HADMÉRNÖK

X. Évfolyam 1. szám - 2015. március

KASSAI Károly
karoly.kassai@hm.gov.hu

ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI ALAPISMERETEK A HONVÉDELMI SZERVEZETEK ÁLTAL KEZELT MINŐSÍTETT ADATOK BIZTONSÁGA ÉRDEKÉBEN

Absztrakt

A honvédelmi szervezetek működése erősen függ a híradó-informatikai rendszerektől. A fegyverirányítási rendszerek, a légi irányítási rendszerek, a harcászati kommunikációs rendszerek vagy a stratégiai kommunikációs rendszerek működése elektronikus kommunikációs és adatkezelő képességekre épül. A katonai műveletek jelentős része szenzitív adatok felhasználásán alapul, így az információs fenyegetések növekedésével az információ biztonsági képességnek is egyre jelentősebb szerepe van. A katonai szervezetek élete gyorsan változó, rugalmas, beleértve a személyi változásokat is. Az az elektronikus információbiztonságra irányuló gyakori kérdések a parancsnokoktól, biztonsági vezetőktől megerősítik a biztonságtudatosság fontosságát. A cikk az általános vezetői ismeretek megerősítését szolgálja a minősített adatok kezelésének megfelelő védelme érdekében.

Operation of the military organizations highly depends on the communications and information systems (CIS). The operation of weapon control systems, air traffic control systems, tactical communication systems or strategic communications based on electronic communication and information management capabilities. A significant number of military operations are based on the use of sensitive information so the increases of information threats the CIS security has increasing role. The life at military organizations is rapidly changing, flexible, including personnel changes. The frequently asked questions from military commanders, security managers about CIS security reinforce the importance of the general security awareness. The article serves to strengthen the overall knowledge of management of military organizations in order to protect classified information appropriately.

Kulcsszavak: *információbiztonság, elektronikus információbiztonság, kiberbiztonság, információbiztonsági tudatosság, információbiztonsági követelmények ~ information security - information assurance, electronic information security (INFOSEC, CIS Security), cyber security, security awareness, information security requirements*

BEVEZETÉS

Az elektronikus információbiztonság területén hazánkban számtalan intézmény szervez általános vagy specializált képzéseket, tanfolyamokat. A képzési paletta színes, a megszerzett ismeretek által széleskörű kompetenciák alakíthatók ki, ugyanakkor a minősített elektronikus adatkezeléshez szükséges tudás kialakítása nem egyszerű eset. Amikor gyakorlati kérdésekről, vagy NATO, EU követelmények szerinti minősített elektronikus adatkezeléséről van szó, az alkalmazható források szemlátomást apadnak…

A cikk célja – a minősített elektronikus adatkezelésre koncentrálva – a fontosabb elektronikus információbiztonsági kérdések bemutatása egyszerűen, érthetően. Az ismertetés átfogó jellegű, Magyar Honvédség specifikus, NATO, EU követelményeket integráltan alkalmazó; célzottan a parancsnokok, vezetők, biztonsági vezetők, végrehajtásba együttműködők szakterületi eligazodása, támogatása érdekében fogalmazott.

A NATO, EU követelmények, jogszabályok, és a Magyar Honvédség belső szabályozói valamint az értelmezéshez szükséges tudás egy átfogó jellegű ismertetésben – felhasználóbarát módon – nem összesíthető, így a cikk eligazodást segítő iránytű, és nem tankönyv, részletes tudástár vagy lexikon.

VEZETŐI FELADATOK – HELYI SZABÁLYOZÁSI KÖTELEZETTSÉG

A honvédelmi szervezeteknél a legfontosabb teendőket a *felelősségek kijelölése,* a *szabályozás* és az *összehangolás* témakörök köré lehet csoportosítani az alábbiak szerint.

1. Szervezeti Működési Szabályzatban (SZMSZ), belső rendelkezésekben a felelősségek és szervezeti feladatok meghatározása, és a felelős személyek kijelölése, mint:
   a) biztonsági vezető;
   b) rejtjelfelügyelő (rejtjelfelügyelet) és rejtjelző;
   c) rendszerbiztonsági felügyelők (felügyelet), szükség szerint kompromittáló kisugárzás elleni védelmi felelősök (elektronikus információbiztonságért való felelősség).
2. Helyi elektronikus információbiztonsági szabályzatok jóváhagyása, naprakészen tartása [1]:
   a) BIZALMAS[1] vagy magasabb minősítés (vagy KORLÁTOZOTT TERJESZTÉSŰ, nyilvános hálózathoz csatlakozó hálózat) esetén Biztonsági Követelmények dokumentum és Üzemeltetés Biztonsági Szabályzat, KORLÁTOZOTT TERJESZTÉSŰ minősítés esetén Üzemeltetés Biztonsági Szabályzat.
   b) Üzemeltetés Biztonsági Szabályzat esetén az üzemeltetői és a felhasználói Szabályzatot elkülönítetten kell kialakítani [2].[2]
   c) A „Biztonsági Követelmények” dokumentumot a rendszer központi üzemeltetője készíti, végpont üzemeltetés esetén azt csak igényelni kell.
   d) Szervezeti Rejtjelszabályzat [2]. A szabályzati kiadása és módosítása esetén a szükséges szakmai ellenőrzés érdekében az elöljáró rejtjelfelügyelet egyetértését ki kell kérni.

[1] A cikk általános értelmezés érdekében a minősítési szinteket egységesen nagybetűvel tartalmazza, jelezve, hogy az adott követelmény a nemzetközi követelmények és jogszabályok alapján a minősítési szinttől és nem az adat eredetétől (NATO, EU vagy egyéb származás) függ.

[2] Az elkülönített szabályozásra vonatkozó követelmény célja a felhasználói környezet védelme, az üzemeltetői és egyéb érzékeny rendszeradatok felesleges publikálásának megakadályozása.

3. A helyi elektronikus információbiztonsági szabályozók és az egyéb területű szabályozók összehangolása:
   a) Biztonsági Szabályzat;
   b) Őrzésvédelmi Terv;
   c) vészhelyzeti tervek.

A felelősségek kijelölésénél „jól működő recept” nem azonosítható. Nagy létszámú, több állomáshelyen települő katonai szervezet esetében nem elégséges egy-egy felelős személy kijelölése, mert az nem támogatja a biztonsági kérdések helyi kézbentartását, másrészt az adminisztratív feladatokat is jelentősen megnehezíti. Azt a célt kell követni, hogy egy elektronikus adatfeldolgozó helyszínen a felhasználók szakmai támogatása, szakfeladatok végzése vagy biztonsági események megoldása minél gyorsabb és egyszerűbb legyen.

Az említett feladatok mellett kiegészítő elemként még említeni kell azt a kötelező, rutin jellegű tevékenységet, hogy:

- a híradó-informatikai rendszer változtatása, fejlesztése során az elektronikus információbiztonsági szempontokat a szereplők integrálják a folyamatokba;
- a szervezetnél a belső ellenőrzési és képzési rendszer terjedjen ki a híradó-informatikai rendszer biztonsági kérdéseire is; illetve
- a biztonsági tudatossághoz szükséges helyi képzési, továbbképzési folyamatok működjenek, a központi lehetőségek kihasználása megtörténjen.

A BIZTONSÁGI VEZETŐ ÁLTALÁNOS KÖTELEZETTSÉGEI

A kötelezettségeket a vonatkozó kormányrendelet határozza meg [4], melynek lényege:

- Elektronikus információbiztonsági szakterületen a szükséges hatósági engedélyek igénylése és az engedélyek fenntartása.
- A rendszerbiztonsági felügyelők (felügyelet), rejtjelfelügyelő (felügyelet), rendszerüzemeltetők biztonsági feladatellátásnak irányítása, felügyelete, az üzemeltető, biztonsági és felhasználói állomány képzésének és továbbképzésének biztosítása, a védelmi rendszabályok érvényesülésének ellenőrzése.
- A helyi biztonsági dokumentumok elkészíttetése.
- A szervezet rejtjeltevékenységéről a Nemzeti Biztonsági Felügyelet által megadott szempontok szerint történő tájékoztatás az MH Központi Rejtjelfelügyeleten keresztül február 28-ig.
- Az elektronikus minősített adatok kezelésére feljogosított rendszerek, eszközök, a rejtjeltevékenység biztonságának sérülése esetén a kárenyhítési, jelentési és kivizsgálási folyamatok irányítása, szoros együttműködésben az elöljáró szerv szakmai irányítójával.[3]

[3] Az azonnali intézkedések elrendelésével párhuzamosan az azonnali („előzetes”) jelentés az elöljáró szervek felé – mint később az olvasható – kiemelt fontosságú.

SZERVEZETI IRÁNYELVEK – JAVASLATOK

A honvédelmi szervezetnél a minősített adatokat kezelő híradó-informatikai rendszer sikeres menedzselése esetében az üzemeltető, a biztonsági (benne a rejtjelző) állomány, a hadműveleti tiszt és az ügyviteli állomány:

- tartson kapcsolatot, ismerje a rendszerekkel kapcsolatos feladatokat és terveket, a részterületek legyenek képesek összehangolni az üzemeltetési és helyreállítási lépéseket;
- legyen képzett, helyettesítésük megoldott, figyelemmel az összeférhetetlenségi szabályokra;
- a tapasztalatok hasznosítása, megosztása érdekében tartson szakmai kapcsolatot más szervezetek állományával;
- tartsa nyilván a hatósági engedélyeket és időben kezdeményezze a hatósági eljárásokat újra-akkreditálás és változáskezelés esetén;
- rendszeresen hajtsa végre az ellenőrzési és képzési feladatokat (benne a felhasználói képzést), dokumentálja azokat;
- a biztonsági események észlelése, jelentése és megoldása során a pontosságot, a gyorsaságot, a jelentési kötelezettséget tartsa szem előtt, és ne a parancsnoki vagy más hatáskörbe tartozó fegyelmi vonzatokat mérlegelje;
- ne tűrje el, hogy az információk „beragadjanak”, időben informálják a biztonsági vezetőt és ne hagyja, hogy a felhasználó, üzemeltető személyek rutinból végezzék munkájukat, vagy engedély nélkül változtassanak, eltérjenek a szabályoktól;
- a híradó-informatikai szolgáltatások fejlesztése, átalakítása során folyamatosan keressék az egyszerűsítési lehetőségeket, tudatosan kerüljék a kényelmi szempontok miatt kialakított kiegészítő megoldások és eljárások beépítését az üzemeltetési vagy biztonsági folyamatokba.

Az elektronikus információbiztonsági szakterület – beleértve a specialitásokkal rendelkező rejtjelzést – a Honvédségnél a szakirányítás rendjén belül centralizált felépítésű. A szakmai irányításért felelős HM szerv eleme ellátja a jogszabályban szereplő központi felügyeleti funkciókat (MH Központi Rendszerbiztonsági Felügyelet és Központi Rejtjelfelügyelet).[4] Rejtjelzés területén a rejtjelanyagok mozgatása és felügyelete az MH Központi Rejtjelfelügyelet szakmai irányítása alatt álló MH Rejtjelelosztó feladata – országos hatáskörrel.

A hierarchikus szakmai rend azt jelenti, hogy a honvédelmi szervezet – (illetékesség esetén) középszintű vezető szerv – MH központi felügyeleti szerv – kormányzati hatóságok, együttműködő szervezetek vonalon történik a szakmai kommunikáció és munkaszervezés. Ez a működési rend biztosítja az MH Kormányzati Célú Elkülönült Hírközlő Hálózat hálózatgazdával történő kapcsolattartást, a szakmai tudás, a központi hadműveleti igények integrálását a szakmai folyamatokba és hatósági ügyintézésbe, illetve párhuzamosság esetén a prioritások szerinti működést.

A hálózati szemléletű működés *kiszolgálja a katonai vezetési és irányítási struktúrát, de belső működési rendje a hálózat felépítését követi*. *Kritikus fontosságú, hogy a katonai szolgálati alá-fölérendeltségi viszonyoktól eltérő üzemeltetési és biztonsági* (beleértve a rejtjelzéssel kapcsolatos, a hálózati felépítéstől esetleg eltérő egyedi rejtjelző hálózati felépítési rendet) *kapcsolattartási rendet, eljárásokat a rendszer-specifikus üzemeltetési és biztonsági szabályozók pontosan rögzítsék, a biztonsági vezetők és más végrehajtók ezeket részletesen ismerjék.*

[4] A felügyeleti funkciókat az érvényben lévő HM SZMSZ-ben kijelölt feladatokat a HVK Híradó, Informatikai és Információvédelmi Csoportfőnökség szakirányú osztálya látja el.

HÍRADÓ-INFORMATIKAI RENDSZER KIALAKÍTÁSI ÉS ÜZEMELTETÉSI JAVASLATOK

A hálózati típusú megoldásokat, központi üzemeltetési és biztonsági menedzsment szolgáltatásokat előnybe kell részesíteni az egyedi, elszigetelt megoldásokkal szemben, ahol a hadműveleti (alkalmazói) követelmények vagy üzemeltetési és biztonsági szempontok azt nem tiltják. A csak nemzeti felhasználású információs infrastruktúra szemlélet helyett előnybe kell helyezni azokat a megoldásokat, *melyek támogatják a NATO, EU (egyéb nemzetközi) és a közös nemzeti adatkezelést*, és *a fizikai elkülönítés helyett a logikai elkülönítést alkalmazzák*.[5]

Az *elektronikus minősített adatkezelő munkahelyeket, híradó-informatikai szolgáltatás elérési pontokat a katonai felhasználók környezetében kell kialakítani* (abba kell integrálni), és nem elkülönített helyszíneket („titokszoba", „olvasószoba") kell kialakítani.

A felhasználói helyszíneket – ahol csak lehet –, közös kialakítású helyekre kell koncentrálni, az üzemeltető központokat (szervertermek, technikai központok) szintén centralizálni kell.

A biztonságért felelős személyeket (szervezeti elemeket) úgy kell kijelölni (létrehozni), hogy az üzemeltető és felhasználói állomány minél hatékonyabban támogatható legyen.

A felhasználók számára nyújtott szolgáltatásokat, rendszerelemeket a „minimalitás" elve szerint kell kialakítani, *mert a nem szükséges szolgáltatások erőforrásokat foglalnak le és felesleges biztonsági kockázatokat hordozhatnak.*

A katonai elektronikus adatkezelő szolgáltatásokat elsődlegesen a katonai vezetési és irányítási igények szerint kell kialakítani, üzemeltetni és engedélyeztetni, és nem csak a rendelkezésre álló kereskedelmi, irodai szolgáltatásokkal kell megoldani, mert a stratégiai – hadműveleti – harcászati szintek és vezetési-irányítási funkciók specialitásainak megértése üzemeltetési és biztonsági bizonytalanságokat, kockázatokat zár ki.

A honvédelmi szervezeteknél *a képzéseket, továbbképzéseket és tájékoztatókat a felhasználói célközönséghez igazítva „testre szabva", dokumentáltan kell kialakítani.*

A biztonsági incidensek során történő tevékenységkor a legfontosabb információkat azonnal továbbítani kell az elöljáró szint felé, mivel a kárenyhítés, egyéb korrekciók más honvédelmi szervezet, hatóság, együttműködő és szövetséges szervezet eljárásait, rendszereit, rejtjelző eszközeit és szolgáltatásait is érinthetik.

A hadműveleti igények felmerülésével egyidejűleg a biztonsági szempontokat integrálni kell a tervezés és kialakítás folyamatába, megválaszolva a gyakran feledett kérdéseket, mint: ki a tulajdonosa a rendszernek, szoftvernek? Ki üzemeltet, felügyel? Ki az adatbirtokos? Milyen biztonsági funkciókat kell kialakítani, beszerezni, akkreditáltatni? Melyik az illetékes biztonsági hatóság?

Az elektronikus információbiztonsági szakterület feladata az elektronikus információbiztonsági célkitűzések – általában a bizalmasság, sértetlenség és rendelkezésre állás – érdekében szükséges védelmi rendszabályok meghatározása és érvényre juttatása. A szakterület a számítógép és hálózati biztonság, és a hálózatok összekapcsolásának biztonsága, a rejtjelzés és a kompromittáló kisugárzás elleni védelem (TEMPEST) területre tagolható, így a cikk is ezt a tagolást követi.

[5] Ez nem jelenti azt, hogy a Magyar Honvédségnél nincs igény olyan híradó-informatikai rendszerre, mely adatok kezelése során csak nemzeti feldolgozást, adatkezelés igényel. A katonai képességek zöme, a MH Kormányzati Célú Elkülönült Hírközlő Hálózat szolgáltatásainak túlnyomó része a szövetségi együttműködési követelmény szerint kell, hogy működjön. Speciális célrendszerek esetében egyedi biztonsági és üzemeltetési követelményeket kell alkalmazni, melyek közül az egyik leghatékonyabb rendszabály az elkülönítés.

ÁLTALÁNOS ELEKTRONIKUS INFORMÁCIÓBIZTONSÁG

A híradó-informatikai rendszerek biztonságával kapcsolatos feladatokat *az életciklus elmélet alapján célszerű értelmezni*. Az erre a szemléletre alapozott általános követelmények a Magyar Honvédség Informatikai Szabályzat biztonsági fejezetében olvashatók. [6]

Az elektronikus minősített adatokat kezelő híradó-informatikai rendszert a vonatkozó NATO, EU követelményeknek, jogszabályoknak megfelelően kell kialakítani és üzemeltetésüket a Nemzeti Biztonsági Felügyelettel kell engedélyeztetni (akkreditálás).

Az üzemeltetési engedély – rendszerengedély – három évig, illetve az akkreditálás során érvényes körülmények fenntartásáig érvényes.[6] A rendszerek összekapcsolását biztosító technikai rendszer akkreditálásra kötelezett. Az összekapcsolásra engedélyezett rendszer rendszerengedélyének megszűnése az összekapcsolás engedélyezését is megszünteti, így *az összekapcsolási engedéllyel rendelkező szervezet felelőseinek mindkét engedély érvényességét figyelemmel kell kísérnie.*

Szövetségi (nemzetközi) híradó-informatikai rendszerhez magyarországi alhálózat csatlakoztatása összetett feladat. Az alhálózat akkreditálása és a szövetségi (nemzetközi) követelményeknek való megfelelés garantálása (compliance) a magyar hatóság feladata. Második lépés az összekapcsolást biztosító technikai rendszer megfelelőségének vizsgálata és tanúsítása (technikai kialakítás, szabályozás és felügyeleti kérdések) az illetékes nemzetközi szervezet által. Végül az első két lépés után következhet a nemzetközi szervezet részéről (gyakran akkreditációs testület – Security Accreditation Board; SAB) történő engedélyezés, a csatlakozás akkreditálása.

Az összekapcsolással – vagy más hálózathoz történő csatlakozással kapcsolatos feladatok – jelentkezhetnek gyakorlatok, kitelepülések vagy bemutatók során itthon és külföldön egyaránt; tartalmazhatnak rejtjelző hálózatok vagy eszközök összehangolására vonatkozó lépéseket, ahol az emelt szintű biztonsági követelmények, bonyolult eszköz és kulcsellátási kérdések gyakran hónapokban mérhető együttműködést igényelnek (és specializált együttműködési megállapodásokat igényelhetnek). Az összekapcsolással kapcsolatos feladatok helyileg és híradó-informatikai rendszer tekintetében nem követik a Honvédség felépítését, így *gyakori eset, hogy ezeket a feladatokat egy honvédelmi szervezet infrastruktúrájához kötötten kell végrehajtani, az említett felügyeleti rendnek megfelelően*. Az összekapcsoláshoz (vagy csatlakozáshoz) szükséges elektronikus információbiztonsági követelményeket, védelmi rendszabályokat és eljárásokat a NATO, EU vagy egyéb nemzetközi követelmény szerint kell kialakítani – beleértve a hardver és szoftvertanúsításra vonatkozó követelményeket is –, ami lényegesen összetettebb feladat, mint a keretjellegű jogszabályok végrehajtása.

A hatósági engedélyek érvényességi idejével kapcsán a biztonsági vezetőnek akkor is van feladata, ha az engedély lejártával a meghosszabbításra nincs szükség. Ebben az esetben a felhasználói és napló adatok mentésével, adathordozó tárolásba helyezésével, a biztonsági dokumentumok irattárazásával kapcsolatos feladatokat kell végrehajtani, tehát *a „lejár a rendszerengedély, van valami teendőnk?” – kérdésre adott nemleges válasz ne legyen megnyugtató a biztonsági vezető számára*.

A híradó-informatikai rendszerek az akkreditált hardver és szoftver konfigurációval, külső adatcsere szolgáltatásokkal, az adatkezelési engedélyben szereplő helyszínen üzemeltethetők. Az akkreditáló hatóság (Nemzeti Biztonsági Felügyelet vagy más illetékes nemzetközi szervezet) kockázatmentesnek ítélt hardver, szoftver megoldásokat engedélyez, így *a felesleges kiadások elkerülése érdekében a kialakítás legkorábbi szakaszában ki kell kérni az akkreditáló hatóság véleményét* a tervezett konfiguráció akkreditálhatóságának ellenőrzése érdekében.

[6] Ideiglenes üzemeltetésre, tesztelésre helyhez, időhöz, művelethez vagy egyéb paraméterhez kötött rendszerengedélyek szolgálnak.

A NATO követelmények, jogszabályok által meghatározott általános biztonsági követelmények a rendszer-specifikus technikai vagy üzemeltetési fenyegetéseket nem biztos, hogy ellensúlyozzák, így *a kiegészítő védelmi rendszabályokat, a vállalható kockázatok elhárításához szükséges vészhelyzeti eljárásokat kockázatelemzéssel kell meghatározni*, a szervezet vezetőjével jóváhagyatni, azonosítva a maradvány kockázatokat.

A Rendszerbiztonsági Követelmények dokumentum alapján készítendő Üzemeltetés Biztonsági Szabályzat esetén az üzemeltetői és a felhasználói feladatokat tartalmazó feladatokat elkülönített szabályzatban kell kialakítani (az felhasználóknak elégséges csak a saját munkavégzésükhöz szükséges rendszabályok ismerete).

Az Üzemeltetés Biztonsági Szabályzatnak tartalmaznia kell *az összes olyan folyamatot, feladatot, melyet a honvédelmi szervezetnél az üzemeltető és felhasználó állománynak ismernie és követnie kell*.

A vezetői feladatokhoz tartozó ellenőrzési kötelmek értelme, lényege a megfelelőségről történő meggyőződés. A honvédelmi szervezeteknél ezeket a feladatokat az Üzemeltetés Biztonsági Szabályzat struktúráját követő szakutasítás segíti, így *akkreditálás előkészítése vagy önellenőrzés esetén nem szükséges új dolgokat kitalálni, elégséges a központi szabályozó szempontjait követni.*[6] A biztonsági vezető a közhiedelemmel ellentétben nem kiszolgáltatott a bonyolult elektronikus információvédelmi rendszabályok területén, csak *élnie kell azzal a lehetőséggel, hogy részleges vagy teljes ellenőrzést rendel el*, melynek eredménye nagy valószínűséggel reálisan tükrözni fogja a rendszernél vagy a honvédelmi szervezet szakterületén az állapotokat.

REJTJELZÉS

A magyar közigazgatási gyakorlat szerint a „rejtjelzés" a minősített adatok védelmére alkalmazott eljárás, azonban a nemzetközi szakirodalom az adat védelmi célú átalakítását és visszaalakítását tartalmazó folyamatot nem minősített adatok esetében is „rejtjelzés"-nek nevezi.[7] A nem minősített adatok védelmére alkalmazott eljárás szokás alapján hazánkban „logikai védelem", „algoritmusos védelem" mellett a „titkosítás" kifejezésként olvasható a szakirodalomban, jogszabályokban.[8]

NATO, EU és nemzeti követelmény szerint rejtjelzést kell alkalmazni minden olyan esetben, amikor a KORLÁTOZOTT TERJESZTÉSŰ vagy magasabb minősítésű elektronikus adat továbbítás során átlépi a védett terület határát, illetve az adatkezelés során a védelem más megoldással nem biztosítható.[9]

Magyarországon rejtjelző eszköznek az tekinthető, melyet a Nemzeti Biztonsági Felügyelet engedélyezett. Külföldi hatóság által engedélyezett eszköz alkalmazását minősített adatok védelmére a Nemzeti Biztonsági Felügyeletnek is engedélyeznie kell. A rejtjelző eszköznek kétfajta engedélye van:

- rendszeresítési engedély (elvi alkalmazási engedély az adott eszközre), és ennek alapján
- az üzemeltető kérésére kiállított rendszerengedély (adott szervezetnél, helyen érvényes).

[7] Az aszimmetrikus rejtjelzésen alapuló elektronikus hitelesítés szolgáltatás (PKI) hazánkban nem a rejtjelzés kategóriába tartozik.

[8] A köznyelvben gyakori a „titkosítás" kifejezés „rejtjelzés"-ként történő alkalmazása.

[9] A „más megoldással nem biztosítható" követelmény napjainkban a fizikai biztonságot, személyes felügyeletet jelentő eljárások szükségességének fenntartása mellett lassan átértékelődik és a mobil kommunikációs eszközöknél, elektronikus adathordozóknál a védelem kiegészítő lépcsőjeként megjelenik a rejtjelzésre, titkosításra vonatkozó követelmény.

A REJTJELZÉS – EGYSZERŰEN

Hazánkban a korábbi gyakorlat szerint a rejtjelző eszköz önmagában is minősített „objektum”, míg a nemzetközi gyártóktól származó, korszerű rejtjelző eszköz önmagában nem minősített, minősítést csak a szükséges üzemi és rejtjelzést biztosító forgalmi kulcsok behelyezése esetén vesz fel.

A rejtjelző eszköz engedélyében szerepel a kezelhető NATO, EU, nemzeti legmagasabb minősítési szint, ami megegyezik az alkalmazott forgalmi kulcs minősítési szintjével. Magasabb minősítésű adat az eszközzel nem rejtjelezhető.

A rejtjelző eszközköz kompromittáló kisugárzás elleni védelemmel (TEMPEST) kell, hogy rendelkezzen.[10]

A rejtjelző eszköz csak a meghatározott műszaki követelmények szerint,[11] és üzemeltetési szabályokkal, kiképzett, szükséges személyi felhatalmazásokkal rendelkező személy által üzemeltethető.

A korábban pont-pont összeköttetésen alapuló rejtjelzett kapcsolatok rendje napjainkban is létezik (és létezését egyes esetekben meg kell őrizni), de *a katonai műveletek támogatása rejtjelzés területén is egyre jobban a „hálózatok világát” jelenti*. A számítógép hálózatokba integrált rejtjelző eszközök nagy száma, az üzemeltetési műveletek felgyorsítása és a biztonsági szint növelése kikényszerítette a rejtjelző eszközök menedzsment központokhoz rendelését és a rejtjelző hálózatok központi felügyeleti rendjének kialakulását (távkezelés, távkulcsolás). Ez a jelenség *a rejtjelző szakterület robbanásszerű fejlődését eredményezi, egyre több hálózati, informatikai tudást integrálva, így a szakterület az évtizedekkel ezelőtti „öntött vas” típusú védelemből a „hálózatba integrált rejtjelző szolgáltatássá” alakul át*.

Ugyanez a jelenség ismerhető fel a harcászati rádiók világában is. A korszerű, szoftver-vezérelt rádiók kulcsellátása az automatizálás irányába fejlődik; az átviteli utak biztonságát jelentő frekvencia hopping vagy szórt spektrumú üzemmódok paraméterei és a rejtjelző kulcsok előállítása *egy folyamatba integrálva történik*. A kulcsellátás elektronikus formátumú, illetve már megjelent az átviteli közegen keresztül történő távkulcsolási szolgáltatás is.

Rejtjelző eszközt (a szükséges személyi biztonsági követelményeknek való megfelelés esetén) az a személy kezelhet, aki:

- elvégezte az adott eszköz kezelési tanfolyamot és sikeres vizsgát tett,
- kezelési engedéllyel rendelkezik és kijelölést kapott a feladatra.

Gyakorlásra, tesztre, képzésre külön szabályozva, elkülönített eszközt, kulcsot és adatot kell alkalmazni.

A rejtjeltevékenységre vonatkozó általános követelményeket, eljárásrendet a Nemzeti Biztonsági Felügyelet egyetértésével kiadott Magyar Honvédség Rejtjelszabályzata tartalmazza.

A rejtjelző szakanyagok tárolása, rejtjelző eszközök üzemeltetése a Nemzeti Biztonsági Felügyelet által kiadott adatkezelési engedélyben meghatározott helyszínen történhet.

A rejtjeltevékenységért a rejtjelfelügyelő (rejtjelfelügyelet vezető), a végrehajtásért a rejtjelző vagy a rejtjelző dokumentációkezelő felel. A rejtjelző dokumentációkezelő titkos ügykezelői vizsgával rendelkező személy (kijelölt helyettessel), aki a szervezeti Biztonsági Szabályzatban azonosított rejtjelző kezelő pontot üzemelteti.

A rejtjeltevékenységre vonatkozó szakiratkezelést szakutasítás szabályozza, a rejtjeliratra vonatkozó tartalmi követelményeket is részletesen meghatározva. [7]

[10] A követelmény a KORLÁTOZOTT TERJESZTÉSŰ minősítésű adatok védelmét szolgáló szoftveres rejtjelzés esetén nem alkalmazandó.

[11] A rejtjelzés emelt szintű biztonsági igényéből következik a technikai követelmény, hogy hibás rejtjelző eszköz vagy kulcs rejtjelzésre nem alkalmazható.

A rejtjeliratok, rejtjelanyagok szervezetek közötti mozgatása az MH Rejtjelszabályzatban meghatározott eljárások szerint, rejtjelző nyilvántartó pontokon keresztül történik.

A rejtjeltevékenység szakmai irányító szerve a Magyar Honvédség Központi Rejtjelfelügyelet, aki az irányítást a középszintű vezető szerv rejtjelfelügyelete és a HM, HVK közvetlen szervezetek rejtjelfelügyelője (vagy rejtjelfelügyelete) útján végzi.

A rejtjelanyagok mozgatásának központi felügyeletét, az utalt (MH és közigazgatási) szervezetek és a NATO szervekkel, magyar EU Központi Rejtjelelosztóval való kapcsolattartást az MH Központi Rejtjelelosztó és Kulcsgyártó szervezet végzi. A tevékenység röviden összefoglalható: információ megosztás az ellátó és kiszolgált szervezetek között, az utalt szervezeti elemek szoros szakmai felügyelete és ellenőrzése, az igények gyűjtése, összegzése, ellenőrzése majd ennek eredményeképpen a szükséges ellátás biztosítása, illetve az ezekhez szükséges folyamatos képzési, tájékoztatási és tanácsadási feladatok végrehajtása, a rejtjelző szakterületen jelentkező biztonsági incidensek során azonnali jelentési, tájékoztatási feladatok, illetve ezek kapcsán a szükséges szakmai műveleti feladatok támogatása.

A honvédelmi szervezetnél:

- A rejtjelzésre vonatkozó szabályokat rejtjelszabályzatban kell meghatározni, melyet az elöljáró rejtjelző szerv egyetértése esetén a szervezet vezetője hagy jóvá.
- A rejtjeltevékenységre negatív hatást kifejtő események megoldása érdekében vészhelyzeti tervet kell készíteni. A vészhelyzeti tervet rejtjelfelügyelő készíti és a szervezet vezetője hagyja jóvá.

A rejtjelzés területén bekövetkező biztonsági események vagy incidensek napjainkban is gyakran pánik jelenségek okozói. A félelem érthető, mert adott helyszínen az esetek többségében nem mérhető fel, hogy a rejtjelző kompromittálódásnak milyen hálózati (nemzeti vagy szövetségesi) következményei lehetnek, milyen információk kerülhetnek veszélybe, vagy milyen híradó-informatikai rendszer funkcionális működése válik veszélyessé.

Ezen a területen a következő generációs jogszabályok nagyobb segítséget adhatnak a minősített adat és a rejtjelzéssel kapcsolatos adatok pontos megfogalmazásával, illetve a szükséges incidenskezelési eljárások specifikálásával. A lényegi dolgokat el kell különíteni és valóban csak azt a helyzetet kell incidensnek kezelni (és olyan módon), ami szakmailag szükséges. Erre jó példa lehet egy rakodás közben megsérült vagy megsemmisült magas minősítésű rejtjelkucs, mely esetben nem biztos, hogy ugyanazt az eljárást kell követni, mint a papír alapú minősített adat veszélyeztetésére vonatkozó eljárásrend. Az adott digitális jelsorozat (rejtjelkulcs) valóban minősített adat, de nem felhasználói értelemben, így ha az adott eset bekövetkezése minősített elektronikus adatkezelést vagy adatkezelő szolgáltatást nem érint, akkor nem biztos, hogy a „normál” minősített adatokra vonatkozó eljárást kell az esetre alkalmazni.

Az MH Rejtjelszabályzat kiadását elrendelő, már említett utasítás központi követelményeket határoz meg annak érdekében, hogy a rejtjelzés területén bekövetkező eseményeket milyen szempontok szerint kell azonnal értékelni, és milyen információkat kell az elöljáró szervezet rendelkezésére bocsátani. Ez a központi követelmény segíti a helyzetek gyors megoldását, és szükségtelenné teszi az indokolatlan kapkodást, felesleges jelentéseket és félreinformálásokat.

Az általános elektronikus információvédelemnél említett központi ellenőrzési szempontrendszer kialakítása a Honvédségnél a rejtjelzés területén is megtörtént.

A honvédelmi szervezetek biztonsági vezetői számára érthető, felhasználói szempontok szerint kialakított eljárások alakultak ki.

Rejtjelzés területén ezek a változások a korábbi jogszabályokban megfogalmazott előzményekhez képest jelentősek, így célszerű ezen a területen a rendelkezésre álló szakterületi információkat megismerni és nem a korábbi beidegződések szerint dolgozni.

KOMPROMITTÁLÓ KISUGÁRZÁS ELLENI VÉDELEM

A kompromittáló kisugárzás elleni védelem (TEMPEST) rendszabályok BIZALMAS, vagy magasabb minősítés esetén kötelezőek.

A védelmi rendszabályok célja, hogy *a nem szándékosan vezetett és a sugárzott elektromágneses energia ne tartalmazzon a kezelt adattartalom visszafejtését támogató adatokat.*[12]

A védelmi rendszabályok specifikusak, a helyszín és eszköz, hálózat jellemzői szerint alakíthatók ki.

A védelmi rendszabályok fontosabb elemei az árnyékolás, a földelés, az erősáramú és gyengeáramú szűrés, az eszközök és vezetékek esetében alkalmazott biztonsági távolságok (RED és BLACK elkülönítés) és az üzemeltetési környezet felesleges vezetékektől, fémfelületektől történő mentesítése. A védelmi rendszabályok összessége adja a szükséges védettséget. Költséghatékonyság szempontjából a biztonsági távolságok alkalmazása a legeredményesebb (de nem mindenütt alkalmazható) megoldás.

Az eszközök elhelyezése, nyomvonalak kialakítása során térben kell gondolkodni, és az „alatta-felette" lévő helyiség, vagy pince-tető helyszíneket is figyelembe kell venni. Biztonsági földelés (secure ground) alkalmazása esetén az életvédelmi földeléstől függetlenül kialakított és időszakos méréssel ellenőrzött földelést kell kialakítani; az életvédelmi földelést is időszakosan méréssel kell ellenőrizni.

A NATO, EU vagy a nemzeti TEMPEST védelmi rendszabályok, paraméterek KORLÁTOZOTT TERJESZTÉSŰ és BIZALMAS minősítésű adatok, így alkalmazásuk, meghatározásuk körültekintést igényel.

A Magyar Honvédség esetében a szövetségi kötelezettségvállalások teljesíthetősége érdekében alapelvként a NATO TEMPEST paramétereket kell követni.

TEMPEST VÉDELEM – EGYSZERŰEN

A kisugárzott elektromágneses energia a távolság nézetével csökken; a szabadtéri csillapításhoz minden tereptárgy csillapítása hozzáadódik. Állandó telepítésű híradó-informatikai rendszer, eszköz esetében az első tervezési adat a minősített elektronikus adatot kezelő eszköztől számítva a felügyelt terület határa, figyelembe véve a területen belüli kiegészítő csillapítás (falak, kerítések, tereptárgyak) mértékét. Ez mérésre támaszkodó, úgynevezett zóna értékben megjelenő adat.[13]

A kezelt adatokat kockázattal arányosan kell védeni, így második tervezési adat a minősítési szint.

Az adott környezeti csillapításhoz viszonyítva a minősítési szint figyelembe vételével az eszköz kiegészítő csillapítását és egyéb védelmét biztosító speciális kialakításra vonatkozó paraméter halmaz a harmadik tervezési adat.

Az előzőek alapján adott zónában, adott minősítési szint szerint meghatározott TEMPEST besorolású eszköz és a kiegészítő rendszabályok összessége biztosítja a szükséges szintű kompromittáló kisugárzás elleni védelmet.[14]

---

[12] A védelmi rendszabályok nem a kisugárzás mentességet célozzák, hanem annak olyan szintre csökkentését, ami már valószínűtlenné teszi a visszafejtést, így ez a szakterület nem keverhető össze az elektronikai hadviselés feladataival.

[13] A zónamérést és besorolást a Nemzeti Biztonsági Felügyelet, NATO szervezet, vagy arra feljogosított szervezet végezheti.

[14] Ezek alapján érthető, hogy az „eszköz TEMPEST-es" vagy „oda TEMPEST-es gép kell" tudományosnak vagy szakértőinek tűnő megállapítások a biztonsági követelményeket nem tükrözik valós mértékben.

A gép és harcjárművek, hajók és repülők fedélzetére szerelt híradó-informatikai eszközre (un. platformokra) specializált szabályok vonatkoznak. A platformból kivett eszközre (pl. önállóan alkalmazott laptop) a platformszabály nem alkalmazható, az eszközre az állandó telepítés szerinti paraméterekkel kell számolni.

A mobil hordozókra (konténerek, törzsbuszok) szintén specializált szabályok vonatkoznak. A mobil hordozó állandó telepítése esetén, vagy abból eszköz önálló alkalmazásakor az állandó telepítésű követelményeket kell figyelembe venni.

A TEMPEST VÉDELEM MEGSZŰNÉSE VAGY CSÖKKENÉSE

Az eredeti telepítési vagy üzemeltetési környezet változhat, így a következő esetekben a TEMPEST védelmi szempontok sérülnek amennyiben:

- az üzemeltetés során a felügyelt terület határa csökken, vagy az eszköz környezetében a csillapítást biztosító elemek megszűnnek (pl. falbontás);
- a kezelt adatok minősítési szintje emelkedik;
- az adott üzemeltetési környezetben alacsonyabb szintű TEMPEST eszköz kerül, a TEMPEST eszköz védőburkolata sérül, vagy kiegészítő védelmi rendszabályok megszűnnek.

Az esetek felhívják a figyelmet arra a gyakran feledett sajátosságra, hogy ezen a szakterülete kevés kivételtől eltekintve *a védelem „testre szabott”*. Ezen ismeretek nélkül kellemetlen magyarázkodásokra kell számolni, hogy egy rendezvény, vagy ideiglenes biztosítást igénylő feladatra miért nem lehet az „akkreditált” számítógépet felhasználni, vagy egyik épületből a másikba áthelyezni, ha az említett paraméterek nem egyeznek (hiába „TEMPEST-es” az adott eszköz).

TERVEZÉSI IRÁNYELVEK

A híradó-informatikai rendszereknél, eszközöknél a TEMPEST védelem biztosítható a TEMPEST kialakítású eszközökkel, hálózati elemekkel (és kiegészítő rendszabályokkal), vagy az üzemeltetési környezet TEMPEST védelmének biztosításával.

Az első eset kevés számú eszköz alkalmazása esetén javasolt (drágább eszközök és kiegészítők, de kevesebb kiadás).

A második eset a nagyszámú, vagy bonyolult kialakítású eszközök esetében alkalmazandó (szervertermek, nagy létszámú felhasználói munkaállomás kis helyen, vagy szervertermeken belül TEMPEST tárolók, rack szekrények alkalmazása), ami lehetővé teszi kereskedelmi forgalomból beszerzett (COTS)[15] olcsóbb eszközök alkalmazását, kezelhetőbb amortizációs cseremegoldást biztosít a helyiség által biztosított speciális üzemeltetési környezet kialakításával (központi szűrés, árnyékolás, nyílászárók védelme és egyéb védelmi megoldások).

[15] COTS: Commercial of the shelfs.

DOKUMENTÁLÁS ÉS GARANCIA

A fentiek alapján az adott telepítést a következő dokumentálással kell támogatni:

- zónázási jegyzőkönyv,
- TEMPEST tanúsítvány;[16]
- TEMPEST telepítési jegyzőkönyv.

A TEMPEST kivitelezésű eszköznek általában nincs években kifejezett garanciaideje, de a gyártó kiköthet garanciális elemeket (pl. időszakos felülvizsgálat), így az üzemeltetőnek ismernie kell ezeket a követelményeket.

A konténerek, platformok, árnyékolt helyiségek tartalmazhatnak műszaki megoldásokat, melyeknek működése mérőszámhoz vagy műszaki állapothoz kötött (pl. nyílászárók kereténél alkalmazott tömítések elhasználódása – meghatározott számú ajtónyitás, biztonsági fólia sérülése). Ezen esetekben ellenőrzés, szakértői javítás nélkül a megoldás TEMPEST garanciája megszűnik, a kiadott rendszerengedély érvényét veszti.

RENDEZVÉNYEK INFORMÁCIÓBIZTONSÁGA

A napi élet nem csak az állandó elektronikus minősített adatkezelő képességekre támaszkodik. A bemutatók, konferenciák és egyéb rendezvények gyakran eseti jelleggel kialakított híradó-informatikai infrastruktúrára támaszkodnak rövid időtartalomra szervezettek, a fizikai biztonsági rendszabályokat zömében az élőerős megoldások képezik.

A minősített elektronikus adatkezelést tartalmazó rendezvények biztonsági követelményeinek meghatározásához szükséges minimum követelmények:

- a rendezvényért felelős szervezet azonosítása, az információbiztonsági feladatokért felelős személyek kijelölése;
- a kezelt adatok minősítési szintjének és a megismerésre (részvételre jogosult személyek, felhatalmazók) körének azonosítása;
- a helyszín, adatkezelési igények és időpontok azonosítása.

Rendezvény előtti feladatok

1. A résztvevői számára előzetes tájékoztatást kell adni a részvétellel kapcsolatosan:
   a) a rendezvény adatkezelési szintje;
   b) a személyi biztonsági követelményekről, a megküldendő adatokról (azonosításhoz szükséges adatok, személyi biztonság tanúsítvány, felhatalmazás);
   c) a helyszínen alkalmazott információvédelmi rendszabályokról, kommunikációs lehetőségekről, saját eszköz használatának lehetőségéről;
   d) az adathordozók, eszközök biztonságos tárolási lehetőségről.
2. A helyszín kijelölése, az adminisztratív zónák, biztonsági területek és nyilvánosan látogatható területek, ki és belépési pontok kijelölése, a fizikai biztonsághoz szükséges rendszabályok kialakítása (belépőkártyák, névsorok és azonosítás rendje, élőerős és technikai védelem), igény esetén kezelőpont kialakítása az ehhez szükséges személyi és tárgyi feltételekkel.
3. A híradó-informatikai rendszerek, eszközök telepítésének előkészítése (beleértve az estlegesen szükséges hatósági ügyintézés feladatait).

[16] Gyári számmal azonosított, részelemeket, kábeleket azonosító, Nemzeti Biztonsági Felügyelet által elismert, gyártó vagy feljogosított szerviz által kiállított dokumentum, mely sértetlen záró címkékkel együtt érvényes.

4. A rendezvény biztosításáért felelős üzemeltető és biztonságért felelős állomány felkészítése.
5. A biztosítási terv elkészítése és jóváhagyatása a rendezvényért felelős szervezet vezetőjével.
6. Közvetlen felkészülési feladatként a helyszín lezárása, biztonsági ellenőrzése, a fizikai biztonsági rendszabályok életbe léptetése, a rendezvényhez szükséges berendezések, szolgáltatások telepítése és a folyamatos biztonsági felügyelet biztosítása a rendezvény befejezéséig.

A rendezvény alatti információbiztonsági feladatok

1. A rendezvény résztvevőit a helyi sajátosságoknak megfelelően kialakított írásbeli vagy szóbeli tájékoztatásban értesíteni kell:
   a) a rendezvény helyszíneivel kapcsolatos információvédelmi rendszabályokról, a meghibásodások, incidensek kezelésének rendjéről, a helyi biztonsági menedzsment elérési lehetőségeiről;
   b) az alkalmazott korlátozásokról vagy tiltásokról (mobiltelefon használat, biztonsági terület lezárása);
   c) a rendező szervezet által nyújtott szolgáltatásokról és azok igénybevételének rendjéről (minősített adat tárolás, védett és nyílt kommunikációs lehetőségek, sokszorosítás, megsemmisítési lehetőség, saját eszköz használatával kapcsolatos lehetőségek és korlátozások).
2. A meghatározott szolgáltatások biztosítása a biztonsági felügyeleti feladatok ellátása, az egyedi esetek kezelése.
3. A résztvevők számára szükség esetén biztosítani kell az adathordozók, hordozható eszközök megbízható őrzését:
   a) átviteli elismervény alapján;
   b) személyi azonosítás esetén;
   c) az átvett anyagok jelölésével.
4. A rendezvényen a tartalék, vagy használaton kívüli eszközöket elkülönítve, nyilvántartva és a hozzáférést szabályozva kell tárolni.
5. A rendezvény szüneteiben az elektronikus adatkezelő eszközök és adatok biztonsága érdekében:
   a) a nem használt helyiségeket zárva vagy felügyelet alatt kell tartani, vagy
   b) az eszközöket, adathordozókat erre a célra kijelölt helyiségben kell őrizni.
   c) A rendezvényen rendszabályokat kell foganatosítani a felügyelet nélkül hagyott eszközök, adathordozók ellenőrzésére és begyűjtésére.

A rendezvény utáni információbiztonsági feladatok

A rendezvény után elsődleges feladat az ideiglenes szolgáltatások megszüntetése, az adatok tárolásba helyezése vagy megsemmisítése.

Az eredeti helyzet helyreállítása tartalmazza a teljes környezet biztonsági ellenőrzését az elhagyott eszközök, adathordozók begyűjtése, vagy rendellenességre utaló jelek felkutatása érdekében.

ÖSSZEFOGLALÁS

Összefoglalásként megállapítható, hogy a híradó-informatikai rendszerek, szolgáltatások elektronikus információbiztonsága összetett, más szakterületekkel történő együttműködésen alapuló, üzemeltetés rendjébe illesztett folyamatok eredménye.

A katonai műveletek információs támogatásához szükséges műveleti és vezetési rendszer technikai alapját képező MH Kormányzati Célú Elkülönült Hírközlő Hálózat fejlődése a szolgáltatások integrálása irányába mozdul el, kiegészülve a nem centralizálható, vagy külső szolgáltatókkal történő együttműködési képességekkel.

Közigazgatási szinten a kor színvonalának megfelelő vezetési és irányítási képességek nem nélkülözhetik a bemutatott követelmények szerinti hálózati szolgáltatások kialakítását és fenntartását. Ugyanígy elképzelhetetlen, hogy a nemzeti minősített elektronikus adatkezelésre feljogosított tartomány (domain) ne rendelkezzen nemzetközi szintű összekapcsolásokkal, adatcsere szolgáltatási lehetőségekkel.

A főbb vonalakban vázolt, nem részletezett elektronikus információvédelmi keretrendszer bemutatása remélhetően építik a biztonsági vezetők és egyéb vezetők szakterületi képviselők ismereteit, támogatják szükséges szintű biztonsági tudatosság kialakulását és fejlődését.

Utolsó gondolatként szükség van annak kifejezésére, hogy egy szakmai kultúra kialakítása és fejlesztése nem képzelhető el szervezett képzési és továbbképzési rendszer nélkül. A Magyar Honvédség szervezeteinél az elektronikus minősített adatkezelés kialakításához és üzemeltetéséhez szükséges, a fenti ismereteket átadó tanfolyamok rendelkezésre állnak, biztosítva az alapvető ismeretek elsajátításának lehetőségét.

A további műszaki, vagy stratégiai szintű ismeretek elsajátítása egy-két tanfolyamon keresztül nem garantálható. Az alapismeretek megléte segíti a szakterületet gyakorlókat abban, hogy ne tekintsenek hitelesnek a napjainkban tapasztalható néhány hetes – hónapos tanfolyamokat, ahol nem történik meg a fenti kérdések elektronikus minősített adatkezelésre specializált tárgyalása.

Felhasznált irodalom

[1] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 59. §.

[2] A Honvéd Vezérkar híradó, informatikai és információvédelmi csoportfőnökének 9/2012. (HK 14.) HIICSF szakutasítása a Minősített Elektronikus Adatkezelő Rendszer Üzemeltetés Biztonsági Szabályzatára vonatkozó általános követelményekről

[3] 75/2013. (XII. 5.) HM utasítás a Magyar honvédség Rejtjelszabályzat kiadásáról, 5. §.

[4] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 8. §.

[5] 39/2014. (05. 30.) HM utasítás a Magyar Honvédség Informatikai Szabályzatának kiadásáról, 1. sz. melléklet, 8. 4. fejezet.

[6] A Honvéd Vezérkar híradó, informatikai és információvédelmi csoportfőnökének 10/2012. (HK 14.) HIICSF szakutasítása a Minősített Elektronikus Adatkezelő Rendszer ellenőrzésére vonatkozó általános követelményekről

[7] A Honvéd Vezérkar híradó, informatikai és információvédelmi csoportfőnökének 18/2014. (HK 8.) HVK HIICSF szakutasítása a Magyar Honvédség rejtjelző szakiratkezeléséről