HADMÉRNÖK

V. Évfolyam 1. szám - 2010. március

Kassai Károly
karoly.kassai@hm.gov.hu

AZ ELEKTRONIKUS ADATKEZELŐ RENDSZEREK EGYES BIZTONSÁGI KÉRDÉSEI

Absztakt

Az elektronikus adatkezelés biztonsága a jelenlegi szabályozók alapján hazánkban összetett kérdés. A minimális szintű védelem meghatározása, a rendszer életútján keresztül a védelmi feladatok ellátása tartalmaz néhány nem általánosan ismert feladatot. A cikk néhány fontosabb, az életciklus szemlélet szerinti biztonsági kérdés bemutatását célozza, mint a hadműveleti követelmények, kockázatelemzés és a tesz feladatok.

The secure electronic information handling is a comprehensive issue according to the relevant governmental regulation in Hungary. The determination of the minimal level of security and the permanent security support during the system life cycle consists of some specific tasks witch are not too known. This article describes some important security issues during the all life cycle of information and CIS as operational requirement, test and risk assessment.

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

BEVEZETÉS

Az elektronikus adatkezelő rendszerek biztonságos üzemeltetése a honvédelmi szervezeteknél a robbanásszerűen fejlődő technológia, a növekvő alkalmazói igények, a folyamatosan változó információs fenyegetettségek és sebezhetőség miatt egyre bonyolultabb kihívás.

A kihívást erősíti a szervezetek csökkenő anyagi erőforrása, a híradó és informatikai szolgáltatások tervezésére és kivitelezésére biztosított kapacitások szűkössége, valamint a műveletek felgyorsult tempójából következő folyamatos időzavar. Emiatt szükség van az elektronikus adatkezelő rendszerek, eszközök életútjának tudatos menedzselésére, mert a biztonsági kérdések figyelmen kívül hagyása, vagy rossz értelmezése többszörös kiadásokat, funkcionális zavarokat, vagy hatósági engedélyek megvonását eredményezheti. Az életciklus

szemlélet támogatása érdekében a cikk a hadműveleti (alkalmazói) követelmények, kockázatelemzés, és a tesztelés egyes kérdéseire keresi a választ.

1. A HADMŰVELETI KÖVETELMÉNYEK MEGHATÁROZÁSA

Új képességek kialakításakor, meglévő képességek fejlesztése, átalakítása során *a legelső, gyakran félreértelmezett feladat a hadműveleti (alkalmazói) követelmények tisztázása*.

Az elektronikus adatkezelő képességekre vonatkozó követelmények a tapasztalatok szerint *az esetek többségében valamilyen meglévő képesség, vagy máshol látott eszköz, rendszer megoldás azonosítása*. Így kerülhetnek segély, ajándék, vagy más szervezet példája alapján eszközök, rendszerek, szoftverek alkalmazásra, melyek rendszerbe történő integrálása, fejlesztése, vagy testre szabása összességében esetenként erőforrás igényesebb, mint a követelmények valódi végiggondolása.

Információbiztonsági szempontból ez a jelenség fokozottan veszélyes, mert az így kialakított adatkezelő szolgáltatás vagy több, vagy kevesebb, mint az adott feladathoz szükséges lenne, ami mindkét kimenet esetében jelentős fenyegetéseket és sebezhetőséget eredményezhet. *Híradó, informatikus kollégák jelentős kihívás előtt állnak, amikor elmagyarázzák, jelentik, hogy feladatszabáskor ne számítógép vagy rádiótípus, operációs rendszer vagy alkalmazói program, hanem a vezetéshez, döntés előkészítéshez vagy döntéshez, szervezeti működéshez szükséges adat és annak jellemzői, a rendelkezésre állással kapcsolatos igények kerüljenek azonosításra, ráadásul a lehető legpontosabban*.

