HADMÉRNÖK

V. Évfolyam 3. szám - 2010. szeptember

Kassai Károly
kassai.karoly@hm.gov.hu

A MOBIL KOMMUNIKÁCIÓS ESZKÖZÖK HASZNÁLATÁNAK ÉS VÉDELMI RENDSZABÁLYAINAK SZABÁLYOZÁSA

Absztrakt

A honvédelmi szervezetek tevékenysége nem képzelhető el hatékonyan mobil kommunikációs megoldások alkalmazása nélkül. A vezetési és irányítási folyamatok, az üzemeltetési környezet, kommunikációs eszközök, különböző felhasználói igények, a kezelt adatok fontossága és bizalmassága olyan kulcsfontosságú tényezők, melyek jelzik ennek a kommunikációs formának – és szabályozásának – összetettségét.
Az említett tényezők mellett a rohamosan fejlődő technológia által biztosított szolgáltatások folyamatosan változó fenyegetés és sebezhetőségi hatások alatt állnak.
A honvédelmi tárca információ biztonságpolitika meghatározza az elektronikus adatkezelő rendszerek biztonsági felügyeletét, így célszerű egy rugalmas és strukturált szabályozást kialakítani a honvédelmi szervezetek széles körű tevékenységének biztonságos kommunikációs támogatása érdekében.

The activity of military units and different supporting organisations cannot be effective without the implementation of mobile communication solutions. The communication and controlling processes, the operating environments, the communication equipments, the different user requirements, and the importance and sensitivity of handled information are key factors which sign the complexity of this communication and its regularisation.
Besides the mentioned factors the new services provided by emerging technology have some impacts from the continuously changing known and hidden threats and vulnerabilities.
The Security Policy of Ministry of Defence requires security control of CIS's so it may be useful to create a flexible and structured set of controls for secure mobile communication supporting the wide scale of activities at military organisations.

Kulcsszavak: *biztonságpolitika, információbiztonság, információvédelem, informatika, mobil kommunikáció - security policy, information security, information protection, IT, mobile communication.*

BEVEZETÉS

A mobil kommunikációs eszközök alkalmazása egyre nagyobb szerepet játszik a honvédelmi szervezetek életében. Szolgáltatási lehetőségeinek sokszínűsége miatt a hagyományos szakterületi elkülönülés alapján nehéz eldönteni, hogy mobil IT szolgáltatáshoz vagy híradáshoz kell sorolni a mobil kommunikációs lehetőségek alkalmazását, ami már többet jelent mobiltelefonnál (korábban rádiótelefon), így helyesebb a címben fogalmazott „mobil kommunikációs eszköz" kifejezés használata.

Ezzel a kérdéssel részben foglalkozik a mobil telefonokkal való ellátásra vonatkozó utasítás [1.], minősített adatkezelés esetén a jogszabályban rögzített helyi szabályozási (biztonsági szabályzat) kötelezettség [2.][3.], de ezen kívül a honvédelmi tárcánál kifejezetten erre a területre vonatkozó specifikus szabályozás nincs. Kis irodalomkutatás után kijelenthető, hogy a közigazgatási szervezetekre vonatkozó kötelező hatályú központi követelmény (jogszabály) ebben a témában nem azonosítható.

A területre vonatkozó szabályozást célszerű a nemzetközi szabványokhoz igazítva kialakítani, melynek elemei a biztonság menedzseléséről szóló szabványok [4.][5.], és az ezek alapján készült nemzeti ajánlás [6.] vonatkozó részei. A szabályozás kialakításánál segítséget nyújtanak még a bevált gyakorlat (best practice) körébe tartozó kiadványok [7.][8.].

A fenti támogatás mellett a szabályozási alapot a biztonságpolitika adja, melynek általános irányelveit és követelményeit [9.] a mobil kommunikációs eszközök esetében is érvényesíteni kell.

A továbbiakban azon szempontok bemutatása látható, ami a felső szintű, keret jellegű szabályozás lényégét kifejezi. Az ehhez szükséges technológiától függő paramétereket, központilag meghatározandó műszaki részleteket szűkebb szabályozási hatályú belső rendelkezésben célszerű rögzíteni.

1. A SZABÁLYOZÁSI KÖR AZONOSÍTÁSA

A mobil kommunikációs eszközök használatával kapcsolatos alapelveket meghatározó szabályozásban a honvédelmi szervezeteknél a mobil eszközökkel történő kommunikáció és adatkezelés biztonságához szükséges irányelvek, általános követelmények kereteit kell meghatározni. A szolgálati mobil kommunikációs eszközöket a honvédelmi tárca információ biztonságpolitikában meghatározott biztonsági cél-, és az elérésére vonatkozó követelményeknek megfelelően kell alkalmazásba venni, konfigurálni, működtetni és felügyelni. A magántulajdonú mobil kommunikációs eszközök alkalmazását ugyanezen általános követelmények figyelembe vételével lehet engedélyezni.

A honvédelmi szervezeteknél biztonsági menedzsment eljárásokat, ellenőrzési feladatokat kell kialakítani a mobil kommunikációs eszközök felett. A védelmi rendszabályokat *a szolgálati mobil kommunikációs eszköz teljes életútján keresztül fenn kell tartani*. A mobil kommunikációs eszközök alkalmazásának engedélyezését, korlátozást, vagy tiltását az adott szervezet vezetőjének (vagy az általa megbízott személynek) a hatáskörében kell rendezni.

A honvédelmi szervezetek belső rendelkezéseiben *a helyi szabályozást a központi, keret jellegű követelményekkel összhangban kell kialakítani*. A külföldön szolgálatot teljesítő katonai szervezetek információvédelmi rendszabályait az említett központi-, valamint az illetékes elöljáró követelményei alapján kell kialakítani. A honvédelmi szervezetekkel

szerződéses kapcsolatban álló személyek esetében a központi követelmények érvényesüléséhez szükséges rendszabályok kialakításáról és fenntartásáról a honvédelmi szervezet vezetőjének kell gondoskodnia.

Ezen általános lehatárolás mellett szükség van meghatározására, hogy ehhez a kérdéshez kell sorolni *minden olyan eszközt, ami a mobil távközlési szolgáltatás mellett adatkezelésre (rögzítés, fájl kezelés) képes*. Nem tartozik a szabályozási körbe az EDR (Egységes Digitális Rendszer) eszközök igénybevétele, melynek üzemeltetési és biztonsági szabályozása önálló jogszabályban rögzített követelmények szerint történik.

2. SZABÁLYOZÁSI KÖVETELMÉNYEK

A honvédelmi szervezet vezetőjének a helyi sajátosságoknak és a végzett tevékenységnek megfelelően szabályoznia kell a mobil kommunikációs eszközökkel történő elektronikus adatkezelést. A szabályozás során azonosítani kell:

- a szolgálati mobil kommunikációs eszközhöz kötött, vagy magántulajdonú eszközzel is végezhető elektronikus adatkezelő műveleteket;
- a mobil kommunikációs eszköz használata szempontjából tiltott helyeket;
- a munkavégzés vagy rendezvények alatt alkalmazandó állandó vagy ideiglenes korlátozásokat, tiltásokat;
- azokat a szolgálati mobil kommunikációs eszközöket, melyek magántulajdonú kommunikációra vagy adatkezelésre nem alkalmazhatók;
- a mobil kommunikációs eszközök használatára vonatkozó rendszabályok betartása érdekében alkalmazott eljárásokat;
- a szolgálati kommunikációs eszközökkel kapcsolatos biztonsági incidensek megoldására szolgáló eljárásokat.

A mobil kommunikációs eszközök alkalmazásának engedélyezésekor figyelembe kell venni:

- az eszközök kommunikációs és adatkezelő képességeit;
- az engedélyezett mobil kommunikációs eszköz használat munkavégzésre irányuló hatását;
- az eszközök elvesztéséből, illetéktelen kezekbe jutásából adódó információs fenyegetéseket.

A fenti követelmények bonyolultnak tűnnek, de a valóság ennél egy kicsit egyszerűbb. A szervezet működéséhez szükséges *információs folyamatokat mindenképpen szabályozni kell*, az tehát nem lehet újság, hogy ebbe az is beleértendő, hogy *mit lehet, és mit nem lehet mobil kommunikációs eszközzel végezni*. Ugyanígy nem lehet meglepő az sem, hogy *a szervezet szabályozza azt a lehetőséget, hogy az egyre korszerűbb eszközök esetében fokozottan jelentkező információs fenyegetések ellensúlyozására milyen magántulajdonú eszközökre vonatkozó korlátozást vezet be*.

Fontos kérdés annak tisztázása is, hogy a mobil kommunikációs eszközzel történő ellátásért felelős vezetőnek *szabályoznia kell a szolgálati mobil kommunikációs eszköz fenntartásával kapcsolatos feladatokat is*. Ez azt jelenti, hogy a korábban csak kiosztott és használt eszköz napjainkban már gyakran *szoftveres karbantartást igényel, melyet bonyolultságtól függően szükséges szakértői szinten támogatni*.

A továbbiakban azok az általánosan megfogalmazható kontrollok olvashatók, melyek áttekintésével, helyszínhez és munkavégzéshez történő igazítással a szabályozási elemek pontosan kialakíthatók.

3. ÁLTALÁNOS ALKALMAZÁSI KÖVETELMÉNYEK

A szolgálati mobil kommunikációs eszköz alapesetben csak szolgálati kommunikációra és adatkezelésre alkalmazható. Általános szabályként célszerű kitűzni, hogy *szolgálati eszköz kölcsön nem adható, illetve más személy részére a hozzáférés nem biztosítható*; a kivételeket átgondoltan, pontosan meg kell határozni. A szolgálati mobil kommunikációs eszközzel az előfizetői szolgáltatáson keresztül történő egyéb szolgáltatás fizetését vagy megrendelését tiltani kell (pl. autópálya matrica, adományozás). Meg kell vizsgálni, hogy melyek azok az esetek, amikor a szolgálati mobil kommunikációs eszköz szolgáltatásai magántulajdonú eszközre nem irányítható át (illetve egyes esetekben célszerű megfontolni az általános tiltást). Magántulajdonú eszköz szolgáltatása szolgálati mobil kommunikációs eszközre abban az esetben irányítható át, ha:

- a felhasználó munkavégzése közben a mobil kommunikációs eszköz használat nem tiltott;
- az adott szolgálati mobil kommunikációs eszközön a magán célú kommunikáció vagy adatkezelés nem tiltott.

Általános, mindenki által érthető követelménynek kell megjelennie arra vonatkozóan, hogy *a szolgálati mobil kommunikációs eszköz, az eszközön tárolt adatok az üzemeltetésért felelős honvédelmi szervezet vagy a felhasználó szerint illetékes munkaadó honvédelmi szervezet vezetője által meghatározottak szerint ellenőrizhető*. Ez a követelmény a közhiedelemmel ellentétben nem zavarhatja a személyes adatok védelmét, mert a szolgálati célú adat, vagy eszköz egyértelműen szervezeti célt szolgál, így az ezzel kapcsolatos híváslisták, egyéb üzemeltetési adatok szintén a szolgálati tevékenység részét képezik. Az esetleges engedélyezett magán használat és a szolgálati használatból adódó keveredés (az a tény, hogy az ellenőrzés személyes adatokat is feltárhat) könnyen kivédhető, mert a magáncélú használat nem kötelező, csak engedélyezhető (tehát csak lehetőség), így egyéni aggály esetén a védelem egyszerű: kerülni kell a magáncélú használatot.

A szolgálati mobil kommunikációs eszköz csak az üzemeltető által rendelkezésre bocsátott konfigurációban, kiegészítő elemekkel és alkalmazásokkal üzemeltethető. A felhasználónak tilos:

- az eszköz felügyelet nélkül hagyása;
- az eszköz vagy kiegészítőjének kezelői szintű szétszerelését meghaladó mértékű szétszerelése, vagy kiegészítése;
- az előfizetői kártyát vagy memóriát más eszközben alkalmazni;
- magántulajdonú kártyát vagy memóriát az eszközbe helyezni vagy arról adatot feltölteni;
- olyan üzemmódot vagy beállítást alkalmazni, melynek eredményeképpen honvédelmi vezetékes vagy vezeték nélküli kommunikációs rendszer internethez, más nyilvános hálózathoz, esetleg magáncélú hálózathoz csatlakozik.
- az eszköz alkalmazása során a meghatározott védelmi rendszabályok megkerülése vagy kiiktatása.

Szolgálati mobil kommunikációs eszközzel magáncélú kommunikáció vagy adatkezelés csak az engedélyezett mértékben és formában végezhető *a szolgálati cél elsődlegességének figyelembe vételével*. A felhasználónak tudomásul kell vennie, hogy:

- a felhasználó a felhasználói engedély korlátozása vagy visszavonása esetén a magántulajdonát képező adatot azonnal köteles törölni vagy eltávolítani, mely tevékenység nem akadályozhatja a szolgálati mobil kommunikációs eszköz használatát;
- az engedélyezett magáncélú adatokban keletkezett sérülésért vagy adatvesztésért az üzemeltető nem vállal felelősséget.

Szolgálati tevékenységhez szükséges kommunikáció vagy adatkezelés magántulajdonú, vagy más szervezet tulajdonában lévő eszközzel csak engedéllyel végezhető.

Szolgálati mobil kommunikációs eszköznél automatikus hang vagy adatszolgáltatás beállítása esetén csak olyan adat alkalmazható, *melynek a hívó fél tudomására jutása nem sért szolgálati érdeket*.

Szolgálati kommunikáció vagy adatkezelés más szervezet tulajdonában lévő eszközzel csak az alábbi feltételek együttes fennállása esetén végezhető:

- szolgálati mobil kommunikációs eszköz hiánya;
- a kommunikáció vagy adatkezelés során az adatok biztonsági osztályához rendelt védelmi rendszabályok biztosíthatók;
- a szolgáltatás megszűnése esetén a hívásadatok, felhasználói adatok törlése és szükség szerint mentése biztosított.

A felhasználónak a szolgálati mobil kommunikációs eszköz felügyelet alatt tartásával biztosítania kell a kezelt adatok bizalmasságát-, az eszköz eltulajdonításának megakadályozását-, az eszköz, illetve az eszközbeállítások módosításának elkerülését-, a nem kívánt szolgáltatások aktivizálásának megakadályozását-, és a szolgáltatások alkalmazásával kapcsolatos visszaélések elkerülését.

Az alkalmazással kapcsolatos felhasználói és biztonsági ismereteket a honvédelmi szervezet képzési rendje szerinti *időszakonként oktatni kell*. Az oktatás más foglalkozásokkal összevonható. A távollévők számára pótfoglalkozást kell szervezni.

A fenti szabályozási elemek *nem tartalmaznak végrehajthatatlan követelményeket, esetleg korábbi felhasználói szokásokkal kerülhetnek összeütközésbe*. A szabályozás vezérfonala *a szolgálati tevékenységhez szükséges kommunikáció és adatkezelés elsődlegességének biztosítása, illetve a magán és a szolgálati használat (illetve magán és szolgálati adat) elkülöníthetőségének biztosítása*.

4. ÁLTALÁNOS VÉDELMI RENDSZABÁLYOK

Az előző fejezetben meghatározott, inkább az alkalmazásra vonatkozó szabályozás mellett szükség van az általánosan megfogalmazható rendszabályok azonosítására, melynek specifikálásával már eszköz és szolgáltatás függően részletes védelmi rendszabályok dolgozhatók ki (az itt azonosított, nem teljes körű lehetőségeket szükség esetén eszközcsaládhoz vagy szolgáltatáshoz illesztve tovább lehet pontosítani és tartalom függvényében meghatározott szintű belső rendelkezésben kiadni).

A felhasználónak a szolgálati mobil kommunikációs eszközt és a szolgáltatás igénybevételére jogosító SIM kártyát, valamint az adatok tárolására alkalmas memória kártyát azonosító kód használatával kell védenie az illetéktelen hozzáféréstől. Ennek érdekében az eszköz használatbavételekor a felhasználónak meg kell változtatnia a rendelkezésére bocsátott kódokat. A felhasználó nem használhat a szolgálati mobil kommunikációs eszközhöz és egyéb számítógépéhez megegyező azonosító kódot. Jelszavas védelmi lehetőséggel rendelkező memória kártyákat csak az azonosítási funkció aktivizálásával lehet üzemeltetni.

Az egyes alkalmazások véletlenszerű elindításának megakadályozása érdekében a felhasználók kötelesek billentyűzárat (manuális vagy automatikus) használni.

Azon szolgálati eszközök esetében, ahol adatvesztés nem engedhető meg, *rendszeres időközönként az eszköz hardver és szoftver lehetőségei szerint kialakított mentést kell végezni*. A mentési eljárást szabályozni kell. Az adatmentés megvalósítható:

- számítógéppel történő mentéssel vagy szinkronizálással;
- adathordozóra történő mentéssel;
- nyomtatással.

Mobil kommunikációs eszköz hálózati számítógéppel történő összekapcsolása, illetve szinkronizálása csak:

- engedélyezett program alkalmazásával, arra kijelölt számítógéppel történhet;
- célszerűen csak naptár, jegyzet adatokra és SMS-re korlátozódjon (az adatok másolását, illetve tárolását egyedi esetekre külön-külön vizsgálni kell, és csak célhoz kötötten lehet engedélyezni).

A teljes címtárral, adatbázissal történő szinkronizálást tiltani kell. *A mobil kommunikációs eszköz szinkronizálásához szükséges telepítéseket, biztonsági beállításokat csak az arra kijelölt, kiképzett rendszeradminisztrátor végezheti*. Az adatmentésre feljogosított felhasználókat az adatmentéssel kapcsolatos műveletekre ki kell képezni.

Memóriakártyára, vagy más adathordozóra történő mentés esetén a mentett adatokat a szolgálati mobil kommunikációs eszköztől elkülönítve, a biztonsági osztálynak megfelelően kell tárolni, illetve védeni.

A szolgálati mobil kommunikációs eszközökön *alkalmazni kell a biztosított logikai védelmi alkalmazásokat, magasabb biztonsági osztályú adat esetén az eszköz sajátosságainak megfelelő kiegészítő szoftveres védelmet kell alkalmazni*.

A memóriakártyákat a használatból történő kivonáskor a visszaállítás és elemzés megakadályozása érdekében az adatok bizalmasságával arányos törlési eljárásokat kell alkalmazni. *Törlésre csak engedélyezett eljárások alkalmazhatók*, ennek hiányában fizikai megsemmisítést kell alkalmazni.

A csatolt fájlokban, üzenetekben lévő rosszindulatú programok elleni védelem érdekében *az ismeretlen forrásból eredő üzenetek esetén a vírusvédelmi rendszabályok szerint kell eljárni*. Vett üzenetek esetében a végrehajtandó utasítások aktivizálása a felhasználó által tilos.

A mobil kommunikációs eszközök által kezdeményezett ismeretlen program telepítésének engedélyezése tilos.

Az ismeretlen forrás felől érkező vezeték nélküli interfész csatlakozási kérelmet tilos engedélyezni. Nem azonosított, nem megbízható forrásból származó adat letöltése és telepítése tilos.

Az automatikus adatátviteli szolgáltatásokat a szolgálati mobil kommunikációs eszközökön ki kell kapcsolni.

A vezeték nélküli interfészeket alaphelyzetben kikapcsolt állapotban kell tartani és csak a szükséges időtartamra lehet bekapcsolni. A vezeték nélküli interfészen keresztüli láthatóságot alaphelyzetben le kell tiltani. Amennyiben az eszköz típusa lehetővé teszi, olyan beállítást kell alkalmazni, ami jelzi a vezeték nélküli interfészen keresztül érkező csatlakozási kérelmet. A vezeték nélküli interfészen keresztüli kommunikáció engedélyezése során az eszköz rendelkezésre álló jelszavas azonosítási szolgáltatását alkalmazni kell.

A vezeték nélküli interfészen keresztüli kommunikáció során kerülni kell azokat a nyilvános helyeket, ahol feltételezhető az adatcsere más eszköz által történő vétele. Amennyiben az eszköz vezeték nélküli interfészének energia szintje szabályozható, a lehető legkevesebb energiaszintet kell alkalmazni.

Az ellopott, vagy elvesztett szolgálati mobil kommunikációs eszköz jelentésére és a szükséges azonnali teendők meghatározására a honvédelmi szervezeteknél eljárást kell kialakítani.

Amennyiben a szolgálai mobil kommunikációs eszköz lehetővé teszi, *alkalmazni kell az eszköz szolgáltatásból történő kizárására, zárolására vagy tartalomtörlésre biztosított távoli elérési szolgáltatásokat*. Az ilyen programok telepítése előtt teszteléssel meg kell, győződni a szolgáltatás működőképességéről, illetve arról, hogy a szolgáltatás nem megkerülhető.

A szükségtelen beállításokat a konfigurációs beállításokon keresztül le kell tiltani, vagy amennyiben az eszköz tulajdonságai lehetővé teszik, el kell azokat távolítani. A szolgáltatók által rendelkezésre bocsátott kiegészítő szolgáltatások engedélyezése előtt *meg kell vizsgálni, hogy a változás milyen új fenyegetést és sebezhetőséget hordoz, és azok ellensúlyozására milyen védelmi rendszabályt kell alkalmazni*.

Amennyiben a szolgálati feladatok ellátása nem kíván internet hozzáférést, a szolgálati mobil kommunikációs eszközre csak hang és SMS szolgáltatást célszerű engedélyezni.

5. SPECIÁLIS ALKALMAZÁSI KÖVETELMÉNYEK

I. vagy II. osztályú biztonsági területre általános esetben mobil kommunikációs eszköz nem vihető be. A korlátozást a biztonsági területre történő belépés előtt közölni kell a látogató személyekkel.

Amennyiben szolgálati feladatok ellátása célhoz kötötten biztonsági területen mobil szolgálati kommunikációs eszköz bevitelét vagy alkalmazását követeli, az eszköz alkalmazásával kapcsolatos részletes szabályokat ki kell dolgozni:

- a biztonsági területre vonatkozó biztonsági szabályzatban;
- a biztonsági területen belül alkalmazott elektronikus adatkezelő rendszerek rendszer-specifikus biztonsági dokumentumaiban.

A minősített adatokat is feldolgozó rendezvényen a mobil kommunikációs eszközök alkalmazásával kapcsolatban szabályozni kell:

- a mobil kommunikációs eszköz használatára engedélyezett területeket;
- a mobil kommunikációs eszköz beviteli tilalma esetén a tárolásra, őrzésre, visszaszolgáltatásra vonatkozó eljárást.

Azon biztonsági területek, adminisztratív zónák, vagy egyéb helyek esetében, ahová mobil kommunikációs eszköz nem vihető be, a rendszabályt meghatározónak gondoskodnia kell:

- a rendszabály látogatók által történő megismeréséről;
- az eszközök biztonságos tárolásáról.

Amennyiben a rendezvényre vonatkozó biztonsági követelmény technikai védelmet is meghatároz, a zavarásra, detektálásra vonatkozó eljárásokat:

- célhoz kötötten, a szükséges mértékre korlátozva-,
- a rendezvényen kívüli kommunikációs szükségletek figyelembe vételével kell kialakítani.

Szolgálati mobil kommunikációs eszköz honvédelmi szervezet vagy más szervezet tagja számára történő kiutalása, biztosítása *csak célhoz, feladathoz kötötten szolgálati célból történhet*. Kiutalásra csak olyan eszköz kerülhet, melyből a korábbi felhasználás során keletkezett napló, forgalmazási, cím, vagy tárolt felhasználói adatok törlése megtörtént.

Minősített adat mobil kommunikációs eszközzel történő kezelése *csak az illetékes hatóság által engedélyezett eszközzel és védelmi megoldások alkalmazásával történhet.*

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A mobil kommunikációs eszközök használatának alkalmazása és felügyelete a fentiekben bemutatott keretrendszer szerint nem túl bonyolultan szabályozható.

Az ajánlott szabályozási elemek pontosítása alapján a honvédelmi szervezeteknél első lépésként annak meghatározására van szükség, hogy *mely helyszíneken van szükség és milyen mértékű korlátozás bevezetésére*, illetve *annak meghatározására, hogy a szolgálati adatok védelme érdekében milyen rendszabályok alkalmazása szükséges (pl. elkülönítés vagy korlátozás).*

Az üzemeltetési helyszínek mellett egyedileg azonosítani kell azokat az eszközöket, melyek esetében szigorúbb rendszabályokra van szükség. Belátható, hogy egy ügyeleti szolgálatot támogató eszköz esetében más eljárásokat kell életbe léptetni, mint a beosztáshoz köthető normál alkalmazás esetében.

Kulcsfontosságú a tájékoztatás és a pontos, félreérthetetlen megfogalmazás, és annak megértetése, hogy *a személyes adatok védelmére hivatkozva nem lehet a szolgálati adatok védelmét háttérbe szorítani, vagy mellékesként kezelni.*

A téma általános szabályozása során az egyik legfontosabb kérdés, hogy a túl szűkre szabott szabályozás, vagy egy technológiához, megoldáshoz köthető követelmény nagyon könnyen alkalmazási, vagy üzemeltetés-támogatási problémákat okozhat. Formailag a bemutatott keret jellegű szabályozás a szükséges pontosítások és egyeztetések után történhet miniszteri utasítással hatályba léptetett szabályzat részeként, vagy önállóan kiadott miniszteri utasítással. E mellett szükség van az üzemeltetés szabályozásának áttekintésére is, valamint

célszerűnek látszik egy lépéssel tovább haladva a különböző képességekkel rendelkező hordozható számítógépekkel kapcsolatos eljárásrendet is pontosítani, a helyi szabályozások központi támogatása érdekében.

Egy ilyen szabályozási keretrendszer nem tekinthető tökéletesnek és véglegesnek, így *az időszakos felülvizsgálat, illetve új szolgáltatások, technikai megoldások megjelenése esetén szükség van a felülvizsgálatra és a pontosításra*. Az esetleges hiányosságok lefedésére irányuló adatgyűjtés támaszkodhat a szakmai továbbképzésekre, a helyi képzésekre, vagy a tanfolyam rendszerű képzésekre.

FELHASZNÁLT IRODALOM

[1.] 64/2007 (HK 12.) HM utasítás 64/2007. (HK 12.) HM utasítás a szolgálati rádiótelefon-ellátás és használat szabályairól, 3. §.

[2.] 90/2010. (III. 26.) Korm. rendelet a Nemzet Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről, 58-59. §.

[3.] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 59. §.

[4.] MSZ ISO/IEC 27001:2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények, A melléklet, A 10. 8. 1. p. és 11.7.1. p

[5.] MSZ ISO/IEC 17799: 2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002:2005), 10.8.1. p és 11. 7. 1. p.

[6.] Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszer (MIBIK), Informatikai Biztonsági Követelmények v 1.1. 2008, 10.8.1. p és 11. 7. 1. p.

[7.] The Standard of Good Practice for Information Security; Information Security Forum (ISF), 2007, UE4. 4.2. p, SM 5.2. 5.2.2. p. SM 5.3. 5. 3. 6. p.

[8.] Guidelines on Cell Phone and PDA Security (SP 800-124), National Institute of Standards and Technology (NIST), 2008

[9.] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról