HADMÉRNÖK

IV. Évfolyam 4. szám - 2009. december

Kassai Károly
karoly.kassai@hm.gov.hu

A HONVÉDELMI TÁRCA BIZTONSÁGPOLITIKÁJÁBAN MEGHATÁROZOTT KÖVETELMÉNYEK, FELADATOK ÉS AZOK FONTOSABB HATÁSAI

Absztrakt

2010. január elsejétől hatályba lépett a honvédelmi miniszter által novemberben jóváhagyott honvédelmi tárca információbiztonság politikája (továbbiakban: politika) [1.]. A cikk a politika központi szabályozó szerepét mutatja be, ismerteti a fontosabb szabályozó elemeket, amelyek meghatározóak a honvédelmi szervezetek szervezeti típusú és rendszer-specifikus információbiztonsági követelményeinek, védelmi rendszabályainak kialakításakor.

From the 1st of January 2010 the Information Security Policy of MoD signed up in November of 2009 by the minister is valid. This article describes the central regulation position of the policy and introduces the key elements which have determining impact in creation of organisation type and system-specific type information security requirements and protection measurements at military organisations.

Keresőszavak: *biztonságpolitika, információbiztonság, információvédelem, informatika, elektronikus adatkezelés ~ security policy, information security, protection of information, IT, information handling*

1. A POLITIKA ALKALMAZÁSA

A honvédelmi tárcánál eddig még nem történt meg az információvédelmi szakterület átfogó szabályozása, így e szabályozó megjelenése új, központilag meghatározott követelményrendszert jelent a honvédelmi tárca szervezetei számára. A belső rendelkezés alkalmazása a honvédelmi tárca szervezeteinél a hatályba lépéstől kötelező. Általános követelmény, hogy az egyéb szakterületeket átfogóan szabályozó, vagy specializált, az adatkezelést is érintő szabályozás csak a politika követelményeivel összhangban készülhet. Ez alapját teremti meg annak, hogy a különböző célú és felépítésű szervezeteknél azonos elvek szerint történjen az adatkezelés szabályozása.

A politika hatályon kívül helyezi a főleg szervezeti kérdéseket tisztázó, az elektronikus információvédelemre vonatkozó belső rendelkezést [2.], ami a végrehajtásra vonatkozó eljárások részletezése nélkül 2002-ben kísérletet tett a NATO és EU védelmi rendszabályok centralizálására. A politika a kompromittáló kisugárzás elleni védelem területén 2010-től az új elektronikus adatkezelő rendszereknél kötelezővé teszi a NATO követelmények közvetlen alkalmazását, ami jogszabályi kötelezettség hiányában is jelzi a honvédelmi tárcánál a nemzeti, NATO és EU minősített elektronikus adatkezelő rendszerek kompatibilitására és az adatmegosztásra vonatkozó kötelezettségek érvényesítési szándékát.

A biztonságpolitika a *biztonsági célok és alapelvek*, a *felelősségi rend*, az *információvédelmi tevékenység szabályai*, az *adatok osztályba sorolásának elvei*, a *kockázatok kezelése*, a *fizikai és környezeti biztonság*, a *személybiztonság*, a *dokumentum biztonság*, és az *elektronikus információbiztonság* területekre bontva határozza meg a legfontosabb követelményeket.

2. INFOMÁCIÓBIZTONSÁGI CÉL ÉS ALAPELVEK

Az *információbiztonsági célkijelölés* a tárcánál alkalmazott elektronikus adatkezelő rendszerek fejlettségének megfelelően, a NATO és EU biztonságpolitikák és a nemzeti információbiztonsági menedzsment szabvány ajánlása szerint történik a bizalmasság, sértetlenség és rendelkezésre állás azonosításával. E célkitűzések mellett az adatkezelésre vonatkozó követelmények szerint a hitelesség, számon kérhetőség, letagadhatatlanság és a megbízhatóság érdekében kockázattal arányos eljárásokat kell kialakítani.

A politika egyik legfontosabb feladata a biztonsági célok végrehajtását támogató *általános alapelvek meghatározása*.

A honvédelmi szervezetek adatkezelő képességeiket csak a jogszabályokban foglalt követelményeknek megfelelően alakíthatják ki. A rendszerek kialakítása és fenntartása során a teljes életciklust lefedő kockázatelemzéssel kell támogatni a védelmi rendszabályok megfelelőségét. A rendszerek kialakítása során a szolgáltatások és a hozzáférések tekintetében a minimalitás elvét teljes körűen kell alkalmazni (rendszerelemre, üzemeltető állományra, felhasználóra), illetve hozzáférés csak a megfelelő személyi feljogosítás alapján biztosítható. A rendszerek használatba vétele csak előre definiált engedélyezési eljárás alapján történhet, illetve az üzemeltetés során a változtatások is engedélykötelesek. A rendszerek kritikus funkcióit megvalósító hardver és szoftver elemek csak a rendszer besorolásának megfelelő tanúsított termékek lehetnek. A rendszerelemek, adatkezelési és üzemeltetési eljárások csak szabványos eljárások lehetnek; a külső csatlakozásokat védelmi mechanizmusokkal kell védeni. A fejlesztésre, tesztelésre és képzésre használt adatkezelő infrastruktúrákat, adatokat egymástól a szükséges mértékben el kell különíteni. A biztonságra hatással lévő eseteket ki kell vizsgálni és a szükséges változtatásokat el kell végezni (üzemeltetési és a biztonsági dokumentumok módosítása).

Az üzemeltetési helyszíntől, biztonsági környezettől és alkalmazott rendszer-specifikus jellemzőktől függetlenül meghatározott alapelvek célja a rendszerek kialakítása és üzemeltetése során a nyomon követhetőség, az átláthatóság, a rendszerek felügyeletének biztosítása, összefoglalóan a rendezettség, a szükséges szintű biztonsági szint garantálása. A fentiekben bemutatott eljárások normálisnak tekinthető üzemeltetési eljárások megléte esetén különleges követelményeket nem jelentenek, csak korlátozzák a rendszerek üzemeltetőinek és felhasználóinak biztonságra veszélyes öntevékenységét. Meghatározzák, hogy az adatkezelő rendszerek esetében az illetékes vezetők azonosítsák a használatbavétel szabályait, a

változásokat tartsák kézben, illetve ne történhessen meg az üzemeltetői, fejlesztői, vagy teszt feladatok erőforráshiány, időhiány vagy éppen szubjektív hiba miatti összemosása, és ez által a szervezetek üzemeltetéséhez és vezetéséhez szükséges adatok és adatkezelő képességek veszélyeztetése.

Elektronikus adatkezelő rendszerek esetében a rendszerek elfogadása különböző szintű és tartalmú eljárásokat jelent. A NATO, EU minősített elektronikus adatkezelő rendszerek használatba vétele a hatályos jogszabályok alapján hatósági eljárás (akkreditálás) alapján lehetséges. Említésre méltó, hogy az EU és NATO biztonsági követelmények akkreditálást BIZALMAS vagy magasabb minősítési szint esetén határoznak meg, hazánkban ez a kötelezettség már KORLÁTOZOTT TERJESZTÉSŰ minősítési szintnél is jelentkezik. A szigorítás eredménye, hogy egy önálló telepítésű számítógép rendszerbe állítása - ami meglévő rendszerekhez képest elenyésző szintű képesség -, egész napos elfoglaltságot jelenthet a Nemzet Biztonsági Felügyelet, a HM Informatikai és Információvédelmi Főosztály, az MH Összhaderőnemi Parancsnokság kijelölt ügyintézőjének, és természetesen visszatérő jellegű elfoglaltság a helyi biztonsági menedzsmentnek. Nemzeti minősített adatok kezelésére történő feljogosításhoz hasonló eljárást jogszabály jelenleg nem határoz meg, csak HM belső rendelkezés szerinti helyi eljárásra van szükség. Rejtjelző eszköz, eljárás esetén a vonatkozó jogszabály kétszintű hatósági eljárást határoz meg (rendszeresítés és használatbavétel) amely hatósági követelmény nem tesz különbséget nemzeti és NATO, EU eszköz, eljárás között, ami szintén elgondolkodtató, és egyben jövőben megoldandó feladatot jelent.

Nem minősített adatok védelmének kialakítása esetén helyi illetékességű használatbavételi eljárás mellett egyes rendszerek, vagy összekapcsolások esetében független szervezet auditálására van szükség. NATO és EU nem minősített adatkezelés esetében vélhetően hasonló eljárásra van szükség azzal a kiegészítéssel, hogy *ezen adatok esetében jogszabály nem határozza meg, hogy kinek, milyen felelőssége van az adatkezelés biztonsága érdekében*.

A kötelezően alkalmazandó irányelvek megfogalmazásának igénye először 2006-ban jelent meg az MH Informatikai Stratégia első változatának kialakításakor, így a Stratégia 2010-es változatának elkészítésekor *kötelezően jelentkező feladat a két szabályozó összehangolása*. A politika felülvizsgálatakor célszerű lesz az alapelvekre vonatkozóan Munk Sándor informatikai szakterületen az alapelvekre vonatkozó kutatásait figyelembe venni [3.].

3. FELELŐSSÉGEK

A *felelősségi rend* meghatározásának legfontosabb eleme a vezetői és a végrehajtói feladatok elhatárolása, valamint az adatkezelés érdekében szükséges együttműködés alapvető követelményeinek meghatározása.

A *vezetői feladatok* közé tartozik a jogszabályban rögzített titokvédelmi felügyelő illetve biztonsági megbízotti, rejtjelfelügyeleti, iratkezelés felügyeleti, adatvédelmi felelős feladatok azonosítása, valamint a nemzeti ajánlás szerinti elektronikus adatkezelésért felelős elektronikus információvédelmi felügyelői feladatkör. Kis szervezeteknél, áttekinthető homogén elektronikus adatkezelő rendszer alkalmazása esetén akár egy személy is elláthatja az elektronikus információvédelmi szakfeladatokat, de bonyolultabb esetben már rendszer-specifikus felelősségi köröket kell azonosítani. Az adatvédelmi felelős és az elektronikus információvédelmi szakfeladatokat ellátó személyek között együttműködést egyértelműen rögzíti a politika, mert meghatározza, hogy az adatvédelmi felelős követelményei szerint a

szükséges védelmi rendszabályok kialakítása és megvalósítása az elektronikus információvédelmi szakállomány feladata.

A fenti feladatok kapcsán megjegyzendő, hogy egységes, kötelező érvényű nemzeti követelmény nem áll rendelkezésre a fenti feladatokra történő személyi felkészítés érdekében.

A *végrehajtói feladatok* között az előbb említett rendszer-specifikus elektronikus információvédelmi feladatok között a rendszerbiztonsági felelősöket kell érteni. Új elem a BIZALMAS és magasabb minősítési szint esetén alkalmazandó kompromittáló kisugárzás elleni védelmi felelős feladatkört, amelyet más megbízás mellett, vagy önálló megbízásként kell kialakítani a honvédelmi szervezeteknél, az alkalmazott elektronikus adatkezelő rendszerek bonyolultságának, méreteinek megfelelően. A honvédelmi szervezeteknél a rejtjeltevékenységtől függően rejtjelző, vagy rejtjelző nyilvántartó beosztásokat kell kialakítani, vagy a feladatok ellátására alkalmas személyt kell megbízni.

A végrehajtói feladatok kijelölése során tervezési szempont, hogy az adatkezelő rendszereket, vagy nagyobb rendszer esetében az alrendszereket, végpontokat felügyelő szervezeti elemek, felelősök között felügyelet nélküli terület ne maradjon, illetve ne legyen átfedéses a szabályozás. Ezek a szervezési feladatok ott jelentenek kihívást, ahol több honvédelmi szervezet közösen használ egy-egy rendszert, illetve az üzemeltetés több szervezet feladata. Ilyen esetekben egy szervezet nem képes megoldani egy adatkezelő rendszer biztonságos üzemeltetését, *szervezetek közötti együttműködési megállapodásokra, a védelmi rendszabályok és felelősök tevékenységének összehangolására van szükség.*

