HADMÉRNÖK

VIII. Évfolyam 4. szám - 2013. december

Kassai Károly
karoly.kassai@hm.gov.hu

A 2013. ÉVI L. TÖRVÉNY VÉGREHAJTÁSA ÉRDEKÉBEN A MAGYAR HONVÉDSÉGNÉL SZÜKSÉGES ELEKTRONIKUS INFORMÁCIÓVÉDELMI SZAKFELADATOK

Absztrakt

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény ez évben – mint stratégiai szintű követelmény – új feladatokat határoz meg a Magyar Honvédség katonai szervezetei számára. Ez az első magyar hivatalos szabályzó, amely országos szinten határoz meg biztonsági követelményeket, a hálózati biztonságért felelős szervezeteket és koordinációért felelős tanácsot alapít, és alacsonyabb szintű követelmények meghatározását rendeli el a szükséges mértékű számítógép és hálózati biztonság érdekében. A közös gondolkodás, az elemzés és értelmezés, a felkészülés nélkülözhetetlen ebben a helyzetben a hatékony biztonsági menedzsment kialakítása érdekében. A cikk célja az új törvény alkalmazásának támogatása, a honvédelmi szervezetek biztonsági menedzsmentjeinek segítése az új követelmények megértése és a helyes prioritás meghatározása érdekében.

The Electronic Information Security of Governmental Organisations Act – as a strategic level requirement – created new tasks at military organisations of Hungarian Defence Forces in this year.This is the first Hungarian official regularization which decides country size framework for security requirements; establish responsible governmental organisations and coordination board for specific control functions about network security, and decides lower level requirements for the appropriate level computer and system security. The common thinking, analysis and explanation, preparation is necessary in this situation for creation of effective security management. The aim of this article to support the better implementation of the new Act, and help the security managements of military organisations to understand the new requirements and decide the right priority.

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

BEVEZETÉS

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban. Ibtv.) új helyzetet teremtett a közigazgatási szervezetek – ezen belül a Magyar Honvédség – számára.

A törvény megjelenése előtt nem volt érvényesíthető jogszabály, mely meghatározta volna az elektronikus adatok kezelésére vonatkozó biztonsági követelményeket és keretet biztosított volna a védelmi rendszabályok kialakítása és fenntartása érdekében. Egyedül a minősített adatkezelésre vonatkozó 2009-ben megjelenő törvény és a végrehajtását támogató kormányrendeletek azonosíthatók, mint részmegoldást célzó szabályozók.

A szerző korábbi cikke megfogalmazta az elektronikus információbiztonság megvalósításával kapcsolatos aktuális kérdéseket a Magyar Honvédségnél,1 melyhez csatlakozva jelen publikáció – mintegy folytatásként – az új jogszabály megjelenésével kapcsolatos teendőket körvonalazza.

AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER BIZTONSÁGÁÉRT VALÓ FELELŐSSÉG MEGHATÁROZÁSA

A felelősség kijelölésére vonatkozó követelmény a Magyar Honvédségnél összességében, vagy egy-egy honvédelmi szervezet esetében nem jelent ismeretlen feladatot. Az Ibtv. egyaránt vonatkozik a minősített és nem minősített elektronikus adatkezelő rendszerekre, szolgáltatásokra, így az elektronikus minősített adatkezelés biztonságára vonatkozó felelősség kijelölésére vonatkozó kötelezettség nem újdonság.

A nem minősített elektronikus adatok védelme esetében jogszabályban megfogalmazott általános követelmény eddig nem volt azonosítható, azonban a honvédség belső szabályozási rendje ezt a kérdést 1993-tól kezdve központi szabályzat formájában rendezte. [1]

A feladat végrehajtása lehetőséget teremt a honvédelmi szervezetek számára, hogy az információbiztonságért felelős menedzsmentet áttekintsék, és elvégezzék a lehetőségek szerinti egyszerűsítést, összevonásokat. Ez jelentheti minősített elektronikus adatkezelő rendszerek felelőseinek összevonását, de ugyanígy egy szervezetnél a feladatok értelmezése támogathatja a felismerést, hogy *a minősített és nem minősített elektronikus adatkezelésért való felelősségek összevonása logikus, erőforrást megtakarító lehetőség*.

A fejlődést mutatja, hogy a honvédelmi szervezeteknél alkalmazott megoldásoknál a felelős személyek kijelölésekor inkább szervezeti felépítés, elhelyezés és a működési sajátosságok figyelembe vétele kezd előtérbe kerülni a hagyományos megközelítés (minősített – nem minősített adatkezelés elkülönítése) helyett.