Tanúságos eset, amikor nemzetközi környezetben egy kritikus fontosságú szakterületen hadműveleti feladatokhoz szükséges kommunikációs igényre egy nem NATO tagállam főtisztje NATO TITKOS minősítésű elektronikus adatkezelő rendszerhez kért munkaállomást. Hosszú percekbe került annak elmagyarázása, hogy munkaállomáshoz való hozzáférés helyett az igénylő legyen szíves, azonosítsa *a szakmai feladat tervezéséhez és támogatásához szükséges beszerzendő adatokat* (minősítési szint és kezelési jelzés), *adatforrásokat, formátumot, frissítési igényt és a szakma specifikus sajátosságokat, valamint azokat a partnereket, akiknek adatokat kell továbbítania* (természetesen a már említett kiegészítő információkkal együtt). Második lépésként a kommunikációt szervező elem kialakítja, hogy az adatcsere szükséglet *milyen külső kapcsolatokat igényel, illetve milyen belső kommunikációra van szükség*. Ennél a fázisnál már szerepet kapnak az információbiztonsági kérdések is. Következő lépés az igényelt képességekhez *a szükséges erőforrások biztosítása* - mint napjainkban aktuális kérdése-, mert a pattogóan rugalmatlan feladatszabás, a feszes határidők az esetek túlnyomó részében hatványozottan erőforrás igényesek. Emiatt *a végleges jóváhagyás előtt gyakran szükség van a követelmények többlépcsős pontosítására*, az erőforrás szükségletek és a lehetőségek összehangolására. Az említett példa esetében az egymondatos igény helyett egy hétre volt szükség az információs szükséglet összeállításához.

A hálózatalapú képességek (Network Enabled Capability; NEC) egyik kulcskérdése az *információcsere, ami különböző hálózatok összekapcsolását igényli*. Az összekapcsoláshoz szükséges feladatok információbiztonsági szempontból fontos elemei a következők:

Az összekapcsolás létrehozását és fenntartását az érintett szervezetek között együttműködési megállapodásban kell rögzíteni. Ez a feladat a honvédelmi tárcánál megköveteli *a honvédelmi szervezetek közötti együttműködési feladatok rögzítési kötelezettségét* például a helyi hálózat – transzport hálózat esetében is, mert egyes feladatokat

nem lehet egy szervezet belső rendelkezésében szabályozni. Az összekapcsolásban érintett szervezet(ek) feladatainak kialakításakor a következő szempontokat kell figyelembe venni:

1) Az összekapcsolás szintjét (a korlátozott adatcserétől az alkalmazások és adatok teljes jogú megosztásáig terjedő szolgáltatások), és módszerét (dedikált vonal, VPN, egyéb).
2) Az összekapcsolás hatását a meglévő hálózatok infrastruktúrájára (pl. új hardver, szoftver komponensek és azok telepítésének hatása az egyéb elemekre), és működtetésére (adatforgalom növekedés, új képzési követelmények, új rendszeradminisztrátori, információvédelmi és fenntartási feladatok).
3) Az adatok védelmi szükségletét:
   a) a cserélt adatok, vagy egy irányba továbbított adatok biztonsági osztályát, az ezen belül alkalmazandó általános vagy specifikus védelmi igényt;
   b) a szervezetek közötti adatcsere során küldött és vett adatok jelölését, illetve a törléssel, megsemmisítéssel kapcsolatos feladatokat.
4) A felhasználói kört, a felhasználói profilok kialakításával és fenntartásával kapcsolatos feladatokat, az adatok nyilvántartásával kapcsolatos feladatokat (személyi biztonsági tanúsítvány, egyedi feljogosítás), a munkaállomások, adatkezelő eszközök azonosítását, a felhasználók azonosítására és hitelesítésére szolgáló eljárásokat).
5) Az összekapcsolás által biztosított szolgáltatásokat és alkalmazásokat.
6) Az összekapcsoláshoz szükséges technikai rendszernél azon beosztásokat, melyeket két, vagy több fő láthat el (pl. karbantartás, felhasználói profilok kezelése, biztonsági felügyelet).
7) Az incidenskezeléshez szükséges feladatokat:
   a) a működési rendellenességek, incidensek jelentéséhez, kivizsgálásához és a szükséges válaszlépések megtételéhez szükséges rendszabályokat (kinek, milyen esetben milyen jelentést kell tennie);
   b) azoknak az incidenseknek az azonosítását, melyek az együttműködő szervezetektől összehangolt tevékenységet igényelnek.
8) A szolgáltatás folytonossággal kapcsolatos feladatokat:
   a) a szervezetek folytonossági tervének kiegészítése az összekapcsolásból adódó technikai és együttműködési feladatokkal;
   b) a vészhelyzetben kapcsolattartó személyek, szervezeti elemek azonosítása;
   c) az összekapcsolásra vonatkozó redundancia kialakításával, fenntartásával, aktivizálásával, tesztelésével és ellenőrzésével kapcsolatos feladatok;
   d) a vészhelyzetek megoldásával kapcsolatos teszt, képzési és gyakorlási feladatok.
9) A biztonsági mentésekre vonatkozó követelményeket:
   a) az összekapcsoláson keresztül továbbított adatok mentési szükségletének azonosítása, és a mentések kezelésére vonatkozó rendszabályok (gyakoriság, felelős szervezet vagy minden szervezet);
   b) a mentések felhasználására vonatkozó eljárások;
   c) a naplófájlok mentésére és tárolására vonatkozó rendszabályok.
10) A változáskezelés feladatait:
   a) a változások kezelésével kapcsolatos azon feladatok azonosítása, melyek hatással lehetnek az összekapcsolásra (hardver és szoftver-frissítések, kiegészítő szolgáltatások bevezetése);

b) a szervezeteknél a változások hatásainak vizsgálatával megbízott személyek, valamint a tájékoztatási kötelezettségek azonosítása.

11) A biztonsági képzés és továbbképzés követelményeit:

a) az összekapcsolás üzemeltetésével, biztonsági feladatainak ellátásával, illetve az adatcsere szolgáltatást felhasználó személyek feladatainak ellátásához szükséges képzési feladatok;

b) a képzések gyakorisága, tematikája, illetve a végrehajtásért felelős személyek (szervezeti elemek);

12) Az összekapcsolás kialakításával, fenntartásával, menedzselésével kapcsolatos feladatokat, beleértve a rendszeradminisztrátorok, karbantartók, biztonságért felelős személyek feladatait.

13) Az összekapcsolás kialakításával fenntartásával, illetve a technikai rendszer továbbfejlesztéséhez szükséges pénzügyi tervezési és jóváhagyási folyamatokat.

Kialakítás előtt *kockázatfelméréssel kell azonosítani az összekapcsolásra vonatkozó fenyegetéseket és sebezhetőséget*, majd az üzemeltetés időszaka folyamatosan kell végezni a kockázatmenedzsment feladatokat.

Az összekapcsolás eszközeinek, interfészeinek és szolgáltatásainak pontos konfigurálásának-, a kialakított eljárások helyességének ellenőrzése érdekében az üzemeltető szervezetnek (szervezeteknek) tesztet kell végezni, melyet *előre meghatározott szempontok szerint kialakított terv alapján kell végrehajtani*. A teszt tervet az illetékes biztonsági hatósággal kell jóváhagyatni. Ez a tervezett, felügyelt és dokumentált folyamat kicsit eltér a „majdnem ugyanolyan, mint a másik", a „másik is lefagy időnként", vagy a „szabvány beállítások esetén nem kell vele foglalkozni" vélekedésektől és *rendszerösszeomlástól, adatvesztéstől, idegességtől menti meg az üzemeltetőt, az esetleges egyéb biztonsági vonzatokról nem is beszélve*.

