HADMÉRNÖK

VIII. Évfolyam 1. szám - 2013. március

Kassai Károly
kassai.karoly@hm.gov.hu

AZ ELEKTRONIKUS INFORMÁCIÓVÉDELEM SZABÁLYOZÁSI KÉRDÉSEI A KÖZELMÚLTBAN[1]

Absztrakt

A kommunikációs szolgáltatások gyorsuló ütemű fejlődése szükségessé teszi az elektronikus információvédelmi rendszabályok fejlesztését is. A biztonsági célkitűzések, biztonsági követelmények, védelmi rendszabályok és mechanizmusok rugalmas, naprakész szabályozása kulcskérdés a szükséges mértékű biztonsági szint kialakítása és fenntartása érdekében. A cikk a katonai híradó és informatikai rendszerek elektronikus információbiztonságával kapcsolatos szabályozási kérdések támogatását célozza az utolsó évtizedek szabályozási lépéseinek áttekintésével és a hadtudományi publikációk eredményeinek összefoglalásával.

The accelerated development of communication services requires communication and information system (CIS) security regulations development as well. The flexible and updated security goals, security requirements, protection methods and mechanisms are key issues in order to develop and maintain the appropriate level of security. This article aims the support of regulation the military CIS security by review the main regulation steps in last decades and summarization of military studies about this topic.

Kulcsszavak: *információbiztonság, elektronikus információvédelem, kiberbiztonság, szabályozás ~ information security, electronic information security (INFOSEC, Information Assurance) cyber security, regulation*

[1] A cikk a szerző Nemzeti Közszolgálati Egyetem, felső vezetői katonai tanfolyam évfolyamdolgozatának (2013) felhasználásával készült.

BEVEZETÉS

A Magyar Honvédség bonyolult feladatokat végző szervezetek összessége, mely szervezetek specializált elektronikus adatkezelésének biztonságát egy szabályozóval nem lehet megoldani. A Magyar Honvédségnél a híradó és informatikai szolgáltatások biztonságához szükséges követelmények, feladatok először a híradó, ügyviteli, rejtjelző és informatikai szabályozókban jelentek meg, majd a szolgáltatások bonyolultságot követve az önálló központi szabályozók irányába kezdenek fejlődni.

A növekvő számú szakmai feladatok miatt logikus követelmény, hogy a szabályozókat az érthetőség, nyomon követhetőség érdekében valamilyen rendbe kell rendezni, tartalmilag egymáshoz kell illeszteni, figyelemmel arra, hogy közöttük átfedések ne legyenek, illetve közöttük hiányzó területek ne maradjanak.

A katonai szabályozóknak illeszkedniük kell a nemzeti, NATO és EU szabályozási környezethez, az alkalmazott híradó és informatikai szolgáltatásokhoz, így a szabályozási témák kiválasztásakor figyelembe kell venni a kapcsolódásokat és függőségeket.

E gondolatok mentén a cikk célja a hasznosítható értékek feltárása érdekében az elektronikus információbiztonságra vonatkozó korábbi alapvető követelmények azonosítása, a szabályozási gondolkodás előzményeinek tanulmányozása.

ÁTTEKINTÉS

Az elektronikus adatkezelésre vonatkozó szabályozás az alkalmazott technológiának megfelelően a rejtjelzés, az ügyvitel, a híradás (benne a vezetékes és vezeték nélküli híradás), és az informatika területein azonosíthatók[2] a következők szerint összefoglalva.

Rejtjelzésre vonatkozó megfogalmazások

Kormányzati szintű, rejtjelzésre vonatkozó központi követelmény 1994-ben határozta meg a szervezetek szaktevékenységére vonatkozó szabályozási kötelezettséget, de a keretjellegű szabályozók sajátossága szerint nem határozott meg minden területen pontos követelményeket (a szervezetek közötti együttműködés az eszközök, eljárások szintjén és támogató szervezési lépéseken keresztül valósulhatott meg).

A szabályozási kötelezettség a következő területekre vonatkozott:

- a rejtjelfelügyelet hatásköre, szervezeti és működési rendje, feladatai;
- a vezetői beosztásokat ellátó személyek azonosítása, akik betekintési engedély nélkül is megismerhetnek rejtjeltevékenységgel kapcsolatos információkat;
- a rejtjeltevékenység védelmét előíró különleges biztonsági követelmények;
- a nyilvántartás és ügyvitel részletes szabályai;
- a rejtjeltevékenység ellenőrzésére jogosultakat.

A jogszabály meghatározta, hogy a rejtjelszabályzat kiadásához előzetes hatósági engedély szükséges (Országos Rejtjelfelügyelet). [1.] E követelmények alapján miniszteri utasításban történt a Magyar Honvédség rejtjelfelügyeleti rendjének szabályozása 1995-ben, majd 1996-ban megjelent a „Magyar Honvédség Rejtjelszabályzata”. A rejtjelző szakiratkezelést e mellett önálló utasítás szabályozta, illetve kiegészítéseként a rejtjelző eszközök üzemeltetési utasításai, az egyedi szolgálati utasítások és munkaköri leírások szolgálták a szabályozási feladatokat.

[2] Az áttekintésnek nem célja minden egyes szabályozó azonosítása és értékelése, célként csak a fontosabb tendenciák feltárása tűzhető ki. Az áttekintésnek tartalmaznia kell a kormányzati követelmények azonosítását is, mert e nélkül nem lehetséges a reális megítéléshez szükséges összehasonlítási lehetőség.

Az 1995-ös miniszteri utasítás kijelölte a felelősségi köröket és a tevékenységet (a rendszeresített eszközök üzemeltetése és az ehhez szükséges rejtjeltevékenység; illetve a gazdálkodó szervezeteknél csak eszközfejlesztés, gyártás, javítás és értékesítés történhet). Meghatározta az MH Központi Rejtjelfelügyelet (MH KRF), középszintű vezető szerveknél pedig rejtjelfelügyelet működését. A rejtjeltevékenységet végző rejtjelző szolgálatok a saját katonai szervezet alárendeltségében, de az illetékes rejtjelfelügyelet szakirányításával végzik feladatukat. Az MH KRF és az önálló rejtjelfelügyeletek az Országos Rejtjelfelügyelet szakirányításával végzik feladatukat. [2.]

