HADMÉRNÖK

VII. Évfolyam 3. szám - 2012. szeptember

Kassai Károly
kassai.karoly@hm.gov.hu

A KATONAI KOMMUNIKÁCIÓS KÉPESSÉGEK REJTJELZÉSSEL TÖRTÉNŐ VÉDELMÉNEK FONTOSABB KÉRDÉSEI

Absztrakt

Az elektronikus adatkezelés napjainkban egyre fontosabbá, nélkülözhetetlenné válik, beleértve az ezzel kapcsolatos problémák kezelését is.
A minősített adatkezelésre vonatkozó követelmények – és kapcsolódó problémák – a napi életben alig ismertek, beleértve a bonyolultnak tekinthető minősített elektronikus adatkezelésre vonatkozó szabályokat.
Hazánkban a 2010-es év jelentős változásokat hozott a minősített adatkezelés területén, benne a rejtjelzésre és a kapcsolódó támogatásra vonatkozó követelményekben, illetve az általános biztonsági követelmények területén.
Jelen cikk a jogszabályok végrehajtása érdekében a rejtjezésre, és annak támogatására vonatkozó szabályozás kérdéseit vizsgálja, figyelembe véve a katonai vezetés és irányítás sajátosságait.

The electronic information handling a more important these days, it becomes essential, including the related problems to be managed.
The requirement of classified information handling - and related problems – in daily life is a little known including the more difficult electronic classified information handling.
In our country, the year 2010 brought significant changes to the classified information management, including the requirement of encryption, the related supporting activities of encryption, and general crypto security requirements.
This article describes the implementation of legislation in the field of general regulation of the military command and communication.

Kulcsszavak: *információbiztonság, információvédelem, minősített adatkezelés, rejtjelzés ~ information security, information protection, classified information protection, encryption.*

BEVEZETÉS

A minősített adatok védelme hazánkban törvény által meghatározott követelmények szerint történik. Az elektronikus adatkezelés – mint speciális adatkezelés – védelme egyes esetekben rejtjelzéssel történő védelmet határoz meg, melyre vonatkozó általános követelmények jogszabályban rögzítettek.

A jogszabály meghatározza a rejtjelzéssel kapcsolatos szaktevékenységre vonatkozó kereteket és általános követelményeket, ugyanakkor nem részletezi a rejtjelzéssel, rejtjeltevékenységgel kapcsolatos szabályozásra vonatkozó követelményeket.

A rejtjelzéssel történő védelem szabályozása kulcsfontosságú kérdés, mert technikai jellegű folyamatok – melyek biztonsága kiemelt fontosságú – működése a részfeladatok, műveletek összehangolása nélkül elképzelhetetlen.

1994 - 2010. között az akkor érvényes jogszabály a rejtjelzésre vonatkozó szabályzat tartalmára vonatkozóan követelményeket határoz meg néhány területen: a rejtjelfelügyelet hatáskörének, szervezeti és működési rendjének és feladatainak meghatározása, a betekintési engedély nélküli megismerésre jogosult vezetők meghatározása, a különleges biztonsági követelmények meghatározása, a nyilvántartás és ügyvitel kérdéseinek szabályozása, a rejtjelzés területén ellenőrzésre jogosultak köre. E mellett a kormányrendelet meghatározza, hogy a szabályzatban rögzíteni kell a „rendeletben meghatározott egyéb kérdéseket”, illetve a szabályzat kiadásához az illetékes hatóság (Országos Rejtjelfelügyelet) előzetes egyetértése szükséges. 0

A jogszabályokban lényeges változás történt 2009-2010-ben, ami a rejtjelzés szakterületét is érintette. Hazánkban egységessé vált a kormányzati felügyeleti rend, közös jogszabály rögzíti az elektronikus információbiztonsági és a rejtjelző kérdéseket. Az új kormányrendelet meghatározza a rejtjelszabályzat fogalmát, mint a rejtjeltevékenység általános szabályozását és a szállítás, tárolás követelményeit (mert a kormányrendelet nem sorolja a rejtjeltevékenység körébe a szállítást és a tárolást) meghatározó belső rendelkezés. Rögzíti, hogy a szervezet vezetője adja ki a szabályzatot, meghatározza a szakterületre vonatkozó belső ellenőrzésére vonatkozó szabályozási kötelezettségét, illetve az előző megfogalmazás szerint meghatározza a rejtjelfelügyelet hatáskörére, feladataira vonatkozó szabályozási kötelezettséget és a hatósági egyetértésre történő benyújtás kötelezettségét. **Error! Reference source not found.**

Összességében kimondható, hogy a nemzeti szabályozás jogszabályi követelményként meghatározza a bizalmi területnek nevezhető szaktevékenység szabályozási kötelezettségét. Ezzel együtt *az is kimondható, hogy ez a kötelezettség a közigazgatás számára kötelező érvényű útmutatást nem ad, a szabályozási kérdésekhez nem biztosít támpontot*, illetve azt sem rögzíti, hogy a speciálisan kialakított funkcionális szervezetek – mint jelen esetben a Magyar Honvédség – milyen elvek szerint alakítsa ki szabályozóját, vagy szabályozási rendszerét. A szervezeti sajátosságokat alapul véve a publikusan tárgyalható tényezők mentén célszerű a szabályozási feladat előkészítéseként a fontosabb feladatok, tényezők áttekintése, kiemelt figyelemmel arra a tényre, hogy *a rejtjelzéssel kapcsolatos hadtudományi publikáció igen szegényesnek tekinthető*.

A VÉDELEM ELSŐ SZINTJE

Kiindulási alapként kijelenthető, hogy a rejtjelzés – tehát az adatok kezelés vagy továbbítás alatti rejtjelzéssel történő védelme – *szolgáltatás*! Ezt a szolgáltatás napjainkban zömében összetett elektronikus adatkezelő szolgáltatásokon keresztül, ritkább esetben egyszerűen, önálló eszközök szintjén – bár akkor is szolgáltatásként – vehető igénybe. A rejtjelzés – mint

szolgáltatás – védelme felbontható két logikai területre, mint eszköz vagy alkalmazás szint, illetve támogatási szint.

A rejtjelző eszköznek vagy alkalmazásnak *önmagában biztosítani kell az elsődleges védelmi szintet*, melyet valamilyen illetékes hatóság megvizsgált, auditált és engedélyezett.

Az első védelmi szint a rejtjelző eszköz vagy alkalmazás előírásszerű működése a specifikusan kialakított üzemeltetési (kezelési) szabályzatok szerint. Itt nincs más szereplő, csak az rejtjelző eszköz vagy alkalmazás működéséhez szükséges erőforrás (hardver, szoftver és a működéshez szükséges kiegészítők, a kezelési utasítások, a kezelő vagy felhasználó állomány) az algoritmus, a kulcs és az adat, annak érdekében, hogy kezelői vezérléssel vagy automatikusan BLACK (rejtjelzett) adat álljon elő tárolás vagy továbbítás céljából.

Ennek megfelelően a rejtjelző eszköz vagy alkalmazás legyen hatósági engedélyek által megerősítetten megbízható, rendelkezzen kezelési utasítással (és egyéb, a kezelésre telepítésre és üzemeltetésre vonatkozó szabályozókkal), mely szabályozók szerint üzemeltetve biztonságosan működik a hálózati vagy helyi rejtjelző szolgáltatás. Logikailag ide tartozik, az a biztonsági feladatrendszer, hogy:

- A rejtjelző eszközhöz vagy alkalmazáshoz szükséges kulcsgyártás – és a műszaki dokumentációk, egyéb segédanyagok előállítása – biztonságos körülmények között, jóváhagyottan történik. Ezek a szintén bizalminak tekintendő feladatok nem az üzemeltető vagy alkalmazó szervezet, hanem a gyártó és egyéb ellátó szervezetek feladatai közé tartoznak.
- A rejtjelző kulcsok (eszközök, dokumentumok, és egyéb, a tartalmat és érvényességi időt tekintve érzékeny anyagok) megsemmisítése időben és biztonságosan történik. Ez már eszköz és anyag-specifikus feladat, melynek egyes részei történhetnek az üzemeltető vagy alkalmazó szervezet hatáskörében.
- A rejtjelző eszközök és egyéb anyagok (összefoglalóan: rejtjelanyagok) mozgatása a specifikumok figyelembe vételével, az illetéktelen megismerés vagy beavatkozás kizárásával, biztonságos feltételek között történik.

Az első szint feladatait áttekintve az összegezhető, hogy arra feljogosított fejlesztők, gyártók, és terjesztők munkája eredményeképpen az alkalmazó szervezetek rendelkezésére állnak hatósági engedélyezett megoldások, melyekkel kapcsolatban a Magyar Honvédség katonai és honvédelmi szervezeteinek a feladatai a fentiek alapján pontosan körvonalazhatók. Ezen a szinten *normál esetben nem szükséges a rendszeresítéssel kapcsolatos kérdésekkel foglalkozni*.

Az a folyamat, amikor jóváhagyó hatóság a fejlesztő-gyártó-terjesztő szervezetekkel együttműködve megvizsgál egy terméket, teszteli, ellenőrzi a hatáskörébe tartozó biztonsági elemeket a fejlesztés, gyártás, alkalmazott anyagok kapcsán, kriptográfiai állóképességet vizsgál, telephely biztonsági tanúsítványon keresztül felügyeletet gyakorol, véletlen szám generálást ellenőriz, kívül áll az alkalmazó szervezet tevékenységi körén. Ennek külföldi rejtelző eszköz vagy alkalmazás esetén is így kell történnie, mert a nemzeti és az illetékes külföldi hatóságok együttműködési feladatai szintén bizalmi körön belüli, zárt tevékenységek. Ezen a szinten *kulcsfontosságú kérdés a szükséges mértékben részletezett érthető, felhasználóbarát és minimális adminisztrációs terheket meghatározó kezelési és üzemeltetési utasítás*. A kiválasztás támogatására jó példa lehet egyes hatósági holnapok tartalma, felhasználói támogatású szemlélete (vagy a NATO ajánlott terméklista), ami azonosítja az engedélyezett rejtjelző eszközöket, alkalmazásokat, biztonsági eszközöket és szoftvereket, megsemmisítő eszközöket és eljárásokat, így *az alkalmazó szervezet könnyen ki tudja választani az adatkezelési szükséglete szerinti terméket, és csak az alkalmazását kell az illetékes hatósággal engedélyeztetnie*.

A valóság természetesen egy kicsit más, mivel a Magyar Honvédség katonai szervezeteinek működését újabb és újabb vezetési és irányítási feladatok szolgálják, illetve a

Szövetség is folyamatosan fejleszti híradó és informatikai rendszereit (communication and information systems; CIS). *Az új szolgáltatásokhoz szükséges rejtjelző szolgáltatások fejlesztése és rendszerbe integrálása e folyamatos fejlesztési szükséglet miatt folyamatos, de erősen rendszer-specifikus, pontosan nem tervezhető folyamatokat jelent, amelyek nem nélkülözhetik katonai szervezetek közreműködését.*

A VÉDELEM MÁSODIK SZINTJE

A második védelmi szintet a rejtjelzést támogató folyamatok biztonságát célzó védelmi rendszabályok képviselik. A biztonsági követelmények alapján kialakított védelmi rendszabályok azok a tényezők, melyek a rejtjelző szolgáltatás bizalmasságának, sértetlenségének és rendelkezésre állásának megvalósulásához szükségesek, mint a rejtjelzés „biztonsági környezete"; ez az eszközt övező „külső védelmi gyűrű" a hagyományosnak tekinthető információbiztonsági területeken: fizikai biztonság, személyi biztonság, adminisztratív biztonság (korábban: dokumentumvédelem) és elektronikus biztonság.

A felsorolást a rejtjelzés speciális jellege miatt célszerű értelmezni, kiegészíteni. A fizikai biztonságra vonatkozó követelmények a vonatkozó kormányrendeletben meghatározottak. Ugyanígy rögzített az adatkezelési engedély megszerzésére vonatkozó követelményrendszer akár nemzeti, akár NATO, EU minősített adatkezelésről vagy rejtjelzésről van szó, így ezt a követelményrendszert kell alkalmazni – és szükség esetén – specializálni a szabályozásnál. A fizikai biztonság témáján belül *meg kell határozni a szállításra vonatkozó követelményeket, illetve kezelni kell a tábori kommunikációs rendszerrel kapcsolatos speciális eseteket és a mobil alkalmazást is*. Ugyanígy megoldandó a felügyelet nélküli létesítmények biztonságának kérdése, mert a felügyelet nélküli objektumok az előre kialakított riasztási rend által értesített reagáló erők kiérkezéséig élőerős védelemmel nem rendelkeznek, ami a rejtjelző eszközök biztonsági szempontjából speciális tervezési tényező.

A személyi biztonsággal kapcsolatos követelményrendszer a vonatkozó kormányrendeletekben rögzített. A jogszabályok az adott képességekre vonatkozó „rendelkezésre állását", határozzák meg (a rejtjelfelügyelő kiállítja a tanfolyam végzettségét igazoló jegyzőkönyv alapján a rejtjelző eszköz kezelési engedélyt, illetve a titkos ügyviteli tanfolyam elvégzése után történhet rejtjelirat kezelése), az ezzel kapcsolatos képességek megszerzése az alkalmazó szervezetek feladata. A képzési követelményekkel kapcsolatban nincs központi kormányzati követelmény támpont, így Magyar Honvédség szinten *meg kell határozni a szakmai képzésre, továbbképzésre vonatkozó követelményeket*.

Az adminisztratív biztonság területén az iratkezelésre vonatkozó döntő lépés az elkülönítésre vonatkozó követelmény megértése, **Error! Reference source not found.** és a végrehajtása érdekében szükséges feladatok végrehajtása. Ennek lényege, hogy a közfeladatot ellátó szervezetek iratkezelésére vonatkozó követelmények érvényesítését **Error! Reference source not found.** a szervezet nyilvántartási rendjében, abból eredően, de a szaktevékenység sajátosságainak figyelembe vételével „elterelve", egy másik rend szerint kell kialakítani. Ez azt jelenti, hogy a rejtjelzéssel, illetve a szaktevékenység támogatásával foglalkozóknak minden ügyben vizsgálni kell, hogy az adott iratot be kell-e sorolni a rejtjelirat körébe, vagy nem. *A feladat egyrészt nehezítés, másrészt az iratkezelés „megtisztítását" is jelenti*. A nehezítés abban áll, hogy az ügyintézőnek mérlegelnie kell az adott ügyet, és döntése szerint kell az ügyviteli feladatokat elvégezni (tehát az ügyintézők két ügyviteli eljárásrend szerint látják el feladatukat). A nehezítés egyben kétségeket szüntet meg, mert meggátolja azt a nyilvánvalóan abszurd helyzetet, hogy nem rejtjelző szervezet elkülönítést igénylő rejtjeliratot kapjon (ami a gyakorlatban csak ügykezelői fejfájást okozhat). Az elkülönítést nem igénylő kommunikáció rejtjelző szervek között is a „normális" iratkezelési rendbe tartozhatnak, így a rejtjelzés körébe tartozó feladatok nem kerülnek mérlegelés nélkül az elkülönített iratkezelés

hatálya alá (egyértelmű például, hogy egy továbbképzéssel kapcsolatos adminisztratív feladatok, mint a résztvevő nevének, rendfokozatának és szállásigényének azonosítása nem rejtjelügy). Az elkülönítés gyakorlati végrehajtását Magyar Honvédség szinten központilag kell támogatni, mert *az egységes működési rendre vonatkozó követelmény nem engedheti meg, hogy az egyéni mérlegeléssel történő besorolás alapján két katonai szervezet ugyanarra az esetre eltérő besorolási döntést hozzon*.

Az adminisztratív területen szakterületi fejlődési lépcsőt jelent, hogy a szakmai irányításért felelős vezető a rejtjelzésre vonatkozóan 2012-ben szakutasítást adott ki a rejtjeliratokra vonatkozóan, **Error! Reference source not found.** ami 2013-tól korszerű alapokra helyezi a szaktevékenységet.

Az elektronikus biztonsági rész a vonatkozó jogszabályban keretjellegűen, inkább a minősített elektronikus adatkezelésre vonatkozóan jelenik meg, így ezen a területen részletesebben kell szabályozni a Magyar Honvédség katonai szervezeteinek működéséhez szükséges szakterületi ügyeket. Ennek lényege:

- a rejtjelző eszközök üzemeltetésére szolgáló helyiségek (tárolást szolgáló helyiségek, hírközpont elemek, csomagoláshoz vagy egyéb művelethez szükséges munkaterek, mobil hírközpont elemek és konténerek) esetében a kezelői utasításokban meghatározott műszaki követelmények érvényesítése;
- a helyiségekben a szükséges esetekben szűrt erősáramú tápellátás biztosítása;
- a kiegészítő földelésre (biztonsági földelés), és annak hitelesítésére vonatkozó követelmények érvényesítése;
- a kábelezésekre, nyomvonalvezetésekre vonatkozó követelmények;
- az eszközök és berendezések közötti biztonsági távolságok alkalmazása, árnyékolás;
- a különböző identitású vagy minősítési szintű adatkezelésre feljogosított rejtjelző eszközök, hálózati eszközök funkcionális elkülönítése, BLACK/RED elkülönítés (nem minősített és minősített adatkezelő eszközök kábelek közötti elkülönítés), egységes jelölési rendszer alkalmazása; eszköz és kábelnyilvántartás,
- az üzemelő és hibás vagy tartalék eszközök, anyagok elkülönítése és jelölése;
- a rendelkezésre állási követelménynek megfelelő tartalék áramellátás biztosítása;
- a szükséges üzemeltetési környezet biztosítása (hűtés, fűtés, elektromágneses kompatibilitás, fizikai és mágneses hatások elleni védelem) az eszközök üzemeltetése, valamint az eszközök és anyagok tárolása során.

A fenti, csak fontosabb témák részletesebb meghatározásakor célszerű a vonatkozó nemzetközi szabvány ajánlásait követni, és a specializált követelményeket ennek megfelelően kialakítani. **Error! Reference source not found. Error! Reference source not found.**

Ezen a szinten jelenik meg az eddig nem szereplő menedzsment feladatrendszer: *az elektronikus adatkezelő rendszerek akkreditálása* (rendszeresített rejtjelző eszköz adott híradó és informatikai rendszerbe történő beépítése és a hatóság által történő engedélyeztetése), illetve az ezt *megelőző tesztek, kockázatelemzés, telepítés és ellenőrzés*. Rögzíteni kell a rejtjelző eszköz vagy alkalmazás módosítására és a karbantartásra vonatkozó általános követelményeket is.

Specifikus, ebben a fejezetben tárgyalandó kérdés az elektronikus formájú kulcsok kezelésére és menedzselésére vonatkozó általános biztonsági követelmények meghatározása. E témakör tartalmazza a minősített adat és a rejtjelzés körébe tartozó minősített adat különbsége miatt szükséges eljárások rendezését (a rejtjelkulcs gyártása során a minősítéshez szükséges alaki kellékek kérdése: minősítési szint, érvényességi idő, minősítő neve és beosztása és aláírása, beosztásának rögzítése), az adathordozó eredeti irattári példányára vonatkozó megsemmisítési tilalom kérdését az érvényességi idő lejárta előtt, **Error! Reference source not found.** illetve *az elektronikus adatkezelésből adódó egyedi nyilvántartási és kezelési szabályok rendezését.*

A rendszeresített rejtjelző eszköz rendszerengedélyeztetése szempontjából a hatóság feladata már nem a rejtjelző eszköz kriptográfiai állóképessége, a szükséges kulcshosszúság mérlegelése, hanem az üzemeltetői környezet, a biztonságos üzemeltetéshez szükséges feltételek komplex vizsgálata. Emiatt a tervezés, kockázatelemzés feladata az alkalmazó szervezet számára az, hogy *a nemzeti vagy más hatóság által engedélyezett rejtjelző eszközt, vagy alkalmazást hogyan lehet biztonságosan üzemeltetni, illetve az ezzel kapcsolatos bizonyítékokat szolgáltatni*.

Ennél a feladatnál érdekes lehet a „rejtjeltevékenység" engedélyezése (pontosabban hatósági egyetértés a szabályozásról) abban az esetben, ha a katonai szervezetnél korábban nem üzemelt rejtjelző eszköz vagy alkalmazás, mert a jogszabály szerint ilyen esetben a hatóság a rendszerengedély mellett a (rejtjelző) szabályzatot is ellenőrzi. Ez felveti azt a központilag eldöntendő kérdést, hogy Magyar Honvédség szinten *a rejtjelzés és támogató tevékenységeinek szabályozása elvégezhető-e egy lépésben, vagy hierarchizálni kell a szabályozást*. A kérdés megválaszolása korábbi döntés értelmezését és felülvizsgálatát is jelenti, mert a 2009-ben kiadott felső szintű információbiztonsági politika az egyszintű szabályozási rend mellett döntött, megerősítve a helyi jellegű általános körben értelmezhető kötelező szabályozási elemekkel (ebbe a körbe tartozik a szervezeti működési leírás, a munkaköri leírás, illetve a szolgálati utasítás). **Error! Reference source not found.**

Adminisztratív jellegű, rejtjelző szempontból nem kulcsfontosságú kérdés, hogy a hálózatban alkalmazott rejtjelző eszköz „rendszerengedélye" önálló hatósági határozat, vagy a híradó és informatikai rendszer „rendszerengedély"-ben feltüntetett adat, de rendezetlenség esetén *az alkalmazott rendszerek számának növekedésével ez problémás kérdéssé is válhat*.

A menedzsment feladatok körébe kell sorolni *a rendkívüli (normálistól eltérő) üzemeltetési helyzetek megoldására meghatározott általános követelményeket és eljárásrendet a kompromittálás, a működés folytonosság és helyreállítás, valamint a vészhelyzeti tevékenység területeken*.

A kompromittálódás szakterületi kérdése azért jelenthet szakmai érdekességet, mert *a vonatkozó jogszabály ezt a jelenséget közvetlenül nem említi*, így az ezzel kapcsolatos feladatok csak közvetetten levezethetők, illetve más szakirodalomra támaszkodva oldhatók meg. Terminológiai elemzés és a minősített adatkezeléssel kapcsolatos párhuzamok keresésének mellőzése nélkül erről a kérdésről annyit érdemes összefoglalni, hogy o*lyan bekövetkezett (vagy vélelmezett) információbiztonsági incidensről van szó, amikor a rejtjelzésre vonatkozó bizalmassági célkitűzést szolgáló rendszabályok sérülnek vagy sérülhetnek*. Ez az eset nem biztos, hogy a kezelt minősített adat bizalmasságát sérti, lehet, hogy csak valamilyen támogató folyamatot érint, ráadásul növeli a fenyegetést, hogy *az incidens eredményeképpen megszerzett technikai vagy adminisztratív jellegű adat térben és időben egy másik ponton jelenthet megelőző jelzések nélküli információs károkozást*. Emiatt kiemelten fontos, hogy még a gyakorlatok, tesztek, karbantartások esetén bekövetkező incidensek is kellő alapossággal kivizsgáltak legyenek, elkerülendő az elégtelen biztonságtudatosságot jelentő képzeletbeli jelentést: „jelentem, csak teszt kulcs volt Főnök!"

A kompromittálódás kezelésének kulcskérdése *a mielőbbi feltárás, a helyzet pontos megértése, és a megelőző rendszabályok meghozatala*. Ilyenkor nem az a legfontosabb kérdés, hogy az adott személy vétkessége milyen mértékű, hanem az, hogy *mielőbb megtörténjen a kárenyhítés, illetve az incidensből eredő jövőbeli károk megelőzése*. Hálózatok esetén ez a feladatkör szoros szervezetek közötti együttműködést igényel, ami szövetségi szinten lényegesen bonyolultabb folyamatokat takar. A feltárást felhasználóbarát kérdőívekkel és folyamatos képzéssel lehet támogatni (*a helyi biztonságért felelős vezető „hálózatos" gondolkodása kulcsfontosságú kérdés*), a hatékony kommunikációt pedig naprakész adatok biztosíthatják.

A kompromittálódások kezeléséhez – az ellenőrzési feladatkörhöz kapcsolva – hozzá kell csatolni a tapasztalat feldolgozást és hasznosítást is, mert a megtörtént esetek alapján történő szabályozási korrekciók nélkül a biztonsági rések egyre szélesebbek lehetnek a szabályozó rendszerben.

A működésfolytonosság és helyreállítás az elektronikus adatkezelés biztonságához tartozó folyamatokat jelent, melyeket specializálni kell a rejtjelzés területére is. Támpontként itt is felhasználhatók a nemzetközi szabványok ajánlásai. **Error! Reference source not found. Error! Reference source not found.** Itt a rendelkezésre állásra vonatkozó követelményeknek való megfelelés a feladat. *A szolgáltatás kiesés, vagy szolgáltatási szint csökkenés esetén alkalmazandó minimális szolgáltatásra vonatkozó követelményeket a hadműveleti (alkalmazói) követelményekre építve lehet és kell meghatározni.* Ez értelemszerűen nem a rejtjelzésre vonatkozó követelményrendszer. *A híradó és informatikai rendszer rendelkezésre állási paraméterei határozzák meg a rejtjelző eszközök és alkalmazások rendelkezésre állási követelményeit*, így ez a tevékenység is rámutat a szakterületek közötti együttműködés fontosságára, nélkülözhetetlenségére. Részletek említése nélkül is belátható, hogy ennél a feladatnál *rendszer-specifikusan kell elemezni az rejtjelző eszköz szintű tartalékolás és hálózatmenedzselés, széles körben értelmezve a működési feltételek biztosítását (áramellátás, javítóanyag, rejtjelkulcs ellátás), illetve a redundáns hálózatok üzemeltetésének eseteit*. A rejtjelzésre vonatkozó működésfolytonosságnál kiemelt fontosságú feladat a tervek és szabályozók naprakészen tartása, működőképességük tesztelése és a változások folyamatos átvezetése, a végrehajtók gyakoroltatása, mert ezek nélkül még hibátlanul működő híradó és informatikai rendszer esetében sem várható el elektronikus adatkezelés.

A vészhelyzeti tevékenység a *természeti katasztrófák vagy ellenséges tényezők rejtjeltevékenységre vonatkozó negatív hatásainak ellensúlyozását célozzák*. A *helyszín és rendszer-specifikus megoldások kockázatfelmérésen és értékelésen kell, hogy alapuljanak*. A *béke elhelyezési vagy missziós feladatok nagymértékben eltérhetnek*, és nyilvánvaló, hogy az életmentésen kívül tartalmazniuk kell a lehető leghatékonyabb megoldásokat a rejtjelzés bizalmasságának sérülése elkerülése érdekében, nem kikerülve azt a gyors döntést sem, amelyik vészmegsemmisítést rendel el. Ennél a feladatnál kiemelt fontosságú az érintett állomány feladatismerete és gyakorlottsága, a megoldási variációk szerint kialakított munkahelyek (a végrehajtók ne gátolják egymást a végrehajtásban), a részfeladatokra bontott tervezés (ne a bekövetkezéskor kezdődjön a rögtönzés), illetve a folyamatok vészhelyzet alatti nyomon követése (a helyzet megoldása után azonosítható legyen az eszközök és anyagok sorsa vagy helye).

A menedzsment feladatok eddigi részei tartalmazták a „mit hogyan kell csinálni”és a „mit kell csinálni a normálistól eltérő helyzetben” kérdéseket, de ezek mellett nem lehet eltekinteni egy hatékony ellenőrzési rendszer kialakításától és fenntartásától. Az ellenőrzési rendszer kialakításának és fenntartásának célja a meghatározottaktól való eltérések észlelése, feltárása, a hibaelhárítás a szükséges eseti és szabályozási korrekciók megtétele érdekében. Az „ellenőrzési rendszer” kifejezés tágan értelmezendő, ide tartozik az időszakos vizsgáztatás (osztályos vizsgaként vagy eseti elrendelt műveletként), a technikai jellegű paraméter ellenőrzések, a telepítések ellenőrzése, az ügyvitel, a készletárolás és készletezés megfelelősége, az önképzés, a vészhelyzeti gyakorlások, a tapasztalat feldolgozás és hasznosítás. Az ellenőrzési feladatok kidolgozásánál érdemes a nemzetközi szabványok gyakorlatát követni, mely szerint a szabályozó rendszer (követelményrendszer) kialakításakor ki kell alakítani a folyamatok és események értékeléséhez szükséges mérőpontokat, ellenőrzési szempontokat. A rejtjelzés területén *a híradó és informatikai rendszer egyéb területeihez hasonlóan ki kell alakítani az általános ellenőrzési szempontrendszert, amit hely, vagy rendszer szerint tovább specializálható*. Az ellenőrzés területén az egységesítés a tapasztalat feldolgozás és a hatékony szabályozási visszacsatolás szempontjából

nélkülözhetetlen, annak ellenére, hogy a napi feladatok szorítása során ezek a szempontok gyakran feledésbe merülnek.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A fentiek alapján jól látható, hogy rejtjelzés szakterülete a híradó és informatikai rendszer, illetve az elektronikus információbiztonság alapvető „mozgatórugói" szerint is értelmezhetők, vizsgálhatók, bár a szakirodalom az alapvető ismeretek és szakterületi feloszlások ismertetésén kívül erre még kevés példát adott. A rejtjelzés helye, szerepe az elektronikus adatkezelésben tisztázható, a szükséges szakmai kapcsolatok kialakíthatók, illetve a helyi vagy rendszer-specifikus eljárások kidolgozhatók.

Magyar Honvédség szinten az elektronikus információbiztonság egyéb területeihez hasonlóan rejtjelzés esetében is *célszerű szabályozási rendszerben és nem szabályozóban gondolkozni*. Ennek lényege, hogy egy jogszabályi követelményeket kielégítő, kellően részletezett központi szabályozó álljon rendelkezésre, ami *pontosan tartalmazza a központilag meghatározható követelményeket és eljárásokat, illetve pontosan meghatározza a helyi vagy rendszer-specifikus szabályozókra vonatkozó tartalmi és formai követelményeket*. Az ilyen „felhasználóbarát" szabályozás lényegesen megkönnyíti az alkalmazó katonai szervezetek munkáját, csökkenti felelősségüket és az adminisztrációs terheket, ugyanakkor javítja a hatósági munka hatékonyságát is, mert egy átlátható, egységes rendszer szerint kialakított szabályozási környezetben kell a hatósági feladatait végeznie.

Részkérdések még jelenthetnek kihívásokat, mert egyértelmű az az igény, hogy *a nemzeti, NATO vagy EU eljárások minél jobban összehangoltak legyenek, lehetőleg ugyanazt az erőforrást igényeljék, ami még számtalan egyedi eljárás kialakítását követeli meg a Magyar Honvédségnél*. Ugyanígy megoldandó kérdés a nemzetközi szakirodalomban olvasható, de jogszabályban nem tárgyalt *rejtjelző besorolású eszközök (crypto controlled item; CCI) mibenlétének megértése, kezelési kérdésének megoldása, ami szintén a felhasználói tevékenységet fogja megkönnyíteni*.

Az első és a második védelmi szint feladatai között *egymástól eltérő jellegű és bonyolultságú folyamatok találhatók*, eltérő technikai és szervezeti szükségletekkel. A híradó és informatikai szolgáltatások fejlődése során *a folyamatok folyamatosan átalakulnak és fejlődnek – benne a rejtjelző szolgáltatások is –*, így *a központi rejtjelző szabályzat feladata inkább a folyamatokra vonatkozó általános biztonsági követelmények meghatározása, mint az alacsonyabb szinten is szabályozható specializált szakfolyamatok meghatározása.*

Felhasznált irodalom

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

[2] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 1.§. 12. p, 6. §. (2), 54.§. (2), és 61. §. (1-2)

[3] 161/2010. (V. 6.) Korm. rendelet, 29. §. (1)

[4] 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről

[5] A Honvéd Vezérkar híradó, informatikai és információvédelmi csoportfőnökének 15/2012. (HK 11.) HVK HIICSF szakutasítása az MH rejtjelző szakiratkezeléséről

[6] MSZ ISO/IEC 27001:2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények, „A” melléklet, A 9. 2. p.

[7] ISO/IEC 17799: 2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002:2006), 9. 2. p.

[8] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről, 38. §. (1) és 56. §. (1)

[9] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról, 14. §. (1) d) és (2) c) p.

[10] MSZ ISO/IEC 27001:2006. Informatika. Biztonságtechnika. Az információbiztonság

[11] irányítási rendszerei. Követelmények, „A” melléklet, A 14. 1 – 14. 1. 5. p.

[12] MSZ ISO/IEC 17799: 2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002:2006), 14. 1. 1 – 14. 1. 5. p.