Az általános vezetői felelősség azonosításánál a minősített adatkezelést felügyelő biztonsági vezető hatáskörének kiterjesztése látszik a legjobb megoldásnak, de csak azzal a kiegészítéssel, hogy ezt a vezetői feladatot nem szabad a végrehajtói feladatokkal összemosni (rendszerbiztonsági felelősi feladatokkal, vagy egyéb megnevezésű, a képességek védelmi rendszabályaiért felelős személyek felelősségével).

INFORMÁCIÓ BIZTONSÁGPOLITIKA KIALAKÍTÁSA

A kormányzati ellenőrzést végző szervezetek megállapításain, és a szakmai politika meghatározására vonatkozó ajánlásokon kívül az Ibtv. hatálybalépését megelőzően jogszabályban e területű követelmény nem azonosítható. A 2009-es honvédelmi tárca

[1] Az elektronikus információvédelem napjainkban aktuális kérdései a Magyar Honvédségnél; HADMÉRNÖK, VIII. Évfolyam 2. szám - 2013. június, p. 345-357.

információbiztonsági politikája[2] ennek megfelelően a szakirodalom ajánlásai és a honvédség gyakorlati tapasztalatai és igényei szerint alakult ki.

Az Ibtv. a stratégiai szintű dokumentumra vonatkozó követelmény meghatározásán kívül *formai és tartalmi követelményeket nem határoz meg*. Az elektronikus információbiztonságra vonatkozó, átfogó jellegű Nemzeti Kiberbiztonsági Stratégia[3] sem határoz meg a végrehajtáshoz támpontot adó részleteket, így *kijelenthető, hogy jelenleg nem azonosítható a közigazgatásra vonatkozó központi szakmai követelmény*, ami egyrészt meghatározná az ágazatokra vonatkozó követelményeket, másrészt egységes közigazgatási szintű szempontrendszert határozna meg.

A honvédelmi tárca információbiztonsági politikáját e tények figyelembe vételével kell felülvizsgálni és ismételten kiadni. A legelső eldöntendő kérdés a politika témája körül adódik, mert el kell dönteni, hogy szűkíteni kell-e a tartalmat elektronikus információbiztonságra vagy jelenlegi formájában – szélesebb értelmezéssel, információbiztonsági tartalommal – kell továbbra is menedzselni. A kérdés eldöntése nem csak elektronikus információbiztonsági kérdés, szakterületi konszenzuson alapuló döntést igényel, de *az elektronikus adatkezelés több szempontú biztonsági követelményei vélhetően a közös megfogalmazás melletti súlyos érvként értékelhető*. A lényegi kérdéseket tekintve az információbiztonsági politika változtatásával kapcsolatban – a részletesség igénye nélkül – a következő szempontok mérlegelése célszerű.

A biztonsági célok pontosítása. A jelenlegi szabályozás az aktuális helyzetnek megfelelően *a bizalmasság, sértetlenség és rendelkezésre állás hármasát határozza meg biztonsági célként*.[4] A szakterületi nemzetközi szabvány e mellett ajánlást tesz egyéb tulajdonság célként történő meghatározására, mint *hitelesség, számonkérhetőség, letagadhatatlanság vagy megbízhatóság*. [3] A közigazgatásban több követelmény fogalmazza meg az *azonosítást* (mint kiemelt szintű célkitűzést), valamint a *letagadhatatlanságot* és elektronikus hitelesítés szolgáltatást rendelnek bizonyos közfeladatok teljesítéséhez. Ezek alapján nyilvánvaló, hogy a Magyar Honvédség esetében is a jelenlegi helyzetnek megfelelően *meg kell fontolni a biztonsági célok kiterjesztését*, még akkor is, ha az új követelmények csak meghatározott területekre, elektronikus adatkezelő szolgáltatásra értendők és nem általánosan érvényesítendők.

A biztonsági osztályok módosítása. Az Ibtv. központi követelményeket határozott meg a biztonsági osztályok kialakítására, ami alapján szükségessé válik a Magyar Honvédségnél alkalmazott rendszer módosítása.[5] A törvény által meghatározott követelmény, hogy a bizalmasság, sértetlenség és rendelkezésre állás szempontjait külön-külön figyelembe kell venni a biztonsági osztályok kialakításakor,[6] és a besoroláshoz ötös skálát kell alkalmazni.[7] A biztonsági osztályba sorolás alapja a kockázatelemzés, melyre vonatkozóan a jogszabály sem formai, sem tartalmi követelményeket nem határoz meg az alkalmazó szervezetek számára. E mellett figyelembe kell venni, hogy a biztonsági osztályba sorolás az adott rendszerért felelős vezető hatáskörébe tartozik, aki a végrehajtási rendeletben megjelenő követelményektől a besoroláskor fölfelé és lefelé is eltérhet.