1997-ben az MH Parancsnoka, Vezérkari Főnöke adminisztratív követelményeket határozott meg az Internet használatáról, benne a rejtjelző eszközök internetes csatlakoztatásának tilalmáról. [3.]

Ügyviteli szakterületű, elektronikus információvédelmet érintő megfogalmazások

Az MH esetében az ügyviteli feladatoknál a nyomtatott formájú adatok kezelése, illetve az elektronikus adathordozók nyilvántartása, felügyelete jelölhető meg szakterületi feladatként, mint: „A számítástechnikai eljárás (nyomtatás) során keletkezett minősített adatot, rontott listát a legrövidebb időn belül az ügyviteli szervnek (aláírás ellenében) le kell adni megsemmisítésre." Adminisztratív szabály, hogy „minősített adatok feldolgozásakor a helyiségben csak betekintésre jogosultak tartózkodhatnak.", illetve „A képernyőn megjelenített adaton a minősítést fel kell tüntetni." Az elektronikus adat is nyilvántartási körbe tartozik: „A minősített adat felírása előtt az adathordozót nyilvántartásba kell venni, kísérőlappal kell ellátni.", az adathordozók is nyilvántartottak kell, hogy legyenek: „a minősített adatot tartalmazó beépített, vagy telepített adattárolót az ügyviteli nyilvántartáson kívül típus és gyári szám szerint a számítástechnikai titokvédelmi felelősnek is nyilván kell tartania.". Az átmeneti másolatok kérdése is szabályozott: „az átmeneti másolatok készítésekor nincs szükség a minősítésre jogosult személy engedélyére, de a másolatot a legrövidebb időn belül nem visszaállítható módon törölni kell.".

Az ügyviteli feladatok mellett a szabályzat a jogszabályban megfogalmazott követelmény szerint meghatározza a minősített adatok elektronikus továbbítására vonatkozó rejtjelzési kötelezettséget. Rögzíti, hogy rejtjelzésre csak jóváhagyott eszközt lehet alkalmazni, illetve ezzel kapcsolatos rendszabály, hogy a vezetési vagy fedőnév és fedőszám táblázatok nem tartoznak a rejtjelzés hatókörébe, az erre vonatkozó megoldások a minősített adatok védelmének körébe tartoznak. Kifejezetten rejtjelzésre vonatkozó követelmény, hogy adattovábbítás csak a rejtjelző eszköz minősítési szintje szerinti, vagy alacsonyabb minősítésű adat esetében történhet, mely rendszabály betartásáért az alkalmazó személy vagy a távbeszélő szolgáltatást igénybevevő személy a felelős. A rejtjelző eszköz engedélyezett szintjét az alkalmazó személyeknek ismerniük kell. [4.][3]

A nem minősített adatok kezelésére vonatkozó iratkezelési szabályzat az iratkezelő szoftver biztonsági kérdéseivel és az elektronikus szervezeti levelező postafiók kérdéseivel foglalkozik, az elektronikus iratokra visszakereshető archiválási követelményt határoz meg, szabályozza az elektronikus irattal kapcsolatos ügyviteli kérdéseket, lehetővé teszi az elektronikus érkező irat átvételének megtagadását kockázat esetén. [5.]

[3] A 2010-ben kormányrendeletben megfogalmazott követelmények alapján az MH-nál is elkészült 2012-ben a minősített adatkezelésre vonatkozó központi Biztonsági Szabályzat (tervezet), mely a bemutatott szabályzat kiváltását célozza. A tervezet az elektronikus információbiztonsági szabályozásra már csak hivatkozik, és kifejezetten csak ügyviteli kérdésekre irányul.

Híradó és informatikai szabályozásban megjelenő megfogalmazások

A szabályozási helyzet objektív megítéléséhez célszerű megvilágítani, hogy nemzeti kormányzati szinten nem minősített elektronikus adatkezelésre vonatkozó általános követelmények jelenleg nem azonosítók. Sspecifikus követelmények jelentek meg pénzügyi, egészségügyi adatok és személyes adatok védelme területén; 1996-ban majd 2008-ban szabványra alapozott – de annak teljesen nem megfelelő –, kormányzati ajánlások kiadása is megtörtént, de ezek kötelező jellegű alkalmazását nem rendelte el jogszabály.[6.] [7.]

Szakmai érdekesség, hogy az állami ellenőrzési feladatokkal megbízott szervezetek informatikai (benne jelentős részben elektronikus információbiztonsági) ellenőrzéseket tartanak, szabályozási hiányosságokat azonosítanak napjainkban is, *de a hiányosságok összehasonlítási alapja nemzetközi szabvány, vagy ajánlás, és nem jogszabályban megfogalmazott követelmény*. Az Állami Számvevőszék elnökének utasítása szerint az informatikai rendszerek ellenőrzése során az ellenőrök vizsgálják, hogy a közigazgatási szervezetnél van-e informatikai stratégia, információ biztonsági politika és informatikai biztonsági szabályzat, és azok figyelembe veszik-e az 1996-os ITB 8-as és 12-es ajánlást, alkalmaznak-e biztonsági osztályokat és kriptográfiai eszközöket.[8.]

Minősített elektronikus adatkezelés esetén az általános követelmények jogszabályban történő egységes megfogalmazása 2010-ben megtörtént, de a keretjellegű megfogalmazáson túlmenően végrehajtást támogató, konkrét követelmények nem azonosíthatók. A minősített adatkezelés területén *megszűnt a NATO, EU és nemzeti adatok védelmére vonatkozó eltérő eljárásrend*. Megjelentek az első kompromittáló kisugárzás elleni védelemre vonatkozó követelmények és megváltozott a rejtjelzésre vonatkozó követelmény és felügyeleti rendszer.

Ezt megelőzően 1999-2010 között a kormányzati szabályozás „kétfokozatú" volt, mert a nemzeti szabályozás mellett megjelent a NATO minősített adatkezelésre vonatkozó követelményrendszer, benne a bonyolultnak tekinthető elektronikus információbiztonsági szemlélet és szabályozás.