Az üzemeltetők, rendszeradminisztrátorok és biztonságért felelős személyek számára *biztosítani kell a szükséges üzemeltetési és biztonsági ismereteket nyújtó képzést* és továbbképzést az összekapcsolást biztosító technikai rendszer teljes életútja során.

Az összekapcsolás által biztosított szolgáltatások korlátozására, vagy a csatlakozás megszüntetésére vonatkozó szervezeti és egyéni feladatokat, illetve az ezekkel kapcsolatos feltételeket *a rendszer-specifikus biztonsági dokumentumokban részletesen ki kell dolgozni*.

2. A KOCKÁZATELEMZÉS KORSZERŰSÍTÉSE

A honvédelmi szervezetek vezetéséhez és működéséhez szükséges elektronikus adatkezelő rendszerekre vonatkozó biztonsági követelmények és védelmi rendszabályok *a vonatkozó NATO, EU követelmények alapján csak kockázatfelmérés, elemzés és értékelés alapján határozhatók meg hatékonyan*.

A nemzeti kormányzati infrastruktúrákhoz való csatlakozás előfeltétele a kapcsolódó rendszerek védelmi rendszabályainak összehangolása, valamint a külső kapcsolati rendszer szükséges mértékű védettségének kialakítása, amit szintén kockázat felmérésre és elemzésre támaszkodva lehet kialakítani.

A kockázatelemzés elméletileg nem bonyolult feladat, csak azt kell tudni az elektronikus adatkezelő rendszerrel kapcsolatban, hogy:

- milyen elemekből áll és milyen környezetben üzemel és ki, hogyan üzemelteti, használja;
- milyen (és milyen gyakoriságú) fenyegetéseknek van kitéve és a fenyegetéseknek milyen negatív hatása lehet;
- melyek a sebezhető pontok.

Az előbbiek alapján különböző módszertanok szerint *kimutatható a kockázat, meghatározható az a szint, ami alatt már nem szükséges védelmi rendszabályokat szervezni (vállalható kockázat; acceptable risk)*. A kockázatelemzés lényege az a felismerés, hogy jogszabályokban, NATO, EU direktívákban nem lehet minden üzemeltetési körülményt átfogó biztonsági követelményeket meghatározni. A másik kulcsfontosságú kérdés annak tudatosítása, hogy az elektronikus adatkezelő rendszerért felelős vezetőnek (vagy a jóváhagyásért, akkreditálásért felelős hatóságnak) *az elemzés alapján azonosítania kell azokat a kockázatokat, amelyeket tudatosan vállal.*

Az elektronikus adatkezelő rendszerek kockázatelemzésre irányuló támogatása érdekében figyelembe venni, hogy *a honvédelmi tárca nem rendelkezik egy fejezeti rendszernek tekinthető hálózattal*. Kockázatmenedzselés szempontjából transzporthálózat, helyi csatlakozó hálózat, illetve elkülönülten kialakított hálózat, vagy önálló eszköz kategóriákat kell megkülönböztetni, amelyek tartalmazzák a tábori eszközök, missziós rendszerek és a mobil eszközök kategóriáit is.

A honvédelmi tárcánál az elektronikus adatkezelő rendszerekkel kapcsolatos kockázatok menedzselése kézi, manuális módszerekkel nem végezhető el az alkalmazott adatkezelő képességek különbözősége, illetve a kialakuló központi infrastruktúrák bonyolultsága miatt, így napjainkban már nincs más lehetőség, mint a feladat szoftveres támogatása. A helyzetet nehezíti, hogy *hazánkban kormányzati ajánlás, vagy a közigazgatásra kifejlesztett szoftver nem áll rendelkezésre.* Ennél szélesebben fogalmazva az is megállapítható, hogy *még a minősített adatok védelme érdekében sincs meghatározva kötelező érvényű kockázatkezelési és menedzselési kötelezettség*.

A kockázatelemzés szoftveres támogatásához első lépésként szükség van az általános követelmények meghatározására, melynek fontosabb elemei az alábbiakban következnek:

A kockázatfelmérés végrehajtásához a védendő adatok, adatkezelő rendszerek, és elemek nyilvántartására rugalmasan bővíthető adatbázis álljon rendelkezésre. A fenyegetések és a sebezhetőségek nyilvántartására bővíthető, rugalmasan változtatható adatbázis szolgáljon.

A rendszerek adataihoz csatoltan és függetlenül legyen lehetőség a biztonsági incidensek és események kategorizált tárolására, valamint saját, kormányzati és NATO, EU ellenőrzési eredmények nyilvántartására.

A meglévő védelmi rendszabályok nyilvántartása során azonosítani kell a különböző nemzeti, nemzetközi szabványoknak, illetve NATO, EU követelményeknek való megfelelőséget. Az alkalmazásnak biztosítani kell, hogy *egy-egy rendszer esetében vizsgálható legyen a védelmi rendszabályok megfelelősége eltérő módszertanok szerint is.*

A kockázatelemzés végrehajtása során a kockázatok azonosításakor *a súlyozási szempontok, valamint a kockázatvállalási küszöbértékek rugalmasan változtathatók legyenek.* A vállalható kockázatok külön is exportálhatók legyenek.

A kockázatok menedzselése során *rögzíthetők legyenek a tervezett védelmi rendszabályok és modellezhető legyen, hogy azok alkalmazása milyen változásokat okoz az adott rendszer védelmében*.

Az elemzési folyamat során legyen lehetőség *az elvégzett és a soron következő feladatok nyomon követésére*. A kockázatfelmérés, elemzés és értékelés során a *rendszer tegye lehetővé a jegyzőkönyvek automatikus készítését*.

A kockázatfelmérés és elemzés, értékelés során *legyen lehetőség a feladatrendszer csökkentett mértékű elvégzésére is* (pl. rendszerelemre, vagy csak adott fenyegetésekre és sebezhetőségre vonatkozóan).

Távlatokban szükség van a kockázatelemző és értékelő feladatok kapcsán *a dinamikus fenyegetés és sebezhetőség elemzésben rejlő lehetőségek integrálására*:

- belső szkennelési lehetőségek, beleértve az eredmények azonnali megjelenítésének, kiértékelésének és dokumentálási lehetőségeivel (pl. tűzfalak, IDS/IPS rendszerek beállításai, portok ellenőrzése, operációs rendszer beállítások illetve kiemelt fontosságú szoftverek integritás ellenőrzése);
- külső szkennelési lehetőségek (hálózati eszközök beállításainak külső ellenőrzési lehetőségei).

Alapvető szükséglet a szoftvert alkalmazó személyek *hozzáférési rendjének szabályozása, valamint a kockázatmenedzsment feladatok végzéséhez szükséges képzési és gyakorlási lehetőségek biztosítása*.

Az interneten több kockázatelemző szoftver elérhető és ingyen letölthető, melyek tanulmányozása hasznos lehet, de egy biztos: mindennek ára van. Nagyobb adatbázisok feltöltése, vagy bonyolult műveletek megkezdése előtt célszerű az adatok menthetőségét, konvertálhatóságát ellenőrizni. Az esetlegesen használhatónak tűnő on-line megoldások alkalmazását a kockázatokkal kapcsolatos adatok bizalmassága (a gyakorlatban ez inkább minősítést jelent) gátolja.

3. TESZTELÉS ÉS ÓVATOSSÁG

Rengeteg történet szól arról, hogy minden másként történt volna, ha rendszeresítés, alkalmazásba vétel előtt megfelelő idő, pénz vagy egyéb erőforrás állt volna rendelkezésre az adott megoldás műszaki vagy felhasználói tesztelésére, vagy csak a feladat részletes kigondolására.