A biztonsági osztályok szerinti védelmi rendszabályokat a végrehajtásra vonatkozó rendeletekben megfogalmazottak alapján kell kialakítani, ami minősített adatok esetén a már rendelkezésre álló kormányrendeletek alkalmazását jelenti.

---

[2] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról.

[3] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

[4] Ez a 2009-es megfogalmazás összhangban van az Ibtv. követelményeivel. [2]

[5] A cikk írásakor az Ibtv. végrehajtását támogató, 2013. július elsejéig kiadásra tervezett végrehajtási rendelet még nem ismert, így e területen végleges információk publikálására nincs lehetőség.

[6] A követelmény értelmezésekor nem szabad figyelmen kívül hagyni, hogy a jogszabály a minősített és a nem minősített adatokra egyaránt vonatkozik.

[7] Az ötös skála meghatározása azért kihívás az alkalmazó szervezet számára, mert a közigazgatásra jellemző minősített adatkezelés ezen a skálán négyet automatikusan elfoglal, így a nem minősített adatok biztonságához szükséges védelmi rendszabályokat egy osztályon belül kell megvalósítani.

Szervezeti biztonsági szint meghatározása. Az Ibtv. ezen a területen eddig a közigazgatásban még nem létező kötelezettséget állapít meg. Az alkalmazó szervezeteknek *a biztonsági osztályokhoz kötötten meg kell határozniuk saját szervezeti biztonsági szintjüket*, majd a biztonsági szintre vonatkozó védelmi rendszabályokat kell érvényesíteni a honvédelmi szervezetnél. A besorolás elvégzésekor az előbb ismertetettek szerint eltérést alkalmazhatnak. Ugyanakkor ezzel párhuzamos követelmény, hogy a honvédelmi szervezeteket a törvényben meghatározott követelmény szerint négyes biztonsági szintbe kell sorolni, ami szakmai kihívásokat jelenthet a honvédelmi szervezetek mérlegelési felelősségét illetően.

A besorolásnál *azokat a tényezőket kell figyelembe venni, melyek hatással vannak az adott elektronikus adatkezelő rendszer biztonságára* (pl. egy szolgáltatásokat alkalmazó szervezet esetében nem lehet értelmezni az üzemeltetésre vonatkozó szabályozás kötelezettséget, a minimális rendelkezésre álláshoz szükséges folytonossági tervezési feladatokat, vagy a rendszerek tervezésére, auditálására vagy akkreditálására vonatkozó követelményeket).

A felelősségi rend aktualizálása. A Magyar Honvédségnél a jogszabályokban megfogalmazott elektronikus információbiztonsággal kapcsolatos követelmények végrehajtása centralizáltan történik. Ennek értelmében a Központi Rejtjelfelügyelet, a Központi Rendszerbiztonsági Felügyelet és az elektronikus információs rendszerek biztonsági felügyelete funkciókat egységesen, közös szakmai felügyeleti rendben kell elképzelni. Az általános követelményeket e területen az Ibtv-ben meghatározottak szerint kell pontosítani. Célszerű annak vizsgálata is, hogy NATO minősített adatkezelés szempontjából kulcsfontosságú Központi Nyilvántartó (Central Registry), és a Központi Rejtjel Elosztó (National Distribution Authority) feladatait szükséges-e – és milyen mélységig – rögzíteni ezen a szabályozási szinten. Az incidenskezelés, illetve az ehhez szükséges külső szervezeti kapcsolattartás szervezettségéhez szükség van az ágazati léptékű összehangolásra vonatkozó követelmény meghatározására. Az Ibtv. követelménye szerint a honvédelmi miniszter rendeletben határozta meg a HM Védelmi Hivatal, a Katonai Nemzetbiztonsági Szolgálat és a Magyar Honvédség (benne a Honvédelmi Minisztérium) együttműködését és a felügyeleti rendet. [4] Ezt a struktúrát át kell vezetni a politika felelősségi rendjén is, valamint ki kell egészíteni a végrehajtáshoz szükséges követelményekkel és feladatokkal.

A szabályozási rend pontosítása. A jogszabály megjelenése lényeges változásokat okoz. Ennek legfontosabb eleme, hogy a 2013. évhez köthetően megjelent az alkalmazó szervezetek számára egy megkerülhetetlen követelmény: szabályozni kell az elektronikus információbiztonsági kérdéseket! A jelentőséget azért kell kiemelni, mert a honvédelmi szervezeteknél eddig is volt hasonló szerepű szabályozó, de a központi ellenőrzési szervezetek (egymáshoz képest eltérő) szabványokon alapuló ellenőrzéseiből adódó ajánlásokon és követelménytámasztásokon kívül[8] egységes közigazgatásban értelmezhető követelmény nem állt rendelkezésre. A már említett 1993-as belső szabályozásban meghatározott követelmények végrehajtására vonatkozóan szabvány alapú központi szabályozó jelent meg 2012-ben,[9] így az Ibtv. végrehajtása ezen a területen nem jelenthet nehézséget.

Elektronikus információbiztonsági területen a 2012-es szabályozó a védelmi rendszabályok strukturált meghatározását rendelte el, ami szervezetek közötti, illetve szervezeteken belüli feladatmegosztást, „profiltisztítást" is eredményez, mely feladatot a szakmai politikában is át kell vezetni. A lényeg, hogy hálózati szinten el kell különíteni az architektúrából adódó feladatokat, mint központi területi és helyi üzemeltetési és elektronikus információvédelmi

[8] Az említett helyzet az ellenőrzések lényegét világítja meg: kötelező jellegű követelmény nélkül hogyan lehet védelmi rendszabályokról, kontrollokról – vagy azok hiányáról – megállapításokat tenni, és követelményeket megfogalmazni?

[9] 3/2012. (I. 13.) HM utasítás a honvédelmi tárca általános elektronikus információbiztonsági követelményeinek meghatározásáról és a védelmi rendszabályok pontosításáról.

feladatok, valamint egy-egy honvédelmi szervezetnél a felhasználói és üzemeltetési elektronikus információvédelmi feladatokat.

A szabályozási rend pontosítását a rejtjelzés területén is értelmezni kell. A Magyar Honvédséghez hasonló strukturált szervezetnél, ahol a honvédelmi szervezetek tevékenysége között lényeges különbségek vannak, be kell látni, hogy egyszintű szabályozással nem lehet a szakterületi kérdéseket rendezni (egy szabályzatban nem lehet minden szervezetre érvényes módon meghatározni a rejtjeltevékenység összes eljárását és követelményét). E miatt a politika rejtjelzésre vonatkozó szabályozási követelményét is pontosítani kell, és *a Magyar Honvédségnél be kell vezetni a többszintű szabályozást*.

A belátás alapú javaslat a központi követelmények, eljárásrend és a helyi szabályozásra vonatkozó strukturálást jelenti. Első lépésként az MH Rejtjelszabályzat – mint központi követelmény – kiadása szükséges, megalapozva a központilag megfogalmazandó, alacsonyabb szintű szabályozás körébe tartozó rejtjelző szakiratkezelésre, az incidenskezelésre és az ellenőrzésre vonatkozó szakutasítás kiadását. Új központi követelmény, hogy *az alkalmazó honvédelmi szervezeteknek helyi rejtjelszabályzatot kell kiadni*, melyben részletesen szabályozni kell a helyi rejtjeltevékenységet. Az új szabályozási feladat megvalósítását az első időszakban biztos, hogy számtalan nehézség fogja gátolni, így *a szabályozásért felelős minisztériumi szervnek gondoskodnia kell az alárendelt honvédelmi szervezetek szakmai tevékenységének támogatásáról*. A szakmai segítség lehet kiadott segédlet, szabályzatminta, központilag megszervezett és biztosított tanfolyam, konzultációs lehetőség – „help desk" szolgáltatás, mely rendszerben *kiemelt helye és szerepe lesz a középszintű vezető szerv szakmai szervének az alárendelt honvédelmi szervezetek támogatása érdekében*. A szakmai értékek egyik legfontosabb jellemzője az adott szakterületre vonatkozó logikusan felépített, a kor színvonalán álló terminológiai keretrendszer kialakítása és folyamatos pontosítása, mely megállapítás a rejtjelzés szakterületére is érvényes kell, hogy legyen, így az előbbiek mellett kezelni kell *a szakkifejezések tisztázásának és rögzítésének ügyét is*.

AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI STRATÉGIA

A fejlesztésre vonatkozó feladatok meghatározásához szükséges stratégia kialakításra vonatkozó követelményt informatikai területen 2005-ben jogszabály rögzítette, majd ez követelmény 2010-ben hatályát vesztette.[10] Az Ibtv. megjelenésével ismét megjelent a szakterületi stratégia kialakításával kapcsolatos követelmény, kifejezetten az elektronikus információ biztonsági területre címezve.

A Stratégia kialakításához hasznos támpontot ad a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának megjelenése.[11] A koncepció kialakítása a stratégiai szintű dokumentumok sajátosságainak megfelelően történt – és azon kívül, hogy megfogalmazza a szakmai célkitűzéseket – támpontot ad a Stratégia kötelező elemeinek kialakításához is (jelenlegi helyzet, stratégiai környezet, logikai kapcsolatok, alapvető kockázatok, a kialakításra vonatkozó elgondolás).

A korábban idézett felügyeleti és ellenőrzési rendről szóló honvédelmi miniszteri rendelet a stratégiai szintű szabályozás területén a hálózatgazdák kezébe adja a dokumentumok kialakításának felelősségét (miniszteri jóváhagyási kötelezettség mellett), ami lehetőséget teremt a rendszer-specifikus jellemzők figyelembe vételére. [4.] A rendszerek jellemzőinek eltérősége, a kezelt adatok sajátossága közös alapokra épül, így nyilvánvaló, hogy a biztonsági környezet, az információs fenyegetések a sebezhetőség, a kockázatok kimutatása, a stratégiai célkitűzések meghatározása, a tervezési folyamat megalapozása nagyrészt azonos adatokból áll. Az elkülönült rendszer-specifikus kidolgozást segítheti a közös megalapozás és

[10] 44/2005. (III. 11.) kormányrendelet a kormányzati informatika koordinációjáról és a kapcsolódó eljárási rendről.
[11] 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról.

helyzetértékelés, így nyilvánvaló lehetőség annak vizsgálata, hogy a stratégiák megalapozhatók-e a felügyeletek által közösen menedzselve.

A jogszabály formai, vagy tartalmi követelményt nem határoz meg, így a stratégiai szintű szabályozásra vonatkozó általános követelmények szerint kell az alkalmazó szervezeteknek eljárnia, és az „intézményi stratégia" kialakítására vonatkozó általános feladatokat kell figyelembe venni, kiegészítve a honvédelmi sajátosságokból adódó eltérésekkel. Lényegi elemek [5.]:

- az intézményi stratégiában a középtávú működési és fejlesztési célok meghatározása, az azok eléréséhez szükséges feladatok, beleértve a hierarchia szerinti elkülöníthető szervezetek céljait is;
- a célok eléréséhez szükséges célterületek és eszközök azonosítása;
- az erőforrások meghatározása és ütemezése;
- a nyomon követésre vonatkozó követelmények.

A hivatkozott stratégiai irányításra vonatkozó jogszabály a nyomon követéssel kapcsolatban részletesebben fogalmaz, ami jelzi, hogy a meghatározott tevékenység a vezetői tájékoztatás érdekében nem önmagában a Stratégia, hanem a stratégia hatálya alátartozó képesség felügyeletére irányul, így a mérőpontokat és jelentéseket úgy kell megtervezni, hogy *a Magyar Honvédség szintű védelmi képességek alakulásáról valóban reális képet lehessen alkotni* a „végrehajtás az erőforrásokkal arányos Főnök!" típusú, valósághű, bár kevésbé tartalmas jelentés helyett.

FELÜGYELETI SZAKFELADATOK

Az eddigiek szemléletesen ábrázolják a honvédelmi szervezetekre váró szakmai kihívás összetettségét. A helyzet megoldásához szükség van a végrehajtás központi támogatására egyrészt a bonyolultság, másrészt a hálózatos gondolkodás, *a Magyar Honvédség egészére kötelező érvényű azonos biztonsági szintek szerinti gondolkodás megvalósítása érdekében*. Az előre látható legfontosabb feladatok a következőkben foglalható össze röviden.

Az elektronikus információs rendszerei védelmének felelőseire, feladataira, a felhasználókra vonatkozó szabályokat tartalmazó Elektronikus Információbiztonsági Szabályzatok kiadásával kapcsolatos feladatok irányítása. A helyi vagy rendszer-specifikus szabályozás vezérlésére megjelenő végrehajtási rendelet várhatóan összetett védelmi rendszabályokat megfogalmazó jogszabály lesz. Ennek megfelelően célszerű a szabályozók kiadásának központi támogatása annak érdekében, hogy *a honvédelmi szervezeteknél egységes szemlélet szerinti védelmi rendszabály halmaz alakuljon ki*.

A felhasználói és üzemeltetői – biztonsági szakfeladatok elkülönítése mellett figyelmet kell szentelni a tábori jellegű híradó - informatikai rendszerek védelmére, a különböző biztonsági tartomány szerinti rendszerek összekapcsolására (pl. tábori rendszer és stratégiai rendszer összekapcsolása).

A helyi szaktevékenység támogatásának fő területei a jogszabályban meghatározott feladatok honvédségi szempontú értelmezése, a kockázatelemzés és kezelés, a biztonsági osztályba sorolás és a szervezeti biztonsági szint meghatározás támogatása – beleértve a hiányosságok felszámolása érdekében szükséges felszámolási terv készítés irányítását, az eltérésekre és helyettesítő rendszabályokra vonatkozó iránymutatás és segítségnyújtás. E területen további részletes feladatok nem határozhatók meg, de a feladatok összetettsége egyértelművé teszi, hogy a képzés, az elektronikus kommunikáció legjobban megfelelő formáit kell alkalmazni a határidőben történő – és a honvédelmi érdekeknek is megfelelő – végrehajtás érdekében.

Éves ellenőrzési terv készítése és jóváhagyatása a Hálózatgazdával. Az Ibtv. az alkalmazó szervezetek biztonságával kapcsolatos helyzetismeret (security awareness) érdekében tervezett

ellenőrzési tevékenységet határoz meg. Az ellenőrzési tevékenység az elektronikus információbiztonsággal foglalkozók számára eddig sem volt ismeretlen feladat, e területen újdonságot csak a végrehajtási rendelet fog jelenteni, ami a tervek szerint meghatározza az alkalmazandó védelmi rendszabályokat. Az ellenőrzési tevékenység tervezése, illetve tágabban értelmezve az ellenőrzések által biztosított adatok hasznosítása érdekében meghatározható néhány minimum követelmény:

- az elektronikus információvédelmi szakellenőrzéseket a honvédség ellenőrzési rendjébe integráltan kell kialakítani;
- az erőforrások takarékos felhasználása érdekében össze kell fogni az ellenőrzési tevékenységeket, mint minősített adatokra irányuló hatósági ellenőrzést – visszaellenőrzést – akkreditálást – újra-akkreditálást, és egyéb, az Ibtv. által meghatározott nem minősített elektronikus adatkezelésre vonatkozó ellenőrzéseket;
- az előző pont kiegészítéseként pontosítani kell az ellenőrzési rendszert, és az új követelmények szerint kategorizálni kell, hogy mi a feladata a helyi, az elöljárói (több szintre bontva) és egyéb ellenőrzéseknek, ami megalapozza, hogy egy hatósági ellenőrzéskor ne legyen egyaránt lekötve a helyi biztonsági menedzsment, a középszintű vezető szerv és a szakmai feladatokért felelős felső szintű szerv szakmai képviselete;
- meg kell tervezni és ki kell alakítani az ellenőrzési feladatok támogatását, hálózati eszközökkel történő végrehajtását, és
- korszerű elvek szerint kialakított tudásbázist kell kialakítani az ellenőrzések során szervezett tapasztalatok visszakereshetősége, hasznosítása érdekében.

Az elektronikus információs rendszerekre irányuló ellenőrzési tevékenységbe bele kell érteni a *honvédelmi szervezetek biztonsági osztályba sorolására és a szervezetek biztonsági szintjére vonatkozó követelmények teljesülésének ellenőrzését*, a szabályzatokba történő megjelenítést és a *feltárt elmaradás felszámolásához szükséges cselekvési tervek készítésének és végrehajtásának ellenőrzését*, illetve a *kockázatelemzés és kezelés feladatainak ellenőrzését* is. Az elektronikus információs rendszerek biztonsági megfelelőségét az ellenőrzésen kívül a kockázatelemzés és kezelés, valamint az auditálás, akkreditálás és egyéb területtű technikai ellenőrzések is hatékonyan támogatják, így a rendszerek sajátosságait figyelembe véve szükség van ezen erőforrások igénybevételére is.

A képzés és továbbképzés biztosítása. Az át- és továbbképzések rendje szerint a Magyar Honvédségnél elektronikus információbiztonsági területen a tanfolyamjellegű képzésnek hagyományai vannak. A kezdetben kizárólag a NATO elektronikus információbiztonsági ismeretek átadása a híradó-informatikai rendszerek fejlődéséhez igazodva lépésről lépésre továbbfejlődött. A tanfolyamjellegű képzés érvényes a rejtjelző szakismeretek oktatására is, rejtjelző alaptanfolyam és a rejtjelző eszközkezelő tanfolyamok formájában. A rejtjelző szakiratkezetésre vonatkozó jogszabályi követelmények miatt megjelent a titkos ügykezelői (TÜK) szaktudásra vonatkozó igény, így az ügyviteli állomány képzését szolgáló tanfolyami rendszerhez csatlakozva történik a szükséges rejtjelző szakállomány TÜK képzése. A tanfolyam jellegű képzés aktuális feladata a tematikák aktualizálása és gyakorlati tapasztalatok beépítése a tanfolyamokba. Rejtjelzés területén a 2014. évben várható két hullámban megjelenő szabályozók kapcsán szükség lesz az alaptanfolyami rendszer változtatására és a kezelhető méretű tanfolyamok érdekében valószínűsíthető a logikai részekre tagolt, egymásra épülő tanfolyami rend megjelenése.

Az éves továbbképzések az elektronikus információvédelmi – benne a rejtjelző – szakállománynak nem jelentenek újdonságot. Ezen a területen szükség van annak jelzésére, hogy a változásokat, tendenciákat és várható feladatokat ismertető, az ellenőrzési és egyéb tapasztalatokat bemutató képzési forma *ismeret kiegészítésre és várható feladatokra történő felkészítésre szolgál, és nem pótolhatja a tanfolyamokon megszerzett alapvető ismereteket*

(tudatos vezetői tervezőmunkával kerülni kell a „menjen el és jelentse mi volt ott” címszóval történő felesleges delegálást). A továbbképzési rendszerben *szinergikus hatás érhető el a központi továbbképzés és a középszintű vezető szerv továbbképzésének összehangolásával* (egymásra épülés, ismétlődések elkerülése), mely területen szintén lépések várhatók.

A képzés területén a Magyar Honvédség belső képzési rendje mellett új feladatként jelentkezik az Ibtv. képzésre vonatkozó követelménye, így az érintett állománynak a Nemzeti Közszolgálati Egyetemen szervezett *vezetői és végrehajtói szintű elektronikus információbiztonsági képzéseket, továbbképzéseket és éves továbbképzéseket* is végre kell hajtani, figyelembe véve a törvény által biztosított könnyítést (meglévő gyakorlati tapasztalatok miatti mentesítés) is. [6.]

A felügyeleti szakfeladatok között meg kell említeni három, egymással is összefüggésben lévő feladatot:

- *az elektronikus információs rendszer eseményeinek nyomon követhetőségének és a biztonsági eseményre történő gyors és hatékony reagálás-, az azt követő biztonsági esemény kezelésének biztosítása;*
- *a biztonsági eseményekről és fenyegetettségről az érintettek tájékoztatása;*
- *együttműködés és kapcsolattartás* a kormányzati eseménykezelő központtal, az ágazati eseménykezelési központokkal, a kormányzati incidens-kezelési munkacsoporttal, a hatósággal, a szakhatósággal és a felügyeletekkel és üzemeltető szervezetekkel, más szakmailag szükséges partnerekkel.

A feladatkör jól érzékelteti, hogy nyilvánvalóan hálózati szintű megoldásokról van szó, melyek felügyeleti, strukturált végrehajtói, információbiztonsági és egyéb, esetenként előre nem is azonosítható feladatok halmazát jelenti. A végrehajtásban érintett a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózat üzemeltetésében és védelmi feladataiban érintett állomány.

A feladat bonyolultságát jelzi, hogy a Magyar Honvédség vezetési és irányítási képességei az említett központi felügyelet alatt álló Hálózat szolgáltatásait kiegészítik a felcsatlakozó hálózatok, illetve az önmagában is tagolt MH tábori hírrendszer, valamint az önálló telepítésű elektronikus adatkezelő rendszerek, melyek csak adathordozón keresztüli adatcserével (off-line) csatlakoznak a vezetési rendszerekhez. [7] A honvédelmi szervezetek működését támogató eseménykezelő képesség megköveteli a Kormányzati Eseménykezelő Központtal való szoros együttműködést, valamint a közigazgatás működéséhez szükséges műveletekben való részvételt. [8]

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Az elektronikus információbiztonsági kérdések szabályozási kötelezettsége a Magyar Honvédségnél nem jelent ismeretlen feladatot. Az Ibtv. és a cikk írásakor még kiadás előtt álló végrehajtási rendelet új szabályozási környezetet teremt, ami *megköveteli a helyzet értelmezését és a soros feladatok meghatározását*.

A cikk bemutatja az új jogszabályokban megfogalmazott követelményeket, és a rájuk adandó válaszokat. Látható, hogy *a feladatok egyrészt már meglévő szabályozók felülvizsgálatát és a változások átvezetését igénylik*, míg más esetekben *új területeken kell feladatokat körvonalazni, célokat kijelölni és a megoldáshoz szükséges alternatívákat, erőforrásigényeket megfogalmazni*.

A kockázatelemzésre és kezelésre alapozott biztonsági osztályba sorolás és szervezeti biztonsági szint meghatározás követelménye önmagában nem okoz megoldhatatlan feladatot. E területen a kihívás a kiadás előtt álló végrehajtási rendeletben *központilag megfogalmazott védelmi rendszabályok, kontrollok adoptálása, illetve a katonai sajátosságok szerinti eltérések, helyettesítő rendszabályok megfogalmazása és alkalmazása* lesz.

A katonai képességek működése során a minősített adatkezelés a közigazgatás átlagos szintjénél magasabb arányú, illetve az együttműködési feladatok külföldi minősített elektronikus adatok biztonságának garantálását is szükségessé teszik. E területen *kihívást a nem minősített és a minősített adatok egységes kezelése, az adminisztrációs feladatok csökkentése jelent*, ami a gyakorlatban azt jelenti, hogy *két, eltérő logika szerint felépített jogszabály követelményeit kell végrehajtó szinten egységesen kezelni*.

A Magyar Honvédség esetében a szövetségi műveletek jellegéből adódik az a sajátosság is, hogy egy-egy adat esetében a körülmények változása meghozhatja azt a döntést, hogy az adatot be kell vonni a minősített adatok körébe (ami más biztonságú információs környezetet igényel), valamint nemzeti adatról is ugyanígy kiderülhet, hogy együttműködő partner számára át kell adni, ami kiegészítő adatkezelési, illetve hálózati szintű műveleteket igényel.

A jogszabályokban megfogalmazott követelmények eltérhetnek az üzemeltetett híradó-informatikai rendszerek jelenlegi rendszabályaitól, így soros feladatként kell tekinteni a rendelkezésre álló jogszabályok – mint követelmény – és a rendelkezésre álló védelmi rendszabályok összehasonlítását, és a katonai sajátosságok miatti eltérések meghatározása mellett cselekvési terveket kell kidolgozni a megfelelőség érdekében.

Az Ibtv. a rejtjelzésre vonatkozóan nem határoz meg követelményeket, de a Magyar Honvédségnél folyamatban lévő szabályozási lépések végrehajtása során kiemelt figyelemmel kell kezelni a rejtjelzéssel kapcsolatos követelményrendszer kiemelt fontosságát, a feladatok bonyolultságát, és a bizalmassággal kapcsolatos specialitásokat.

Az elektronikus információ biztonság szakterületén stratégia készítésre vonatkozó követelmény eddig nem volt azonosítható, így a miniszteri jóváhagyással kiadott Magyar Honvédség Kibervédelmi Szakmai Koncepció alapján kialakítandó szakmai stratégia új feladatot jelent a szakterület számára.

Összegzésként megállapítható, hogy az Ibtv. szempontrendszere a honvédelmi szervezetek működéséhez szükséges elektronikus információvédelmi szaktevékenységére pozitívan fog hatni, annak ellenére, hogy a bonyolultnak tűnő helyzetben meglévő védelmi rendszabályok, követelmények pontosítására is szükség lesz a kifejezetten új feladatok megoldása mellett, illetve szükség lesz a feladatokkal járó többlet erőforrásigény kezelésére is.

Felhasznált irodalom

[1] A Magyar Honvédség Informatikai Szabályzata, Ált/210, 1993. p. 197. p.

[2] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 1. § 15. pont és 5. §.

[3] MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények, 3.4. pont.

[4] 16/2013. (VIII. 30.) HM rendelet a Magyar Honvédség, a Katonai Nemzetbiztonsági Szolgálat, a Honvédelmi Tanács és a Kormány speciális működését támogató elektronikus infokommunikációs rendszerek biztonságának felügyeletéről és ellenőrzéséről, 2. §. (2-4), 3. §.

[5] 38/2012. (III. 12.) Korm. rendelet a kormányzati stratégiai irányításról, 37. §.

[6] 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról; 4.§ - 18. §

[7] 55/2013. (ix. 13.) HM utasítás a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának békeidejű üzemeltetési és felügyeleti rendjéről, valamint az alapvető szolgáltatások biztosításának és igénybevételének szabályairól; 3. §

[8] 233/2013. (VI. 30.) Korm. rendelet az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről, 2. §. (2)