell? Mit és miért kell védeni? Kinek és mit kell, vagy lehet tennie? A cikk szerzője ezekre a kérdésekre keresi a választ.

Kulcsszavak: *információbiztonság, informatikai biztonság*

Abstract

As more frequently appearing the news of hacker attacks, and foreign and national cyber defence tasks in the media were found, over and above in the scientific works, job briefings, and even the school curriculum draft more and more often we can meet electronically handled data security issue, in one word: information security.
But what is information security? Only fashion, or indeed important to deal with it? What should be protected and why? Who and what you should or can do? The author seeks to answer these questions.

Keywords: *information security, Information Assurance INFOSEC, IT security*

A kézirat benyújtásának dátuma (Date of the submission): 2017.07.03.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.11.27.

BEVEZETÉS

A hírekben mind sűrűbben megjelenő hacker-támadások, vagy a médiában szereplő külföldi és hazai kibervédelmi feladatok hallatán, tudományos munkákban, munkahelyi tájékoztatókon, de még iskolai tananyag-tervezetként is egyre gyakrabban találkozhatunk az elektronikusan kezelt adatok biztonsági kérdésivel, egy szóval az információbiztonsággal. A téma aktualitását mutatja, hogy 2016 júniusában a NATO varsói csúcstalálkozóján az elektronikus formában lévő információ létezési közegét jelentő kiberteret hivatalosan is elismerik ötödik műveleti dimenzióként a korábbi négy fizikai (szárazföldi, légi, tengeri, kozmikus) hadszíntér mellett. [1]

A téma egyre magasabb szinten és egyre gyakoribb megjelenése indokolttá teszi, hogy kiemelt figyelemmel foglalkozzunk az információbiztonsággal. Már a téma szakirodalmának felületes tanulmányozásából is megállapítható, hogy a megoldandó probléma igen összetett, megoldására különböző biztonságszervezői (menedzsment) módszerek vannak, amelyek megértéséhez, további tanulmányozásához elkerülhetetlen az információbiztonság alapkérdéseinek tisztázása. E cikk célja az információbiztonság alapkérdéseinek áttekintése, a biztonság kialakítására és fenntartására alkalmazható módszerek vizsgálatának megalapozása érdekében.

AZ INFORMÁCIÓS TÁRSADALOM

Az információbiztonság alapkérdéseinek vizsgálatát kézenfekvő egy rövid történeti áttekintéssel kezdeni, amely rávilágit az információbiztonság fontosságára is.

Az ősidőkig visszatekintve megállapítható, hogy az információk megszerzésére, illetve annak megakadályozására való törekvés – vagyis az információ védelme – a beszéd megjelenésével párhuzamosan, az első emberi társadalmak kialakulásával egyidős tevékenység: „Már az ősközösségi társadalmakban is „lopták” az információkat, amikor megpróbálták kifürkészni a másik közösség vadászati szokásait vagy túlélési praktikáit”. [2: 251]

Ebből következően az információbiztonság története az őskorig vezethető vissza. Természetesen a társadalmi fejlődéssel együtt a megszerzendő információk köre, megjelenésének formája, keltezésének módja, valamint ebből következően az információ megszerzéséhez felhasználható, illetve ennek megakadályozásához szükséges módszerek is folyamatosan fejlődtek.

Az ókorban az írás megjelenésével az információ rögzített formában is tárolhatóvá és továbbíthatóvá vált, ezzel átlépve az emberi emlékezőképesség és a személyes közlés határait. Az írás megjelenésével lehetőség nyílt az információ változatlan formában és emellett nagyobb mennyiségben való tárolására és továbbítására is. Az információ pontos és bizalmas átadása többé már nem igényelt a személyes találkozást. A hírnökök, futárok a szóbeli helyett már írásos közleményt továbbítottak, így a korábban jellemzően kis mennyiségű, esetenként torzítottan átadott hír helyett nagy mennyiségű, sértetlenül átadott információ hordozóivá válhattak ráadásul úgy, hogy annak tartalmát sem kellett megismerniük. Lényegében megállapítható, hogy az írás megjelenése forradalmasította az információ kezelését. Természetesen, mint minden új technológia, az írásos közleménytovábbítás is rejtett magában új kockázatokat, ahogyan a hírvivő elfogásával a teljes és valós szövegű üzenet elfogása történt meg, amelyet felhasználhattak. Fennállt annak a veszélye is, hogy az elfogott üzenet helyett, vagy akár előzmény nélkül is küldhető olyan félrevezető üzenet, amelyet a címzett az írás hiteleségében bízva valósnak vélt.

Biztonsági szempontból nézve az új információkezelési módszerek új biztonsági lehetőségeket is nyújtottak, amelyek kiaknázására szükség is volt az új kockázatok csökkentése érdekében. Az írásos közleménytovábbításnak voltak önmagában rejlő biztonsági funkciói is, mint ahogyan a hírvivő hozzáférésének lehetősége már eleve korlátozottabb egy lezártan továbbítandó üzenet esetében a szóbeli információhoz képest. Kezdetben az írástudók alacsony számából eredően maga az írás is védettséget jelentett, majd megjelentek a különböző algoritmusú titkosítások, jelszavas, és rejtjelzési megoldások is. [3]

Az írás megjelenése szerepet játszott az ókori államok kialakulásában is, amelyek irányításában, működésében meghatározó szerepe volt hatalmi szempontból érzékeny információk kezelésének. Ennek fényében nem meglepő, hogy már az első ókori államok eszközrendszerében megjelenik a kémkedés és ezzel együtt az elhárítás is. [4]

A középkor jeles eseményei közül témánkhoz kapcsolóan ki kell emelni a könyvnyomtatás feltalálását,[1] amely információtechnológiai szempontból a nagy mennyiségben való sokszorosítás és a széles körben való hozzáférés előnyei és az ezzel járó biztonsági problémák megjelenése szempontjából jelentős. Másrészt – a tudomány oldaláról megközelítve – a könyvnyomtatás az újkori technológiai fejlődést megalapozó műszaki tudományok kialakulása, fejlődése és elterjedése szempontjából is kiemelt szerepet játszott.

Az újkori társadalom fejlődésébe a tudományos, majd ennek hatására a több hullámban országonként akár néhány évtizedes eltéréssel végbemenő ipari forradalmak számtalan technikai újítást hoztak. A megjelenő új technológiák közül a távíró, a telefon és a rádió megjelenésével létrejön elektronikus hírközlés, amely az információk gyors és nagy távolságra való eljuttatásának következményeként összezsugorodik a világ. Itt kell megjegyezni, hogy a rádió katonai alkalmazásával szinte egyidejűleg megjelenik a kisugárzott információ lehallgatása és a zavarása is, majd megtörténnek az ezek elleni első válaszlépések, amelyekről már elektronikus információvédelmi intézkedésként beszélhetünk.

Az ipari forradalmak a technológiai fejlődésen túl komoly társadalmi-gazdasági változásokat is eredményeztek A munkaerő megoszlás változásainak vizsgálata alapján megállapítható, hogy 19–20. század fordulóján a mezőgazdaságban dolgozók számát meghaladta az iparban, majd az 1960-as évektől[2] az információs szektorban dolgozók száma. [5]

A távközlés fejlődése, a műsorszóró rádióadások, a televízió elterjedése már a 20. század közepétől hajtotta az információs technológia fejlődését, amely a századvégre a személyi számítógépek, hálózatok, internet, multimédia elterjedésével robbanásszerű mértéket öltött. A fejlődéshez szükséges ipari termelés, az információtechnológia magán, vállalati, és állami szférában egyre elterjedtebb alkalmazása, komoly társadalmi változásokat is hozott. A gépipari tömegtermelésre épülő ipari társadalom fokozatosan átalakult a tudásra, információra és információtechnológiára alapuló „posztindusztriális”[3] vagy az 1970-től elterjedő kifejezéssel[4] „információs társadalommá”. [6]

---

[1] Európában Johann Gutenberg mainzi aranyműves által, a korábbi ázsiai nyomtatási módszerektől feltehetően függetlenül 1450 körül megalkotott, mozgatható nyomóelemek széles körű használatával történő technikai eljárás. (Wikipédia: Johann Gutenberg)

[2] Országonként eltérő a technológia fejlettség függvényében Az USA-ban 1967 Daniel Bell munkája [Bell] alapján.

[3] Daniell Bell amerikai szociológus preindusztriális – indusztriális – posztindusztriális felosztása alapján.

[4] Yoneji Masuda japán származású szociológus használta egy konferencián.

Napjainkban a rohamosan fejlődő technológia, illetve az általa nyújtott lehetőségek, szolgáltatások egyre nagyobb mértékű kihasználásának elkerülhetetlen következménye az ezzel járó veszélyek – szakmai szóhasználattal élve a fenyegetések – hatványozott mértékben történő növekedése is. Ezen fenyegetések által okozható károk kiemelt jelentőséggel bírnak, amelyek elkerülése illetve csökkentése érdekében lépéseket kell tenni.

BIZTONSÁG ÉS VÉDELEM

Az előző történeti áttekintéssel képet kaphattunk az információbiztonság kialakulásáról és fontosságáról. Ebben a fejezetben körül járjuk, hogy egyáltalán mi is az a biztonság, milyen területei vannak, illetve kialakulásához milyen alapelveket kell figyelembe vennünk.

A biztonság és védelem közötti különbség

Az információs társadalom kialakulásának folyamata mutatja, hogy hogyan és milyen történelmi távlatokban gyökerező kihívásokra való válaszlépésként jött létre az információbiztonság (vagy információvédelem). Szinte magától értetődő, hogy a témakör további részletezéséhez elkerülhetetlen a „biztonság” a „védelem” illetve a külföldi szakirodalomban használt megfelelőjük értelmezése.

A biztonság és védelem, különböző megközelítésből született megfogalmazásaiból színes képet mutat a szakirodalom. [7: 5–9] [6: 19] A két kifejezés használata közötti különbség a magyar nyelvben jól körvonalazódik. A biztonság egy megkívánt – kialakítandó és fenntartandó – állapotot jelent, a védelem pedig a biztonság eléréséhez és fenntartásához szükséges tevékenységet. Az angol nyelvű szakmai terminológiában mindkét értelemben a „security” (biztonság) szót használják. Habár a „defence” szó néha az információ „védelem”-ként is előfordul, leginkább a fizikai és katonai értelemben vett védelemként használatos, hasonlóan a „safety” (biztonságos) kifejezéshez. A NATO és az USA terminológiájában a magyar „biztonság” és „védelem” szavak mindegyikét kifejező „security” mellett leggyakrabban a „Information Security” rövidítéséből származó „INFOSEC” kifejezést használják. Ezen kívül egyre gyakrabban találkozhatunk a garanciának, garantált vagy szavatolt védelemnek fordítható „assurance” kifejezéssel is.

Az információt az „Information Assurance” (a továbbiakban: IA) elveit alkalmazva kell védeni, amely védelmi intézkedésekkel teszi elérhetővé a kommunikációs, informatikai és egyéb elektronikus és nem elektronikus információs rendszerek, valamint a tárolt, feldolgozott és továbbított információk elvárt biztonsági szintjét a bizalmasság sértetlenség, rendelkezésre állás, letagadhatatlanságát és hitelesség vonatkozásában. [8: Ann. 1]

Az INFOSEC és az IA fogalomkörét összehasonlítva elmondható, hogy az INFOSEC kimondottan az elektronikus információs rendszerek és az abban kezelt adatok védelmét tűzi ki céljául [9] egyenértékűen a magyar „elektronikus információbiztonság” fogalomkörrel, míg az IA az információk és információs rendszerek mindegyikére értelmezendő, beleértve a nem elektronikus rendszereket is. [10]

Az információbiztonság területei

A biztonság alanya szerint számtalan „biztonság” létezik, amelyekből jelen írásban csak az információbiztonsággal foglalkozunk, azon belül leginkább az elektronikusan kezelt információk biztonságára fókuszálva. Joggal merül fel a kérdés, hogy az információbiztonságnak milyen egyéb területei vannak és azok milyen viszonyban állnak egymással.

Az információbiztonság általánosan elfogadott nézet szerint személyi- fizikai- dokumentum- (vagy adminisztratív) biztonsági, valamint elektronikus információbiztonság területekre osztható fel.

A hazai és a külföldi terminológiák összegzésével az elektronikus információbiztonság (INFOSEC) területeiként az átvitelbiztonságot (TRANSSEC), a kompromittáló kisugárzás elleni védelmet (EMSEC/TEMPEST), számítógép és hálózati biztonságot (COMP&LANSEC), valamint a rejtjelzést [CRYPTOSEC] tekinthetjük, de ettől eltérő felosztással is találkozhatunk. [11]

Az elvárt szintű információbiztonság csak úgy alakítható ki, illetve tartható fenn, ha az az információbiztonság, és ezen belül az elektronikus információbiztonság valamennyi területén egyaránt biztosított az ehhez szükséges védelem. Ezt nevezzük a biztonság komplexitásának. [12] A komplex védelem fogalma így egyaránt értelmezhető az információbiztonság, illetve ezen belül az elektronikus információbiztonság valamennyi területére, amelyek összefoglaltan az 1. ábrán láthatók.

1. ábra A komplex információbiztonság elemei [12.]

Biztonsági alapelvek és célkitűzések

Az információbiztonság kialakulásához és fenntartásához elengedhetetlen definiálni azokat a biztonság három attribútumaként, aspektusaként, tulajdonságaként vagy biztonsági célkitűzésként nevezett, kezdőbetűik alapján BSR-nek (angolul CIA-nak[5]) rövidített kritériumokat, valamint egyéb biztonsági alapelveket, amelyek megfelelő szinten történő teljesítése esetén a biztonságot megvalósultnak tekinthetjük.

Ezen biztonsági célkitűzések és alapelvek alapján került meghatározásra a vonatkozó nemzeti jogszabályban [13] az elektronikus információs rendszer biztonságának fogalmai is, amely „az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.”

[5] BSR: Bizalmasság, Sértetlenség, Rendelkezésre állás CIA: Confidentiality, Integrity, Availability

A meghatározásban szereplő biztonsági célkitűzések és alapelvek az alábbiak szerint értelmezhetőek.

A bizalmasság az elektronikus rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról. [13: para. 1 bek. 8]

A sértetlenség az adatra vonatkozóan azt jelenti, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot, abban, hogy az az elvárt forrásból származik (hitelesség) és a származás megtörténtének bizonyosságát (letagadhatatlanság) is. A sértetlenség a rendszerre vonatkozóan azt jelenti, hogy a rendszerelem rendeltetésének megfelelően használható. [13: para. 1 bek. 39]

A rendelkezésre állás annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek. [13: para. 1. bek. 38]

A zárt védelem elve szerint a védelem kialakítása az összes számításba vehető fenyegetést figyelembe veszi. [13: para. 1 bek. 48]

A teljes körű védelem elve szerint a védelmi intézkedések a rendszer összes elemére kiterjednek. [13: para. 1 bek. 44]

A folytonos védelem elve az időben változó körülmények és viszonyok ellenére is folyamatosan megvalósuló védelmet jelenti. [13: para. 1 bek. 21]

A kockázatokkal arányos védelem alapelve rögzíti, hogy a védelem költségeinek arányosnak kell lenniük a fenyegetések által okozható károk értékével. [13: para. 1 bek. 31]

A fejezet összegzéseként megállapítható, hogy az információbiztonság egyidős az emberi társadalommal, ahogyan az elektronikusa információbiztonság is az elektronikus adatkezelés megjelenése óta létezik. Az új technológiák új kockázatokat hordoznak magukban. Ebből következően napjaink információs társadalmában az életünket egyre szélesebb körben átszövő és egyre összetettebb információs technológia alkalmazása egyre magasabb kockázattal jár, amelyet megfelelő biztonsági intézkedésekkel csökkenteni kell. A fogalmak vizsgálata során megállapítható, hogy a terminológia elég vegyes képet mutat. Megfigyelhető, hogy akár eltérő jelentésű kifejezések akár egymás szinonimájaként is használhatóak, valamint előfordul, hogy egyazon fogalom jelentése még az egymással szorosan összefüggő szakterületek szóhasználatában is eltérő területet fed le. A szakterületek biztonsági szabályzóit vizsgálva még a biztonság területeinek, feladatrendszerének felosztásában is eltéréseket találhatunk. Ugyanakkor az eltérések ellenére megállapítható, hogy az információbiztonság kialakítása és fenntartása szempontjából jelentős biztonsági alapelvek és célkitűzések azonosak.

VÉDENDŐ ÉRTÉKEINK

Adat és információ

A védendő értékek sorában elsődleges fogalomként találkozunk az „információ”-val, illetve a köznyelvben és néha még a szakemberek körében is szinonimaként használt „adat” kifejezéssel. A különböző információelméletekből és szakirodalmi forrásokból eredően mindkét fogalomnak számos definíciója van. [14] Ezek közül szakmai megfontolásból az információbiztonsági törvényben [13] (a továbbiakban Ibtv,) rögzített meghatározásokat célszerű mérvadónak tekinteni, amelyben utalást találunk a két fogalom viszonyára is:

Az *„adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.”* [13: para. 1 bek. 1]

Az *„információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét,*

annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti." [13: para. 1 bek. 25]

A két fogalom információelméleti összehasonlításaként megállapítható, hogy az információ, az adatok értelmezett jelentéssel bíró formájaként magasabb tudati szintet képvisel. [12] Műszaki megközelítéssel vizsgálva ugyanakkor megállapítható, hogy az elektronikus információbiztonság szempontjából elektronikus jelek formájában az információ hordozójaként valójában az „adattal" találkozunk. Ennek ellenére a szakmai szóhasználatban az „információ"- biztonság és védelem a jellemző. „Adat"-biztonságról vagy védelemről szakmai szempontból legfeljebb az elektronikus adathordozók kapcsán eshet szó, ezekkel a szóösszetételekkel jellemzően a személyes és a közérdekű adatok védelmének területén találkozhatunk. A fogalmak angol megfelelőjeként a „data" és az „information" kifejezések használata között ugyanezen különbségek figyelhetők meg.

A két fogalom jelentése a fentiek alapján látszólag egyértelműen elhatárolható, ugyanakkor szövegkörnyezettől függően előfordul, hogy a kifejezések felcserélt használata sem módosít a szöveg értelmén.

A rendszer

Az információ, vagy az annak hordozójaként tekinthető adat biztonságának garantáláshoz elengedhetetlen, hogy az azokat feldolgozó elektronikus információs rendszerek biztonságáról is gondoskodjunk. A különböző rendszerelméletek szerint számos meghatározást találunk az általános értelembe vett információs rendszerekhez is, és ezen belül az elektronikus rendszerre is. A kimondottan elektronikus információkezelő rendszerekre (a továbbiakban: rendszer) vonatkozó fogalom is többféle kifejezés formájában jelenik meg. Csak az általános szóhasználatot alapul véve beszélhetünk „informatikai technológiák" (IT), vagy ennek a szabványok és ajánlások terminológiáiban megjelenő „Információ- és kommunikációs technológiák" (ICT és IKT) kifejezésekről is.

A rendszer fogalmánál érdemes kihangsúlyozni, hogy az elektronikus rendszer fogalmába az „tisztán" informatikai rendszereken és hálózatokon kívül beleértendők az alábbi infokommunikációs rendszerek mindegyike, függetlenül attól, hogy az adott rendszer milyen arányban tartalmaz informatikai komponenseket.

Így elektronikus rendszerként értelmezendők a vezetékes, a mobil, a rádiós és műholdas távközlés; a vezetékes, a rádiófrekvenciás és műholdas műsorszórás; a rádiós vagy műholdas navigáció, automatizálási, vezérlési és ellenőrzési rendszerek (SCADA), távmérő, távérzékelő és telemetriai rendszerek, valamint ezek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek. [15: 124–208]

Az elektronikus információbiztonságra vonatkozó nemzeti, külföldi és nemzetközi szabványok, ajánlások, direktívák, jogszabályok és egyéb szabályzókat megvizsgálva gyakran találkozhatunk s szóhasználatukat tekintve gyakran „informatikai biztonság" címekkel és terminológiával, ugyanakkor tartalmilag szinte minden esetben a bővebb értelemben vett IKT rendszerek biztonságáról esik szó.

A rendszer kifejezés különböző rendszerelméleti és szakterületi megfogalmazása közül a minősített adatok védelméről szóló törvényben [16] (továbbiakban: Mavtv.) szereplő rövid, tömör, lényegre törő megfogalmazást kiemelni, amely szerint az elektronikus adatkezelő rendszer a *„minősített adat elektronikus, elektromagnetikus vagy optikai úton történő kezelésére alkalmas berendezés, módszer és eljárás együttese*". Mindenképpen érdemes még rendszer fogalmát jobban részletező, a személyzettel szabályozással és kapcsolód folyamatokkal kiegészített az Ibtv. szerinti megfogalmazást is megemlíteni, amely szerint az *„elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver*

és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese" [13: para.1 bek. 14b]
A részletes megfogalmazás mellett az Ibtv. az információs önrendelkezési jogról és az információszabadságról szóló törvénnyel [17] való összhangot megteremtése érdekében az adatgazdával összefüggésben is definiálja a rendszer fogalmát az általános megfogalmazással azonos módon. [13: para. 1 bek. 48 (3)]

Egyéb védendő értékek

Az információ biztonságát veszélyeztető fenyegetések csak viszonylag ritkán irányulnak közvetlenül az információra. A véletlen vagy szándékos fenyegetések jelentős része a rendszeren, vagy az azzal kapcsolatban álló tényezőkön keresztül éri a rendszert. Már a rendszer fogalma Ibtv. szerinti megfogalmazásából is látható, hogy a rendszer klasszikus hardver és szoftver komponensein kívül megjelenik az ember, a környezeti infrastruktúra, a hálózat, – a nem feltétlenül elektronikus – adathordozó, mint például a kinyomtatott papír. A megfogalmazás szerint ide tartozik még a rendszer működéséhez szükséges szabályozás és az összes kapcsolódó folyamat is. Következtetésként a védendő értékek közé kell sorolni minden olyan tényezőt, ami a rendszer biztonságos működését befolyásolja. [13: para. 1. bek. 14b]
Természetesen így történik az a minősített adatkezelés esetében is, azzal az eltéréssel, hogy a Mavtv.-hez kapcsolódóan két külön végrehajtási rendelet szabályozza az elektronikus biztonság, [18] illetve a biztonság egyéb területeit. [19] További eltérést jelnet, hogy az elektronikus biztonságról szóló rendelet a Mavtv. által szűkebben értelmezett „rendszer" biztonsága mellett a külön tevékenységként foglalkozik rendszer részeként tekintett rejtjelzéssel, és a hálózatbiztonsággal. A rendeletek tartalmát és szakterületek viszonyát vizsgálva mégis megállapítható, hogy – a rendeleti és a szakterületi elkülönítés ellenére – a személyi-, fizikai-, adminisztratív-, és az elektronikus információbiztonság, illetve ez utóbbi részterületei egymással szoros kapcsolatban állnak a biztonság komplexitásának megfelelően.
A fejezet összegzéseként megállapítható, hogy az elektronikus információbiztonság kialakítása és a fenttartása csak úgy valósítható meg, ha védendő információ mellett gondoskodunk az azt feldolgozó rendszer biztonságáról is, valamint – a biztonság komplexitásának megfelelően – a kapcsolódó személyi-, fizikai-, és adminisztratív biztonságról is. Továbbá a védelemi intézkedéseknek a biztonság garantálásához szükséges mértékben ki kell terjednie minden a rendszer biztonságát befolyásoló személyre, folyamatra, szabályozásra, eszközre, infrastruktúrára és annak használatára.

KÖVETKEZTETÉSEK

Megállapítható, hogy az információbiztonság egyidős az emberi társadalommal, ahogyan az elektronikusa információbiztonság is az elektronikus adatkezelés megjelenése óta létezik. Az információbiztonság aktualitását mutatja, hogy az információs technológia rohamos fejlődéséből adódó lehetőségek kihasználása egyre nagyobb jelentőséggel bír a társadalmi élet minden területén, beleértve a magán-, a vállalati- és a kormányzati szférát is. A technológia fejlődésének, illetve az általa nyújtott lehetőségek, szolgáltatások egyre nagyobb mértékű kihasználásának elkerülhetetlen következménye az ezzel járó veszélyek (fenyegetések) hatványozott mértékben történő növekedése is. Ezen fenyegetések által okozható károk kiemelt jelentőséggel bírnak, amelyek elkerülése illetve csökkentése érdekében a biztonsági alapelvek és célkitűzések megfelelő védelmet kell alkalmazni.

A biztonság tárgyát képező védendő értékek vizsgálata során megállapítást nyert, hogy az információ biztonsága érdekében gondoskodni kell az információt feldolgozó rendszer biztonságáról is. Ezen kívül a biztonság komplexitásából adódóan a védelmi intézkedéseknek

a biztonság garantálásához szükséges mértékben ki kell terjednie minden a rendszer biztonságát befolyásoló személyre, folyamatra, szabályozásra, eszközre, infrastruktúrára is.

A fogalmak vizsgálata során megállapítható, hogy a terminológia elég vegyes képet mutat. Megfigyelhető, hogy akár eltérő jelentésű kifejezések akár egymás szinonimájaként is használhatóak, valamint előfordul, hogy egyazon fogalom jelentése még az egymással szorosan összefüggő szakterületek szóhasználatában is eltérő területet fed le. A szakterületek biztonsági szabályzóit vizsgálva még a biztonság területeinek, feladatrendszerének felosztásában is eltéréseket találhatunk. Ugyanakkor az eltérések ellenére megállapítható, hogy az információbiztonság kialakítása és fenntartása szempontjából jelentős biztonsági alapelvek és célkitűzések azonosak.

A biztonság kialakításához és fenntartásához hozzáértő biztonságszervezői munka szükséges, amelynek támogatására számos menedzsment módszer létezik. Ezen módszerek – az adott szervezet és az elektronikus rendszerei sajátosságainak megfelelő – kiválasztása, önálló vagy együttes alkalmazása igen összetett problémákat vet fel, amelyek hatékony megoldásához a téma részletes vizsgálata szükséges.

FELHASZNÁLT IRODALOM

[1] SZENES Z.: *Meglepetések nélkül. A varsói NATO csúcs értékelése.* http://biztonsagpolitika.hu/kiemelt/meglepetesek-nelkul-a-varsoi-nato-csucs-ertekelese (A letöltés dátuma: 2016. 11. 06.)

[2] MUHA L. (szerk), Az *informatikai biztonság kézikönyve.* 10. javított kiadás. Budapest: Verlag Dashöfer, 2004.

[3] SINGH, S.: *The Code Book – The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* SZENTGYÖRGYI J. (ford.), *(Kódkönyv – A rejtjelezés és rejtjelfejtés története.)* Budapest: Park, 2002.

[4] PIEKALKIWICZ, J: *A kémkedés világtörténete I.* Budapest: Zrínyi Kiadó, 1997.

[5] BELL, D.: Az információs társadalom társas keretrendszere. In. *Információs társadalom I.* 3–33. Budapest: Infonia, 2001.

[6] HAIG Zs.: *Információ, társadalom, biztonság.* Budapest: NKE Szolgáltató Kft., 2015.

[7] MUNK S.*:* Információbiztonság vs. informatikai biztonság. In. *Robothadviselés 7 Konferencia.* Budapest, 2007. 11. 27. http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.pdf (A letöltés dátuma: 2016. 11. 06.)

[8] *C-M(2007)0118 NATO Information Management Policy (NIMP).* Brussels: North Atlantic Council (NAC) – NATO HQ Document, 2008.

[9] *NIST SP 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations.* Gaithersburg: NIST Special Publication National Institute of Standards and Technology – U.S. Department of Commerce, 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (A letöltés dátuma: 2016. 11. 09.)

[10] *SP 800-59, Guideline for Identifying an Information System as a National Security System.* 2003. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf (A letöltés dátuma: 2016. 11. 09.)

[11] *AC/35-D/2004-REV2 Primary Directive on INFOSEC.* NSC and the C3 Board (C3B) – NATO HQ Document, 2010.

[12] HAIG ZS.: *Az információs társadalom információbiztonsága*. Budapest: ZMNE, 2009. jegyzet https://ludita.uni-nke.hu/repozitorium/handle/11410/8514

[13] *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.* http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV (A letöltés dátuma: 2016. 11. 09.)

[14] MUNK S.: Információs színtér, információs környezet, információs infrastruktúra. *Nemzetvédelmi Egyetemi Közlemények,* 2 (2002). http://m.ludita.uni-nke.hu/repozitorium/handle/11410/1083 (A letöltés dátuma: 2016. 11. 09.)

[15] HAIG ZS., VÁRHEGY I.: *Információs műveletek I. Információs korszak hadügyi forradalma és információs rendszerei*. Budapest: ZMNE, 2004.

[16] *2009. évi CLV. törvény. a minősített adat védelméről.* http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0900155.TV (A letöltés dátuma: 2016. 11. 11.)

[17] *2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról*. http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV (A letöltés dátuma: 2016. 11. 11.)

[18] *161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól.* http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1000161.KOR (A letöltés dátuma: 2016. 11. 11.)

[19] *90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről.* http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1000090.KOR (A letöltés dátuma: 2016. 11.11.)