A politika lehetőséget teremt a honvédelmi szervezeteknél a felelősségek és szakfeladatok összevonására (melyek előnyeit kis szervezetnél, vagy egyszerűnek tekinthető adatkezelés esetén célszerű kihasználni), csak a helyi sajátosságok szerinti összeférhetetlenségeket kell szakszerűen vizsgálni. Ez általában elektronikus adatkezelés esetén lehet bonyolultabb, amikor az üzemeltetői, felhasználói, információvédelmi, biztonsági felügyeleti és esetleg tervezői, fejlesztői feladatokat kell összehangolni, illetve elhatárolni. Ilyen esetekben segíthet az érintett adatkezelő feladatok pontos vizsgálata, a kockázatok elemzése, vagy létszámhiány, speciális üzemeltetői környezet esetén a kiegészítő védelmi rendszabályok alkalmazása.

A szakirányítási feladatok azonosítása mellett megtörténik a *középszintű katonai szerv* feladatának és a *honvédelmi szervezet szintű* feladatok azonosítása. *A középszintű katonai szervnek egyértelműen ráhatással kell lennie az alárendelt szervezetek szakmai tevékenységére*, ami a hadműveleti igényeken keresztül a fejlesztési irányok meghatározása-, a szervezetek felépítése és állománytáblája-, az ellenőrzési tevékenység során a rendellenességek feltárása-, a képzések és továbbképzések szervezése, erőforrások biztosítása területek mellett az adatkezelő rendszerek életciklusa során számtalan egyéb feladatot is tartalmaz.

A jogszabályok, egyéb követelmények szerint kialakított és üzemeltetett rendszerek biztonsága érdekében az ismertetett vezetői feladatokat ellátó személyeknek és végrehajtóknak kötelező az együttműködés, illetve a szolgáltatást nyújtó szervezet tevékenységén belül felelős a védelemért. *A szolgáltatást nyújtó és az alkalmazó szervezeteknek kötelező az együttműködés* az adatkezelés biztonsága érdekében.

4. SZABÁLYOZÁS

Az információvédelmi tevékenység szabályai részben a szabályozási rend azonosítása történik. Az iratkezelés, a minősített adatok védelme, az elektronikus adatkezelés védelme kétszintű szabályozáson alapul (*központi és helyi szabályozás*).

A jelenlegi szakmai álláspont szerint a rejtjeltevékenység szabályozása nem kétszintű, csak *központilag* szabályozott. Nyilvánvaló, hogy e szakterületnél is érvényes az a jelenség, hogy egy-egy szakfeladatot, folyamatot a szükséges részletezettséggel csak helyben lehet szabályozni. Az elektronikus adatkezelés fejlődésével, a hálózatok gyarapodásával párhuzamosan előre jelezhető, hogy a rejtjelzés területén is megjelenik a kétszintű szabályozásra vonatkozó igény.

Az elektronikus adatkezeléssel kapcsolatos védelem szabályozása területén a jelenlegi technológiai szinten szükség van a honvédelmi szervezetek esetében a *helyi hálózatok és egyedi eszközök tömegének szervezeti szintű szabályozására*. Rendszerek esetében *rendszer-specifikus szabályozást kell kialakítani* úgy, hogy a két szabályozás egymást ne korlátozza, illetve ne keletkezzen bürokratikus célú, használhatatlan, a napi életet megfojtó rendszabály halmaz.

5. AZ ADATOK BIZTONSÁGI OSZTÁLYBA SOROLÁSA

Az egyik legjobban félreértett, és egyben közigazgatási szinten központi szabályozás nélküli terület az adatok besorolási kötelezettsége, melynek célja a szükséges mértékű védelem kategorizálhatóságának megteremtése.

A jogszabályokban egymástól eltérő megfogalmazású besorolási rendszerek találhatók, illetve általánosságban kijelenthető, hogy keveredik a kárérték szerinti besorolás és a bizalmasság szintje szerinti besorolás. E két besorolási rendet az alkalmazó szervezeteknek egymás mellett kellene alkalmazni, mert a kizárólag kárérték szerinti megközelítés téves vezetői, üzemeltetői és felhasználói reakciókhoz vezethet. Az országos lefedettség igénye szerinti Egységes Digitális Rendszer esetében például egy kézi rádió érteke szerint alacsony besorolású, de egy katasztrófa helyzetben, vagy egy rendőri intézkedés során egy-egy eszköz által nyújtott adat vagy hang kommunikációs szolgáltatás - vagy annak hiánya - könnyen kritikussá válhat. A légi vezetés és irányítás támogatását szolgáló NATO elektronikus adatkezelő rendszerek esetében egy-egy számítógép vagy rádió távvezérlő által biztosított képesség megléte vagy hiánya (egy kiegészítő elem, vagy alacsony értékű alkatrész meghibásodása, kellékanyag hiánya) szintén olyan példák, amelyek rámutatnak, hogy a kizárólag érték alapú megközelítés a közigazgatásban vagy a honvédelem területén esetenként félrevezethető lehet.

Az honvédelmi tárca adatait a minősítési szintekhez igazított biztonsági osztályokba kell sorolni. A nem minősített adatok esetében az ALAP biztonsági osztály mellett megjelenik a FOKOZOTT biztonsági osztály. Ennek feladata, hogy lehetőség legyen a nem minősített, de funkció vagy halmozódási hatás miatt érzékeny adatok védelmi szintjének emelt szintű kialakítására. Így kell védeni az országos rendszerek központi üzemeltetési adatbázisait, címtárait, a nagymennyiségű üzleti vagy személyes adatokat, a különleges adatokat. Ez a védelem általában a fizikai védelem emelt szintű rendszabályaival (beléptetés, őrzésvédelem), egyedileg kialakított üzemeltetési környezettel, a személybiztonság egyedi szabályaival (nemzetbiztonsági ellenőrzés, általános és szakmai végzettségre, gyakorlatra vonatkozó követelmények) valósítható meg.

Az osztályba sorolással kapcsolatosan egységes közigazgatási követelmények-, illetve a pontosan összehangolt védelmi rendszabályokra vonatkozó követelmények hiányában nehéz annak eldöntése, hogy milyen egységes elgondolás szerint kell elképzelni a különböző célú rendszerek összekapcsolását, adatkezelő szolgáltatások rendelkezésre bocsátását más szervezet felhasználói számára, így előre jelezhető, hogy ezen a területen is valamilyen kormányzati szintű központi rendezés várható.

6. A KOCKÁZATOK KEZELÉSE

Jelenleg a minősített vagy a nem minősített adatokat kezeléséhez kialakított infrastruktúrákra kötelező jellegűen érvényes kockázatelemzési kötelezettség nincs. Hiányzik az egységes nemzeti módszertan (vagy nemzetközi szabványokra, esetleg ajánlásra épített módszertan). A kockázatkezelési tevékenység csak a pénzügyi szektorban kötelező; a közigazgatásnál a szervezeti kockázatok kezelésének rendjébe az adatkezelés ugyan beletartozik, de az alkalmazó szervezeteken múlik, hogy milyen mélységig foglalkoznak ezzel a témával.

A politika a honvédelmi szervezetek esetében a hagyományos vagy elektronikus adatkezelő rendszerekhez életciklusban rögzített feladatként hozzárendeli a kockázatelemzést és kezelést. Az életciklus említése azért fontos, mert összetett rendszer kialakításakor a hadműveleti (alkalmazói) követelmények, a műszaki követelmények és a részletes műszaki tervezés, a kivitelezés (benne telepítés, tesztelés) és az üzembe helyezés más-más szervezetek hatáskörébe tartozik. A részletes műszaki tervezésnek reagálnia kell a kockázatelemzés során megállapított hiányosságokra és sebezhetőségre, tehát a hadműveleti (alkalmazói) követelmények elemzése, a rendszer szintű kockázatfelmérés és értékelés kiegészítő adatokkal, követelményekkel pontosítja a műszaki tervezést. Ha a kockázatkezelés során szervezeti határokat kell átlépni, kiemelkedő szerepe van a szervezeti együttműködésnek, a vezetői szándék esetleges pontosításához, módosításához szükséges visszacsatolás működésének, illetve az adott műszaki megoldás ellenőrzése érdekében a többfokozatú biztonsági tesztelésnek, ami a műszaki követelményeket meghatározó szervezet felelősségét hangsúlyozza.

A politika minősített adatkezelés-, több szervezet által közösen üzemeltetett rendszer-, illetve MH szintű rendszer esetében kötelezővé teszi a kockázatkezelést, melynek felelősségét az adatkezelésért felelős honvédelmi szervezet vezetője viseli. A kockázatelemzés során két szintre tagolt eljárást kell alkalmazni, ki kell mutatni és jóvá kell hagyni a maradvány (vagy elfogadható) kockázatokat, illetve a rendszer életciklus állapota szerint szükségszerűen részletezetten, ismétlő jelleggel kell végezni ezeket a szakfeladatokat. A kockázatelemzés során keletkezett adatokat a rendszer biztonsági dokumentumaihoz kell csatolni, és az időben következő biztonságot is érintő szakfeladatot (pl. akkreditálás, auditálás, rendszerfejlesztés vagy átalakítás) ezekre az adatokra kell építeni.

7. A FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

Adatkezelés az adatok biztonsági osztálya szerint kialakított környezetben engedélyezhető. Nagykiterjedésű rendszerek, érzékeny adatok esetében megjelenik a FOKOZOTT biztonsági osztály kialakítására vonatkozó követelmény, egyébként jól alkalmazható a NATO, EU adatkezelés során alkalmazott adminisztratív zóna, illetve a minősítési szinthez kötött I. vagy II. osztályú biztonsági terület szerinti szemléletmód.

NATO és EU minősített adatkezelés esetében hazánkban az illetékes hatóság kettős eljárást alkalmaz: külön hatósági eljárással dönt a fizikai-, személyi-, és dokumentumbiztonsági

megfelelőségéről, valamint az elektronikus információbiztonsági megfelelőségről. Nemzeti adatkezelés esetén jogszabály hasonló követelményt nem határoz meg. A rejtjeltevékenységre külön jogszabály határoz meg eljárásokat.

Előrelépést jelentene elektronikus adatkezelő rendszerek esetén a hatósági eljárások összevonása, illetve a nemzeti és egyéb adatkezelés egységes eljárásrendben történő rendezése, így ezen a területen is fejlődés várható.

A fizikai biztonsági szakterületen gyakorlati változás érzékelhető, mert az újabban kialakított üzemeltetési helyszíneken már pontosabban kerül mérlegelésre az adatkezelés típusa és az adatkezelés személyes felügyeletének védelmi elemként történő értékelése. Pozitív jelenség a NATO csatlakozás időszakában szigorú nemzeti - NATO elkülönítés átalakulása inkább funkcionális elkülönítéssé.

8. A SZEMÉLYI BIZTONSÁG

A hagyományosnak tekinthető nemzetbiztonsági ellenőrzés, titoktartási nyilatkozat, és NATO, EU minősített adatokat kezelő rendszer esetében a szükséges szintű személyi biztonsági tanúsítvány megléte mellett a politika meghatározza az *összeférhetetlenség vizsgálatára vonatkozó kötelezettséget*, rögzíti, hogy hozzáférési jogosultságok csak adott munkakör ellátásának idejére szólóan adhatók. Külső fél (szerződéses partner, együttműködő szervezet alkalmazottja) által történő üzemeltetési feladatok, vagy felhasználói hozzáférések esetében meghatározza *a kiegészítő védelmi rendszabályok meghatározásáért való felelősséget*.

9. A DOKUMENTUMBIZTONSÁG

Az évtizedeken keresztül formált, pontosított ügyviteli és dokumentumvédelmi rendszabályok megléte nem teszi szükségessé kiegészítő eljárások meghatározását, így a politika ezen a területen főleg az elektronikus adatkezelés sajátosságaira reagál.

Az adathordozók használatbavétele előtt kötelező a funkcionális és a vírusvédelmi ellenőrzés, kezelési jelzések feltüntetése és nyilvántartásba vétel. Az adatok törlése, illetve az adathordozó megsemmisítése a biztonsági osztálynak megfelelő eljárással történhet.

10. AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁG

Az elektronikus adatkezelés során a biztonsági célok elérése érdekében a jogszabályokban és egyéb szabályozókban meghatározott minimum védelmi rendszabályokat kell alkalmazni, melyeket a kockázatelemzés által kimutatott, veszélyesnek ítélt fenyegetések és sebezhetőségek ellensúlyozása érdekében meg kell erősíteni. Az adatkezelő képességek kialakítása és üzemeltetése során tudatos kontrollt kell alkalmazni az üzemeltetési és felhasználói tevékenységek felügyeletére, a rendszer állapotának figyelemmel kísérésére, illetve minden rendszer esetében ki kell alakítani azt a jelentési és tájékoztatási rendszert, ami a rendellenes működés vagy biztonsági incidensek mielőbbi felszámolásához szükséges.

A honvédelmi szervezetek működéséhez és irányításához szükséges elektronikus adatkezelő szolgáltatások védelmére - amennyire az lehetséges - azonos védelmi rendszabályokat kell kialakítani a különböző identitású (nemzeti, NATO, EU, két-, vagy többoldalú szerződésen alapuló) adatok védelme érdekében.

Az információvédelmi védelmi rendszabályokat kiegyensúlyozva, a teljes életciklus során kell alkalmazni. A katonai sajátosságok gyakori kihívást jelentenek a védelmet kialakítók, az üzemeltetők, a biztonsági menedzsment, illetve a különböző hatóságok számára. A mobilitás vagy hordozhatóság követelménye, a speciális alkalmazások, a hálózati kapcsolati-, a különböző identitású adatok együttes kezelésére vonatkozó igény gyakran jelent olyan kihívást, amikor *a jogszabályok szellemében önálló megoldásokat kell kialakítani és jóváhagyatni*, mert átfogó jellegű kormányrendeletektől nem várható el a katonai sajátosságoknak megfelelő specialitások részletes szabályozása.

A katonai képességek szervezeti szintű védelme érdekében egyértelmű követelmény, hogy az egyre bonyolultabb elektronikus adatkezelő képességek kialakításához, teszteléséhez, fenntartásához, ellenőrzéséhez szükséges technikai műveleteket - amennyiben lehetséges -, honvédelmi szervezettel kell elvégeztetni, és csak a megfelelő képességek hiányában lehet külső erőforrásokat igénybe venni.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A hivatkozott, szakmai előzmény nélküli belső rendelkezés láthatóan szerteágazó jogszabályi és NATO, EU követelmények összehangolását végzi. Az információvédelem szakterületeire vonatkozó átfogó követelmények megfogalmazása alapot ad a szabályozási rend korszerűsítésére és az alacsonyabb szintű szabályozók megalapozására. Korszerűségének szükséges és nélkülözhetetlen feltétele: a szabályozásért felelős szervezeti elemnek legyen szakmai elkötelezettsége és erőforrása a jogszabályok és egyéb követelmények változása-, illetve az alkalmazás során tapasztalt hiányosságok észlelése esetén a politika felülvizsgálatára és a változások átvezetésére, szélsőséges esetben akár új szabályozó kiadására a technikai és technológiai változások felgyorsulása mellett több éves lemaradással rendelkező szabályozók „bennragadása” fenyegetettség elkerülése érdekében.

A 2010. április elsejétől hatályba lépő minősített adat védelméről rendelkező törvény [4.] és végrehajtási utasításai is vélhetően szükségessé teszik a felülvizsgálatot, ami jelzi, ezt a politikát a szakmának célszerű valóban „élő dokumentum”-ként kezelni. A felülvizsgálatnak célszerű lesz vizsgálnia azt a NATO csatlakozás óta nem pontosan rendezett kérdést is, hogy kinek, milyen szabályozás keretén belül kell meghatároznia a honvédelmi tárcára kirótt NATO/NYEU Központi Rejtjelelosztó (National Distribution Authority; NDA) és a NATO/NYEU Központi Nyilvántartó (Central Registry; CR) országos hatáskörű nemzeti feladatokat.

Hivatkozások

[1.] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról

[2.] 33/2002. (HK 13.) HM utasítás az elektronikus információvédelemről

[3.] Munk Sándor: A katonai informatika alapelvei a Magyar Honvédségben I. (alapok); Hadmérnök, IV. Évfolyam 3. szám, 2009, p. 333-340.

[4.] 2009. évi CLV. törvény a minősített adat védelméről