Az 1995-ben megjelent minősített adatok kezelését szabályozó kormányrendelet lényegében papír alapú szabályozási szempontokat tartalmazott. Az elektronikus adatkezelés kapcsán csak a hozzáférés korlátozására, az adathordozók nyilvántartásba vételére illetve a rejtjelzési kötelezettségre deklarált szabályokat, az adatkezelésre vonatkozó részletes és végrehajtható követelményeket nem határozott meg, hatósági auditálási vagy akkreditálási feladatokat nem azonosított. [9.][4]

Az eddigiekben vázolt kormányzati követelmények alatti szinten központi szabályozóként azonosítható az 1993-ban kiadott MH Informatikai Szabályzat. A szabályzat szerint a katonai szervezeteknél titkos ügykezelésben is jártas és megfelelő számítástechnikai ismeretekkel rendelkező[5] számítástechnikai felelőst (felelősöket) kell kijelölni. A felelősnek ki kell dolgoznia a Számítástechnikai Védelmi Szabályzatot (SZVSZ), naprakészen kell tartani a számítástechnikai eljárásokba betekintésre jogosultakat, ellenőriznie kell a védelmi előírások betartását, figyelemmel kell kísérni a veszélyforrásokat, és már a tervezési fázisban érvényesíteni kell a titokvédelmi szempontokat.

A szabályzatot a feldolgozott adatok minősítési fokozatának és a katonai szervezet sajátosságainak megfelelően kell készíteni és a parancsnoknak kell kiadnia. A szabályzatban meg kell határozni a felelős és az ügyviteli szerv együttműködésének rendjét. Meg kell határozni a minősített adatok készítésének, feldolgozásának, hozzáférhetőségének,

[4] E „hőskorszak" jellegzetessége, hogy a NATO követelmények honosítására szolgáló első jogszabály *az elektronikus információbiztonsági kérdéseket nem kezelte*, ilyen tartalmú fejezet a kormányrendelet nem tartalmazott. [10.] A helyzet a szakterületet újraszabályozó kormányrendelet megjelenésével 2003-ban változott.

[5] Ez a követelmény a gyakorlatban rengeteg problémát okozott, mivel a „jártasság"-ot a vezetők automatikusan az informatikai állományhoz kötötték. Így az informatikai üzemeltetés biztonsági ellenőrzésének (felügyeletének) felelőssége ugyanarra a végrehajtásban érintett informatikai állományra hárult.

tárolásának, másolásának, felülírásának, megsemmisítésének szabályait. Meg kell határozni továbbá az átmeneti és biztonsági másolatok készítésére, használata, megsemmisítése, valamint a számítógépes vírusok elhárítására vonatkozó előírásokat. [11.]

A vezetékes vagy rádióhíradásra vonatkozó követelmények komplexen tartalmazták a védelmi rendszabályokat, például legkevesebb átkötés, legrövidebb útvonal, vezetékes járőr, jelszavak és jelszámok rendje, hírközpontok őrzése és a beléptetés szabályozása vagy minimális kisugárzott teljesítmény, irányított antenna alkalmazása, minimális adásidő, egyéni billentyűzési jellemzők tiltása, vezetési táblázatok alkalmazása. Részletes, nagy hagyományokkal rendelkező adminisztratív szabályozásnak tekinthető a rádiófogalmi szakutasítás, mely az eljárások között azonosítja a szükséges védelmi rendszabályokat. Kifejezett „híradó biztonsági" területű, önálló központi szabályzat ezek mellett nincs kialakítva.

Az MH-nál az 1999-es NATO csatlakozás okozta azt a változást, ami alapján a biztonsági kérdések elkülönültek az informatikai és híradó szakterületi kérdésektől, másrészt a NATO követelmények szerint megjelent az eddigi szervezeti típusú gondolkodás mellett a szervezeti határokat átlépő hálózati gondolkodás. A minősített elektronikus adatkezelésre ösztönző erővel jelentkezett a NATO követelményrendszer [12.], mert a NATO adatok védelmét a felhasználó és az üzemeltető állománynak közvetlenül a szövetségi követelmények szerint kell, hogy végezze (a jogszabályokban foglalt követelményektől függetlenül). A NATO követelmények gyakorlati adoptálásának negatívumként értékelhető a kezdeti rengeteg félreértelmezés, illetve mesterséges (és gyakran felesleges) nemzeti - NATO elkülönítés, melynek káros hatásait még napjainkban sem sikerült felszámolni.[6]

A NATO követelményeknek való megfelelésnél szakmai érdekesség a NATO/NYEU Központi nyilvántartó és a NATO/NYEU Központi Rejtjelelosztó esete. E központi funkciókkal kapcsolatban egy tárca szintű szabályozási szándék történt 2000-ben.[7] Ezt követően 2009-ben és 2010-ben az ügyviteli és az elektronikus információbiztonsági kérdések kormányrendeletben történő szabályozásakor már említés történik a két funkcióra, megtörténik a tárcavezető miniszter felelősségének kijelölése, de a minősített adatkezelés általános szabályain kívül *részletes működési vagy szolgáltatási követelmények nem azonosíthatók.*

Az MH-nál elektronikus információvédelemre vonatkozó egységes szabályozási szándék 2002-ben kezdődött miniszteri utasítás formájában. Az utasítás az elektronikus információbiztonság szakterületeit a rejtjelbiztonsági, kompromittáló kisugárzás elleni védelmi, átvitelbiztonsági és informatikai biztonsági területekre bontotta. Kijelölte a minisztérium szakfeladatokért felelős szervét, és meghatározta, hogy minden szervezetnél ki kell jelölni az elektronikus információvédelmi szakfeladatokért felelős személyt, vagy szervezeti elemet. A központi szerv feladata az eszközök, eljárások és alkalmazások engedélyezése, a szakfeladatokat végzők számára a képzés és vizsgáztatás irányelveinek kidolgozása, illetve általánosságban szakfelügyelet ellátása, együttműködésben a nemzeti hatósági feladatokat ellátó szervezetekkel.

Az utasítás részletes biztonsági követelményeket, feladatokat nem határozott meg, de ez tekinthető az első olyan szabályozási kísérletnek, amelynek célja egységes, korszerű mederbe

[6] Kivételként kezelendő Király Imre, aki 2002-ben a dokumentumbiztonság helyi szabályozása kapcsán az addigi gyakorlattól eltérően azt írta, hogy „a katonai szervezetek szintjén nem célszerű külön-külön szabályzatban rögzíteni a nemzeti és a NATO adathordozók kezelésével kapcsolatos helyi eljárási szabályokat". [13.]

[7] 4/2000. (II. 29.) HM rendelet és a 13/2000. (HK 6.) HM utasítás a NATO/NYEU Központi Nyilvántartó és a nyilvántartási rendszerről (hatályon kívül).

terelni az elektronikus információbiztonság kérdését és *a korábbi rejtjelzésre koncentráló védelmi szemlélet helyett szélesebb értelmezést kijelölni*.[8] [14.]

Kifejezetten a NATO követelmények adoptálása történt, amikor Váncsa Julianna a NATO Üzemeltetési Biztonsági Szabályzat kialakítására vonatkozó központi segédletet készített 2003-ban.[9] Ugyanígy az ő nevéhez köthető a központi szabályozási kísérlet 2004-ban, amikor a már említett az MH Informatikai Szabályzatba ágyazott elektronikus információvédelmi szabályozás felváltását célozta meg NATO mintát alapul véve, a számítógépes hálózatok és önálló telepítésű eszközök biztonságát komplex módon kezelve (fizikai-, személyi-, dokumentum és elektronikus információbiztonsági szakterületű gondolkodás).[10]

A híradó és informatikai rendszerek biztonságának témakörét is érintette az ellenőrzésekre vonatkozó egységesítési szándék, amelynek megfelelően 2005-ben elkészült a katonai szervezetek központi ellenőrzésére vonatkozó ideiglenes ellenőrzési kézikönyv. A kézikönyvben a szakterületekért felelős szerveknek meg kellett határozni az ellenőrzési szempontokat, illetve az értékelési mutatókat. A mai fogalmakkal elektronikus információvédelem szakterületére vonatkozóan az informatikai, a titokvédelmi és az úgynevezett információvédelmi szakterületen[11] olvashatók ellenőrzési követelmények.

A meghatározottak szerint *informatikai szakterületen* ellenőrizni kell az SZVSZ tartalmát és naprakészségét, az események naplózását és nyilvántartását, az archiválást és az adatmentést.

Titokvédelmi szakterületen ellenőrizni kell az SZVSZ-t és annak felhasználói szintű ismeretét, a számítástechnikai berendezések, eljárások titok és adatvédelmével kapcsolatos előírások betartását, a felelős kijelölését és okmányrendszerét, valamint a felhasználói jogosultságokra vonatkozó követelmények teljesülését. Ellenőrizni kell az SZMSZ-ben a rejtjeltevékenységgel kapcsolatos felelősség, jog- és hatáskör, szabályozottságát. A (helyi) Titokvédelmi Szabályzatnak tartalmaznia kell a rejtjeltevékenységre vonatkozó előírásokat.[12]

Információvédelmi szakterületen ellenőrizni kell az alárendelt szervezetek irányítására, a rejtjeltevékenységre vonatkozó előírások megfelelőségét. Ellenőrizni kell továbbá a béke és tábori vezetési pontokon az információvédelmi eszközök megbízható működését, az elkülönített ügyvitel megvalósulását, a szaküggyviteli szabályok érvényesülését.

A szabályozás területén a következő fejlődési lépcső 2009-ben a honvédelmi tárca információ biztonságpolitika megjelenése,[13] illetve erre építve később alacsonyabb szintű szabályozók kiadása.

A fentiek szerint megfogalmazott rendszabályok és eljárások mellett azonosíthatók még a kiadási formát tekintve azonos elrendelési szintű szabályozók. Erre a teljesség igénye nélkül példaként említhető miniszteri utasítások a NATO Irodaautomatizálási Rendszer (NIAR) biztonsági kérdéseiről,[14] a HM Költségvetési és Gazdálkodási Rendszer (KGIR) üzemeltetésének és biztonságának szabályozása, az Egységes Digitális Rendszer üzemeltetési és biztonsági kérdései, vagy a mobil kommunikációs eszközök biztonsági kérdéseinek szabályozása. Ezekhez hasonlítható szabályozó az MH állandó jellegű távközlő hálózatának békeidejű üzemeltetési és felügyeleti rendjéről szóló vezérkar főnöki intézkedés 2003-ban.

---

[8] Az utasítás a korábban említett 23/1995 (HK 13.) HM utasítást hatályon kívül helyezte.

[9] NATO Irodaautomatizálási Rendszer Üzemeltetés Biztonsági Szabályzat kitöltési útmutató, 2003.

[10] A Honvédelmi Minisztérium és a Magyar Honvédség ideiglenes elektronikus információvédelmi szabályzata (tervezet), 2004. Az ideiglenes szabályozat kidolgozása az első szakmai köröztetés után megállt, a komplex, új szemléletet mutató szabályozási szándék szakterületi támogatások hiányában megszakadt.

[11] Az „információvédelem" kifejezés ebben a szabályozóban egyértelműen „rejtjelzés"-ként értendő, de az akkori szervezeti megnevezések, szokás alapján a „rejtjelzés" kifejezés alkalmazása nem volt gyakorlat.

[12] Ez a követelmény nyilvánvaló átfedés a rejtjelzésre vonatkozó szabályozási követelménnyel.

[13] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról.

[14] A 2002-es szabályozást HM utasítás, Vezérkar Főnöki intézkedés és ezek alapján helyi parancs, valamint a NATO követelmények szerinti rendszer-specifikus biztonsági dokumentumok lépezték.

A híradó és informatikai szakterületen régóta megoldatlan kérdés a szakkifejezések szabályozása, melynek kapcsolódó következménye az információvédelem – szűkebben fogalmazva az elektronikus információvédelem – területén is tapasztalható terminológiai összehangolatlanság. A helyzet rendezésére informatikai szakterületen egy kísérlet történt 2002-ben Munk Sándor vezetésében az akkori ZMNE informatikai tanszék szervezésében, de a megrendezett konferencia és a konferencia kiadvány megjelenéséből adódó hasznon kívül további eredmény nem született.

A jogszabályok értelmező rendelkezésein kívül a szakkifejezések pontos meghatározására a Hadtudományi Lexikon (1995), az önkéntes alapon kialakított Katonai Lexikon 4000, az MH Összhaderőnemi Doktrína (3) által meghatározott rövid fogalomtár, a NATO kifejezések kapcsán pedig a 2012-ben honosított NATO AAP-6[15] állnak rendelkezésre.

A TÉMÁHOZ KAPCSOLÓDÓ HADTUDOMÁNYI FORRÁSOK ÁTTEKINTÉSE

A fontosabb szabályozási lépések bemutatása mellett az eddigi eredmények hasznosítása érdekében célszerű a hadtudományi források lényegi áttekintése is, kifejezetten a 2010-2011. előtti időszakra koncentrálva.[16]

Szabó László 2004-ben az információvédelem tanulmányozása kapcsán a HM szintű fontosabb szabályozók azonosításával rávilágított, hogy a „*szabályozók évszámából is kitűnik egyfajta rendszertelenség*", a szabályozók jelentős része NATO csatlakozás előtti, így nyilvánvalóan nem lehetnek összehangolva a NATO, EU követelményekkel. A nemzeti követelmények területén *a nemzeti elektronikus minősített adatok védelmi kérdése nem szabályozott*, a *rejtjelzésre vonatkozó kormányrendelet túl általános*. A tárcán belüli egységes szabályozási rendszer kialakításának nagy akadálya „*a szervezeti elkülönültségből fakadóan a szakkifejezések nem egységes értelmezése*". A hatékony működés feltételei között fogalmazta meg a szerző az „adat (információ) biztonság *teljes szabályozó rendszerének felülvizsgálata, egységes filozófián alapuló új, átfogó* részletes szabályozók kiadása." követelményt és a továbbképzési rendszer áttekintését, továbbfejlesztését. [16.]

Beinschróth József 2007-ben informatikai területen működésfolytonosság szempontjából vizsgálta az alkalmazható bevált gyakorlat körébe tartozó dokumentumokat és megállapította, hogy *a kérdést taglaló szakirodalom „elsősorban az informatikai biztonságra vonatkozó ajánlásokra támaszkodik"*. Az ITIL,[17] az ITIL-re épülő gyártófüggő megoldások és a COBIT[18] módszertan rövid bemutatása mellett *felhívta a figyelmet az ITIL és a COBIT összehasonlíthatóságára* (megmutatja mely ITIL témakörök fedik a másik ajánlás tartalmi elemeit), illetve utalt arra, hogy NATO szervezeteknél, illetve a brit hadseregnél felismerhető az ITIL alkalmazással kapcsolatos szabályozási szándék. [17.]

Haig Zsolt 2007-es előadásában a nemzetközi szabványokat[19] ismertette, és megállapította, hogy azok „szinte kizárólag az informatika területére koncentrálnak", az ISO/IEC 27000 szabványcsalád tekinthető az első átfogó jellegű szabályozónak. A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság (ITB) ajánlásait tekintve megállapította, hogy azok a kormányzati és a közigazgatási információs rendszerek

[15] NATO Glossary of Terms and Definitions AAP-6 (V). A 2012-ben magyarul megjelenő – egyébként hiánypótlásként értékelhető – NATO szabályozó a szakmai terminológiai helyzet megoldására nem alkalmas.
[16] Az áttekintésben nem szerepelnek a szerző korábbi cikkei.
[17] ITIL: Information Technology Infrastructure Library.
[18] COBIT: Control Objectives for Information and Related Technology.
[19] Ismertetett szabványok: Common Criteria v.2 (ISO/IEC 15408) - Common Criteria for Information Technology Security Evaluation; ITIL v.3 (BS 15000:2000); COBIT4 4.1; és ISO/IEC 27000 szabványcsalád.

biztonságos működtetésének szabályozására születtek, de nem kerültek bevezetésre,[20] majd összegzi, hogy „a szabványok és ajánlások terén látható a törekvés az egységesítésre”, de *a kidolgozók az informatikai biztonságot tekintik szabályozandónak az információbiztonság átfogó szabályzása helyett*. Ennek megfelelően javasolta *egy komplex, infokommunikációs rendszer szemléletű biztonsági szabályozás kialakítását* a kormányzati és a közszféra területén. [18.]

Munk Sándor 2007-ben írt munkájában látható az információbiztonsággal kapcsolatos fogalmak lépésről-lépésre történő megközelítése, alapmodell megjelenítése. A szerző utalt arra, hogy az „információvédelem” kifejezés a múltban más tartalommal bírt (rejtjelzés). A „biztonsági esemény” kifejezés kapcsán kettős jelentés tapasztalható (fenyegetés bekövetkezése az adott objektum sérülése nélkül, vagy bekövetkezett a védendő objektum biztonságának sérülése). Jelentős megállapítás, hogy a biztonság értelmezésénél korábban a védendő objektum az információ volt, míg napjainkban e helyett szélesen értelmezve az információ – információs szolgáltatás – és az azokat biztosító informatikai rendszer értelemben kellene gondolkozni. [19.]

Kerti András 2008-ban megfogalmazta, hogy a szárazföldi csapatok híradásának szervezési elveire vonatkozó szabályzat hatályon kívül helyezése szabályozatlan helyzetet teremtett és cikkében az vizsgálta, hogy helyette egy „infokommunikációs szabályzat”-ot kell kiadni, illetve e mellett szabályozó struktúrát kell kialakítani. A struktúrát az „infokommunikációs irányelv” – a (híradó, információvédelmi és informatikai) doktrínák – és a (híradó, információvédelmi és informatikai szakterületű) szabályzatok rendje képezi. [20.]

Muha Lajos cikkében (2008) vizsgálta a szakkifejezéseket (információbiztonság/védelem, informatikai biztonság, elektronikus információbiztonság/védelem), összefüggéseiket, eredetüket és Munk Sándor 2007-es munkáját hivatkozva jelzi, hogy terminológia területén a tartalmi kérdéseknek elsőbbsége kell, hogy legyen a megnevezésekkel szemben, amit a fordítási problémák bemutatásával is alátámaszt. A szerző „informatikai biztonság” megnevezéssel az MSZ/ISO 27001 szabvány struktúrájához hasonlítható rendszertant mutat be. [21.]

Munk Sándor 2009-es cikkében az új Informatikai Szabályzat kidolgozása kapcsán az informatikai fejlesztés és üzemeltetés területén rámutatott *az új terminológia, szabványok és ajánlások megjelenésére*. Megfogalmazta, hogy *a szabályozás kialakításánál szükség van alapelvek, illetve azokhoz illeszkedő szabályok rögzítésére*. Az alapelveket ellentmondásmentesen kell összeállítani, szükség esetén prioritásokat kell közöttük felállítani, illetve fontos szerepe van az időtállóságnak, beleértve az esetleges pontosítás lehetőségét is. [22.]

Pristyák János 2009-es felsővezetői tanfolyam dolgozatában a kiszolgálás oldaláról közelítve azonosította az MH központi informatikai alapszolgáltatásait és megállapította, hogy „A jelenlegi központi szabályozók elavultak és hiányosak.”[21] A dolgozat átfogóan bemutatja az ITIL és a MOF[22] módszertanokat. Következtetése, hogy *mindkét esetben precíz leírásokra van szükség, a folyamatokhoz mérési elveket és mérőszámokat kell kialakítani*, illetve az, hogy ez a típusú szabályozás átlépi („nem tiszteli”) a szervezeti határokat A szerző javasolja *az üzemeltetés szervezésekor, korszerűsítésekor az ITIL és a MOF módszertani*

[20] A szerző jelzi, hogy a cikk írásakor az ajánlások átdolgozása folyamatban van.

[21] A szerző korábban megállapítja, hogy az informatikai terület működését az 1993-ban kiadott MH Informatikai Szabályzat tartalmazza (röviden ismerteti a benne lévő általános biztonsági követelményeket). Megállapítja továbbá, hogy a NATO, EU minősített elektronikus adatkezelő rendszereket un. rendszer-specifikus dokumentumok szabályozzák, az Üzemeltetési Biztonsági Szabályzat említésénél szerepel, hogy „… a szabályzatra vonatkozó tartalmi és formai követelmény központilag szabályozott.”. További megállapítás, hogy „a honvédelmi miniszter utasításban rögzítette az elektronikus információvédelem általános felelősségi rendjét” (p. 8-9.).

[22] Microsoft Operations Framework (az ITIL nagyvállalati specifikációja).

ajánlások figyelembe vételét, mert az ajánlásokat a szervezetek igény szerint alkalmazhatják, illetve a javasolt a folyamatszemlélet alkalmazása. [23.]

Muha Lajos 2009-es cikkében megállapította, hogy „az infokommunikációs biztonságra vonatkozó ajánlásokat tíz éve nem frissítették, azok elavultak." *A közigazgatásban nincsenek érvényes informatikai biztonsági, infokommunikációs biztonsági követelmények.* [24.]

Talabos Tibor felsővezetői tanfolyam dolgozatával 2010-ben megkezdte a rejtjelzésre vonatkozó 2010-es jogszabály követelménye szerinti szabályozás előkészítését „A HM és MH rejtjeltevékenységének szabályai" címmel, ami a későbbi szabályozási lépések egyértelmű megalapozásaként azonosítható.

Haig Zsolt 2011-es cikkében az információs műveletek sajátosságait, összetevőit tanulmányozta. Az USA Információs Műveletek Doktrína[23] említése mellett azonosítja a NATO hasonló témájú doktrínájában[24] az információs műveletek összetevőit ahol látható, hogy *a korábbiakhoz képest az információbiztonság*[25] *a műveleti biztonság területéből kiválva már önállóan jelenik meg, illetve összetevőként megjelenik a számítógép hálózati műveletek terület is* (Computer Network Operations; CNO). A szerző jelzi, hogy a képességek, eszközök és eljárások azonosítása a doktrínában nem elég pontos, átfedések is azonosíthatók.[26] A magyar Összhaderőnemi Doktrína (2. kiadás) ismertetésekor olvasható, hogy magyar információs műveletek megközelítés összhangban van a NATO szemlélettel. Az új doktrína kidolgozása kapcsán a szerző jelzi a támadó képesség fejlesztésének kérdését, amely területen nem elsősorban a költségigényes megoldásokon van a hangsúly. [25.]

Kovács László – Illés Zsolt 2011-es cikkükben azonosították a cybertér összetettségét, jelezve, hogy a vezeték nélküli tartomány és a vezetékes hálózatok annak egyaránt részei. Megállapítják, hogy *a hatékony felderítést és elemzést nehezíti a szakértők szűkös eszközrendszere, a hatékony kommunikáció hiánya, a szakértők technikai tudásának esetlegessége, illetve a felderítési, nyomozati módszertanok kidolgozatlansága*. Összefoglalásként jelzik, hogy szükség van annak eldöntésére, hogy hazánknak kell-e támadó képességeket fenntartani, illetve ez milyen szervezet feladata kell, hogy legyen. [26.]

ÖSSZEGZÉS ÉS KÖVETKEZTETÉSEK

A fentiek alapján megállapítható, hogy az MH szervezeteinél az elektronikus adatkezelés biztonsági kérdéseinek szabályozására informatikai területen 1993-tól szervezeti szabályozási követelmény szolgál. *Biztonsági célú rendszabályok azonosíthatók híradó és ügyviteli szabályzatokban*. A rejtjelzés szabályozása 1996-tól központi követelmények meghatározását tartalmazó szabályozóban történt.

Közigazgatási szinten kötelező jellegű részletes követelmények, irányelvek, vagy ellenőrzési szempontok nem azonosíthatók, de a megjelent ajánlásokban már megjelent a szabványok alkalmazási igénye.

Az előbbiek alapján megállapítható, hogy az MH elektronikus adatkezelésének szabályozása a jogszabályok követelményeinek megfelelő, de a jogszabályban meghatározottakkal összhangban – főleg a vizsgálati időszakban – nem tekinthető teljes körűnek és részletesnek.

---

[23] JP 3-13; 2006.

[24] AJP-3.10; 2009.

[25] Az információbiztonság a szerző megfogalmazásában a legszélesebb körű kategória (information security), melynek eleme az elektronikus információbiztonság.

[26] A szerző példái mellett szükség van az elektronikus információbiztonság és a számítógép hálózati műveleteken belül azonosított számítógép hálózati védelem (CND) tartalmi tisztázására is, mert „az információs műveleti képességeinek meghatározásakor az egyértelműségre kell törekedni". A cikk összegzésében a szerző kiemeli, hogy „a számítógép hálózatok védelme alapvető fontosságú a hatékony vezetés és irányítás megvalósításához".

A NATO tagság elektronikus információbiztonsági szempontból hajtóerőként értékelhető, mert a jogszabályok alkalmazhatóságától függetlenül[27] megkezdődött az MH-nál a NATO információbiztonsági követelmények alkalmazása. Ezek a változások szervezeti feladatokban történő változásokat is okoztak, mert a volt „számítástechnikai" védelmi kérdések felügyelete ekkor került át az informatikától az akkor „információvédelem"-nek nevezett rejtjelző szakterülethez. Elektronikus információbiztonság területén *a számítógépes hálózatok biztonsága, a kompromittáló kisugárzás elleni védelmi (TEMPEST) kérdések megjelenése egyértelműen támogatták a nemzeti rendszabályok fejlődését*, amely jelenség lassabban, de a rejtjelzés területén is érzékelhető.

Az ismertetett MH szabályozók nemzetközi vagy nemzeti szabványt nem követnek. A *szabályzatok a szabályozási cél szerinti területek mellett jól láthatóan más szakterületekre is kiterjednek*. Ez a szakterületek eltérő feladatrendje miatt jelentősen megnehezíti a rendszabályok pontosításának lehetőségét, ami elavult szabályozást eredményezhet.

Az ellenőrzés egységesítésének szándéka (így az objektivitásra való törekvés) a kiadott ideiglenes szabályzat formájában felismerhető, azonban nyilvánvaló, hogy *az elektronikus információvédelmi kérdések ellenőrzése három szakterület között nem rendezett* (a végrehajtás során nem kevés bonyodalmat okozva).

A jogszabályok a minősített adatkezelést 2009-től egységesítették, de *a nem minősített elektronikus adatkezelés biztonságára vonatkozó követelmények nem azonosíthatók*, illetve *a minősített és nem minősített adatok biztonságának egységes szabályozására vonatkozó közigazgatási szándék sem azonosítható*.

A szakkifejezések kapcsán megállapítható, hogy korszerűségük, illetve más-más szemléletük miatt az említett források az elektronikus információbiztonság, vagy azon belül szűkebb területeken (rejtjelzés, kompromittáló kisugárzás elleni védelem) *nem alkalmasak szakterületi alkalmazásra*.

A szabályozásra vonatkozó *hadtudományi publikációkban megjelent a nemzetközi szabványok, ajánlások megismerésének igénye*, azonosítható az útkeresés, megkezdődött az alkalmazhatósággal kapcsolatos gondolkozás, javaslattétel. *Felismerhető a szabályozási rendben (hierarchiában) történő gondolkozás* az egy-egy szabályzat kiadásának szemlélete mellett. *Megjelent az alapelvek megfogalmazásának igénye is*.

A szabályozási kérdések vizsgálata megalapozza annak kijelentését is, hogy az elektronikus információbiztonság – de tágabban tekintve az információbiztonság és a híradó és informatikai szakterületek – *szabályozási kérdéseinek vizsgálata szegényesen publikáltnak tekinthető*.

Következtetésként levonható, hogy az adatkezelés bonyolultabbá válásával párhuzamosan *megjelent az elektronikus információvédelem szabályozására vonatkozó szakterületi igény is*. A hagyományos értelembe vett katonai „szabályzat"-ban (mint kiadványban) való gondolkodás *a szabályozást rugalmatlanná tette*. A jogszabályok ügyviteli („papír alapú") szemlélete szintén nem támogatta az elektronikus információvédelmi kérdések önálló megjelenését, mely területen a NATO csatlakozással kapcsolatos feladatok jelentettek változást.

A NATO Irodaautomatizálási Rendszerre vonatkozó utasítások kapcsán meghatározható az az igény, hogy a szakterületi kérdések általános szabályozásának támogatnia kell az egyes rendszerek üzemeltetésének és biztonsági kérdéseinek szabályozását. Lehetővé kell tenni, hogy egy központi rendszer specifikus követelmény (érintett szervezetek, hatáskörök és

[27] A NATO (és az erre hasonlító EU) minősített elektronikus adatkezelés szabályozása politika (policy) - direktíva (directive) - irányelv (guideline) logikai vonalon történik. Elektronikus információbiztonság vonatkozásában ez a szabályozási hierarchia tízes nagyságrendű, egymással összehangolt szabályozók halmazát jelenti, melynek magyar alkalmazása napjainkban egy kormányrendelet közvetítésével történik.

feladatok) alapján minden érintett szervezetnél elvégezhetők legyenek a szükséges kijelölések, felhatalmazások.

Ellenőrzési területen az egységes szemlélet támogatása, a rögtönzések elkerülése és az összehasonlíthatóság biztosítása érdekében soron következő feladatnak kell tekinteni a *minél részletesebb ellenőrzési kérdőívek kidolgozását a híradó és informatikai rendszerek védelmi képességeinek azonosítása érdekében*, mely feladat vonatkozik a rejtjelző szakterületre is.

A hadtudományt művelők sok részterületen azonosítottak problémákat. Ennek összefoglalásaként egyértelműen azonosítható a szabványok alkalmazásának igénye, mely területen jelen áttekintés során *nem lehetett olyan megfogalmazást azonosítani, mely az MSZ/ISO 27000-es szabvány alkalmazása ellen érvelt volna*.

A nemzeti követelmények területén a nem minősített és a minősített elektronikus adatkezelés más jogszabályokon alapul és eltérő szabályozási követelményeket határoz meg, ami *fennakadásokat okozhat például különleges jogi helyzetben, ami a Magyar Honvédség szervezetei számára létfontosságú rugalmasságot és gyorsaságot negatívan befolyásolhatja*. Ezen a területen nyilvánvaló *szakterületi feladat az adminisztrációs terheket csökkentő megoldás kialakítása*.

Felhasznált irodalom

[1.] 43/1994. (III. 29.) Korm. r. a rejtjeltevékenységről (hatályon kívül), 7. § (1-2), 8. §, 8. § 7. § (1) (2), 12. §. (5), 16. §. (3), 17. §. (2) és 19. § (1)

[2.] 23/1995. (HK 13.) HM utasítás a rejtjelzés felügyeleti rendjéről (hatályon kívül), 1-3. §.

[3.] 81/1997. (HK 20.) MH PK VKF intézkedés az Internet igénybevételével kapcsolatos titokvédelmi és adatbiztonsági rendszabályok betartásáról

[4.] HM-MH Titokvédelmi és Ügyviteli Szabályzat, Ált/3, 1996, 148, 146, 152, 147, 149, és 111-114. p.

[5.] A Magyar Honvédség egységes iratkezelési szabályzata (Ált/40); 2007; 22. 30. és 54. p.

[6.] Informatikai Tárcaközi Bizottság (ITB) 12. ajánlás, Informatikai rendszerek biztonsági követelményei, 1996.

[7.] Közigazgatási Informatikai Bizottság 25. számú Ajánlása, Magyar Informatikai Biztonsági Ajánlások (MIBA) 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK) 25/1-2. kötet Informatikai Biztonság Irányítási Követelmények (IBIK) 1.0 verzió; 2008. június)

[8.] 6/2011. (X. 7.) ÁSZ utasítása a számvevőszéki ellenőrzésre vonatkozó eljárási szabályok és módszerek alkalmazásáról, valamint azok nyilvánosságra hozataláról, és a végrehajtását szolgáló „Módszertan az informatikai rendszerek kontrolljainak ellenőrzéséhez”, 2004, p. 55, 72. és 91; http://www.asz.hu/modszertan/modszertan-az-informacios-rendszerek-kontrolljainak-ellenorzesehez/it-ell-modsz-2004-02.pdf)

[9.] 79/1995. (VI. 30.) Korm. rendelet a minősített adat kezelésének rendjéről (hatályon kívül), 27. és 31. §

[10.] 56/1999. (IV. 2.) Korm. rendelet a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített, valamint a korlátozottan megismerhető adat védelmének eljárási szabályairól (hatályon kívül)

[11.] A Magyar Honvédség Informatikai Szabályzata, Ált/210, 1993, p. 197. 199 és 200. p.

[12.] 2000. évi IV. törvény az információ biztonságról szóló, Brüsszelben 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről

[13.] Király Imre: A helyi Titokvédelmi Szabályzat rendeltetése, elkészítésének tartalmi követelményei; Új Honvédségi Szemle 2002/9, p. 85.

[14.] 33/2002. (HK 13.) HM utasítás az elektronikus információvédelemről (hatályon kívül), 1-2, 4. p.

[15.] Ideiglenes szakutasítás a katonai szervezetek rendeltetésével összefüggő ellenőrzések követelményeire és értékelési rendjére (Ált/13), 2004; 7.3.1.6, 7.3.2.4, 7.3.5.4, 7.4.1, 7.4.4, 7.6.1, 7.6.2, 7.6.5, és 7.6.6. p.

[16.] Szabó László: az információvédelem továbbfejlesztésnek lehetőségei, 2004, ZMNE, VKT-14 tanfolyamdolgozat, p. 8-9, 37.

[17.] Beinschróth József: a működésfolytonosság kérdése az informatikai rendszerek üzemeltetésére vonatkozó ajánlásokban, Nemzetvédelmi Egyetemi közlemények p. 191, 197-198.
http://portal.zmne.hu/download/konyvtar/digitgy/nek/2005_2/10_beinschroth.pdf

[18.] Haig Zsolt: Az információbiztonság szabályozói és szervezeti keretei; 2007. p. 5, 11.

[19.] Munk Sándor: Információbiztonság vs. informatikai biztonság (A "Robothadviselés 7" konferencián 2007. november 27-én elhangzott előadás kibővített, szerkesztett változata), p. 5, 6, 9 és 19.

[20.] Kerti András: Katonai infokommunikációs rendszerszervezés, Hadmérnök, 2008. június, p. 96-97, 103.

[21.] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, 2008. Robothadviselés Konferencia, p. 139, 147-15
www.portal.zmne.hu/download/bjkmk/bsz/.../4/10_Muha_Lajos.pdf

[22.] Munk Sándor: A katonai informatika alapelvei a Magyar Honvédségben I. (alapok), Hadtudomány, 2009. szeptember, p. 334, 336, és 337.

[23.] Pristyák János: A Magyar Honvédség informatikai rendszere üzemeltetésének megszervezése, ZMNE Kossuth Lajos Hadtudományi Kar, Budapest, felsővezetői tanfolyam szakdolgozat, p. 10, 26, és 34-35.

[24.] Muha Lajos: Infokommunikációs Biztonsági Stratégia, Hadmérnök 2009. március, p. 220.

[25.] Haig Zsolt: Az információs hadviselés kialakulása, katonai értelmezése, Hadtudomány, 2011/1-2. szám, p. 12-28. 24, 25 és 27.

[26.] Kovács László – Illés Zsolt: Cyberhadviselés, Hadtudomány, 2011/1-2. szám, p. 30, 40, és 41.