Amikor a honvédelmi szervezetek folyamatos időzavar mellett fejlesztés alatt álló rendszerekkel látják el feladataikat, vagy az elektronikus adatkezelő rendszerek, szolgáltatások egy része külső forrásból származik, súlyos veszélyek háríthatók el néhány alapvető, a tervezett változások tesztelésére, ellenőrzésére vonatkozó kérdéssel, mint:

- ki tesztelte az adott megoldást, és milyen eredményre jutott;
- az adott elektronikus adatkezelésre vonatkozó nemzeti vagy NATO, EU biztonsági követelmények az új változatnál is érvényesülnek;
- ki javította ki a hibákat, és mi alapján;
- ki engedélyezte a változást és mi alapján;

- milyen műszaki és kezelői dokumentáció áll rendelkezésre, illetve a változásokat, mely dokumentumokban kell átvezetni;
- az új megoldás bevezetése milyen felhasználói, kiszolgálói képzést, vagy erőforrásokat igényel?

Az ilyen kérdések segítik elkerülni azokat a helyzeteket, amikor telepített, beüzemelt rendszerben *utólag kell biztonsági beállításokat változtatni, vagy kiegészítő alkalmazásokat integrálni*.

Külföldi eszközök, termékek paramétereinek tanulmányozásakor ezért vessen fel kérdőjeleket a NATO kompatibilis biztonsági megoldásra való hivatkozás, kompromittáló kisugárzás elleni védelmi megfelelőség, vagy éppen egy ismeretlen nemzeti katonai szabvány NATO megfelelősége (főleg nem NATO tagállamban gyártott esetben).

Beszerzéskor, vagy beruházások tervezésekor nem minden esetben lehet a meglévő sablonok szerint gondolkozni, mert az említett jelenségek mellett jelentősen fejlődnek, alakulnak a szabványok, NATO, EU követelmények. Emiatt a „múltkor is így csináltuk", megoldás automatikus alkalmazását felül kell írni *a biztonsági szervezetekkel történő konzultációval*.

A rendszerbeállításhoz, meglévő rendszer átalakításához, eszköz változtatásához a szervezetre, az egyéb rendszerekre, környezetre gyakorolt hatások feltárása érdekében *az üzemeltetési környezetnek megfelelő teszt környezetet kell kialakítani* (minősítési szint, védelmi rendszabályok, üzemeltetési és ellenőrzési eljárások, szükséges mértékű kapacitás).

Üzemelő rendszer esetében a változtatások független környezetben történő tesztelését *az üzemelő infrastruktúrába történő migráció előtt kell végrehajtani*.

A tesztelést terv alapján kell végrehajtani. A teszt tervet a vonatkozó jogszabályok és technikai szabványok, valamint az alkalmazó honvédelmi szervezet belső rendelkezéseinek megfelelően kel kialakítani. A teszt tervben *meg kell határozni a végrehajtással kapcsolatos felelősségeket és feladatokat*, valamint a teszt indítási és befejezési kritériumait.

A teszt tervet az illetékes biztonsági akkreditáló hatósággal (jóváhagyó szervezettel) kell jóváhagyatni. A teszt tervet a következők szerint célszerű kialakítani:

1) A teszt *célja* (új hardver vagy szoftver elem vizsgálata, módosítás ellenőrzése).
2) A *teszt feladat* (teszt környezet, tesztelendő esetek és paraméterek, végrehajtási idő, a végrehajtáshoz szükséges támogató feladatok azonosítása), *a végrehajtására vonatkozó biztonsági követelmények* (hardver és szoftver konfiguráció, telepítési és biztonsági beállítások, végrehajtásért felelős személyek, általános és kiegészítő védelmi rendszabályok), a teszt kezdetéséhez és befejezéséhez szükséges *átállási és visszaállítási feladatok*, valamint a teszt közben bekövetkező *nem kívánt esetek megoldásához szükséges eljárások*.
3) A teszt által *igazolandó eredmények* (milyen paraméterek, jellemzők bizonyítják a tesztet hardver/szoftver elem alkalmazhatóságát, vagy támasztják alá a bevezetés elutasítását).

A végrehajtott tesztet *dokumentálni kell*, majd kiértékelés után az azonosított hibák kiküszöbölése érdekében kiegészítő tesztet (teszteket), vagy végső tesztet kell végrehajtani. *A sikeres további tesztek elvégzése után történhet meg a tervezett rendszerbeállítás vagy változás jóváhagyása*.

A rendszerbeállítás vagy a változtatás végrehajtására tervet kell készíteni, amelyben rögzíteni kell az érintett személyek és szervezetek feladatait, beleértve a felhasználók értesítésével és képzésével kapcsolatos teendőket is.

Amennyiben az átállás *szolgáltatás kieséssel vagy eltérő szolgáltatási szint biztosításával jár az összes érintett felet értesíteni kell*. Esetenként szükség lehet a régi és az új szolgáltatás párhuzamos üzemeltetésére, mely esetben rendszabályokat kell bevezetni a két üzemeltetés eredményeinek összehasonlíthatósága érdekében.

A rendszerbeállítás vagy a változtatás elvégzése után a felhasználói, üzemeltetői és biztonsági szempontok megfelelőségét ellenőrző *felülvizsgálatot kell tervezni és végrehajtani*. A felülvizsgálatnak ki kell mutatnia, hogy *a kitűzött célok megvalósultak-e, illetve milyen hiányosságok merültek fel*, a rendszerbeállítás vagy változtatás kapcsán melyek a hasznosítható tapasztalatok.

A fentiek mellett *az elektronikus adatkezelő rendszer életútja során különböző célú és tartalmú biztonsági teszt (security test) végrehajtása indokolt*, melyek részletezése meghaladja jelen cikk kereteit.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Napjainkban egyre több tanulmány, cikk foglalkozik a katonai elektronikus adatkezelés korszerű megoldásaival, az információbiztonsággal. Egy-egy műszaki megoldás vizsgálata mellett egyre több munka sürgeti a szabványosítást, illetve igényli a szabályozási rendszer korszerűsítését, az átlátható eljárásokat, tipizált megoldásokat.

Bizonyítást nem igénylő tény, hogy a felgyorsult technikai fejlődési ütem lehagyta a szabályozást. Ezzel párhuzamosan az utolsó időszak szervezési változásai *nem támogatták azon szakmai rétegek kialakulását, amelyek a katonai hierarchia szintjei szerint a napi élet rohanó tempójú végzése mellett* ellátnák az IT biztonsági feladatok előremutató keretrendszerű szabályozását, rendszer-specifikus szabályozási feladatokat látnak el, támogatják a fejlesztéseket, K + F célokat jelölnek ki, oktatnak, képeznek, egyszóval *lefedik az információbiztonság összes vetületét*.

A kiragadott életciklus feladatok részletezése, követelmények és eljárások formájában történő megfogalmazása és szabályzatokba történő integrálása jövőbeli feladat. Ennek során a honvédelmi tárcánál célszerű a NATO és EU szakmai politikák, direktívák és irányelvek, valamint nemzetközi szabványok minél szorosabb alkalmazása, mert a jogszabályok a választott témákban még feltűnően hiányosak. A vázolt területeken egyes katonai szervezeteknél már jó példákkal szolgáló gyakorlati lépések történtek, a ZMNE bázisán az elméleti alapozás kialakulása megkezdődött, a kockázatelemzésre vonatkozó szervezeti követelmény megfogalmazása megtörtént, ami a belátáson alapuló biztonság helyett a biztonság tudatos magatartás, a szakmai kultúra erősödését jelenti.

FELHASZNÁLT IRODALOM

[1.]MSZ ISO/IEC 27001:2006, Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények

[2.]27002 MSZ ISO/IEC 17799:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (MSZ ISO/IEC 27002)

[3.]Control Objectives for Information and related Technology (CobiT) 4.1.

[4.]ISO/IEC 20000 1-2:2007, Information technology - Service management

[5.]94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról