A ZMNE KLHTK TUDOMÁNYOS FOLYÓIRATA BIZTONSÁG ÉS RENDVÉDELEM

HADTUDOMÁNYI SZEMLE

Budapest, 2010.
3. évfolyam 3. szám

KASSAI Károly

AZ ELEKTRONIKUS ADATKEZELÉS SORÁN SZÜKSÉGES SZEMÉLYI BIZTONSÁG KÉRDÉSEI

PERSONNEL SECURITY ISSUES OF ELECTRONIC INFORMATION HANDLING DURING LIFE CYCLE

Az elektronikus adatkezelő rendszerek biztonságának gyorsan változó szempontjai mellett *a humán tényező* az, ami az alkalmazott technológia, az adatok fontossága és egyéb mérlegelési szempontok mellett mindig kiemelt szerepet játszik.

A cikk célja a fontosabb személyi biztonsági tényezők azonosítása, ezáltal a katonai elektronikus *adatkezelés szabályozásához szüksége folyamatok támogatása* az életciklus elméletnek megfelelően.

Beside the fast changes of security of CIS *the human factor has key* role independently from the implemented technology, the importance of information and other points of view.

The goal of this article is the identification of the important elements of personnel security and thus *supporting processes needed for regularization of information handling in CIS*, according to the life cycle theory.

BEVEZETÉS

Az elektronikus adatkezelő rendszerek használata és üzemeltetése a feljogosítás előtti, az adatkezelés alatti és a feljogosítás megszüntetése utáni szakaszokra bontható.

Ennek megfelelően a személyi biztonság kérdései is három részre tagolhatók:

- az adatokhoz, adatkezelő rendszerekhez történő hozzáférésre feljogosított személyek kiválasztása, a munkakörök meghatározása;
- az adatkezelés, a beosztások változása során az időszakosan visszatérő jellegű biztonsági tájékoztatások, képzések és továbbképzések a felhasználók, a rendszerek üzemeltető és biztonsági feladatokat ellátó állománya számára, valamint a változások nyomon követése és felügyelete;
- az adatkezelési jogosultság megszűnése esetén a hozzáférési jogosultságok törlése.

A jogszabályok a személyi biztonsággal kapcsolatosan általános követelményeket határoznak meg. A minősített adatkezelést szabályozó törvény az adatkezelésre vonatkozó adminisztratív rendszabályok mellett például a képzést és a továbbképzést egyedül a Nemzeti Biztonsági Felügyelet feladatainál említi, részletesebb követelmények nélkül [1.]. Ugyanez tapasztalható a minősített NATO, EU és egyéb külföldi adatkezelést szabályozó 2010. március 31-ig érvényes kormányrendelet esetében is.

Emiatt célszerűnek látszik a személyi biztonság kérdéseinek pontosabb vizsgálata. Az életciklus szerinti megközelítés már megjelenik a nemzeti szabványokban [2.], a jelenleg érvényes nemzeti ajánlás is ezt a szemléletet tükrözi [4.], illetve az informatikai szolgáltatások szabályozása területén is megfigyelhető [5.]. Az említett források feldolgozása a honvédelmi szervezetek információvédelmi munkáját támogathatja, így jelen cikk jó példája a szabványok, a civil ajánlások alkalmazhatóságának vizsgálatára is.

A ZMNE KLHTK TUDOMÁNYOS FOLYÓIRATA BIZTONSÁG ÉS RENDVÉDELEM
HADTUDOMÁNYI SZEMLE
Budapest, 2010.
3. évfolyam 3. szám

KASSAI Károly

A BEOSZTÁSBA HELYEZÉSSEL, VAGY MEGBÍZÁSSAL KAPCSOLATOS FELADATOK

Egyértelmű követelmény, hogy a honvédelmi szervezeteknél az adatkezeléshez történő feljogosítás, az elektronikus adatkezelő rendszerek üzemeltetési feladatainak ellátása csak a kezelt adatok érzékenységével arányos személyi biztonsági feltételek megléte esetén történhet. A beosztásba helyezés (vagy munkaerő-felvételi eljárás), a más beosztás mellett végzett megbízás csak a meghatározott személyügyi eljárás után történhet.

Az eljárás során vizsgálni kell a munkavégzésre tervezett személy önéletrajzát, végzettségét és a jogszabályoknak megfelelő hatósági igazolásokat. A beosztásba helyezés során olyan, a jogszabályoknak megfelelő vizsgálatokat lehet lefolytatni, melyek egyértelmű képet adnak a jelentkező információbiztonsági alkalmasságáról, különösen az üzemeltetés vagy az információvédelem szempontjából kiemelt fontosságú munkakörök esetén. Ennek során az adatvédelemre vonatkozó követelményeknek megfelelően csak olyan nyilatkozat megtétele kérhető, illetve csak olyan alkalmassági vizsgálat alkalmazható, ami nem sért személyiségi jogot, a munkaviszony szempontjából lényeges tájékoztatást nyújthat, és ahhoz az érintett írásban hozzájárult. A pályázatkor a beküldött jelentkezéseket, a csatolt iratokat a pályáztató szervezeteknek a munkakör feltöltéséhez kötötten, a szükséges védelmi rendszabály által biztosítva kell őrizniük. A bekért adatokat a felvételi eljárás befejezésekor haladéktalanul meg kell semmisíteni, vagy vissza kell szolgáltatni, amely eljárásról a pályázót értesíteni kell.

Minősített adatok kezelése esetén a munkakör ellátásához a jogszabályokban rögzített szintű kockázatmentes nemzetbiztonsági ellenőrzési eredményre van szükség. A nemzetbiztonsági ellenőrzés mellett a minősítési szintnek megfelelő személyi biztonsági tanúsítvány szükséges, amelynek kiadása a jelenlegi követelmények szerint NATO, EU adat esetében a Nemzeti Biztonsági Felügyelet, nemzeti adat esetében az adatkezelő szervezet biztonsági vezetőjének feladata.

Nemzetközi gyakorlatok, tanácskozások és egyéb rendezvények esetében a személyi biztonsági tanúsítványra vonatkozó követelmények meghatározása a minősítési szintnek megfelelően a rendező szervezet feladata. NATO, EU tagállam állampolgárainak NATO, EU KORLÁTOZOTT TERJESZTÉSŰ adathozzáférés – amennyiben a „need to know” elv megvalósul – személyi biztonsági tanúsítvány nélkül is engedélyezhető biztonsági tájékoztatás megtartása után, nyilvántartási kötelezettség mellett.

Az elektronikus adatkezelő rendszerek tervezése, fejlesztése, üzemeltetése, illetve a rendszerek biztonságához szükséges információvédelmi feladatok bizalmi munkakörnek minősülnek. Az ezzel kapcsolatos nemzetbiztonsági ellenőrzésre vonatkozó követelményeket a fontos és bizalmas munkakörök ellátására vonatkozó HM jogszabály tartalmazza. Új munkakörök kialakítása esetén az elektronikus adatkezelő rendszer tervezéséért felelős szervezetnek az információvédelmi szakirányítást támogató HM szervvel való egyeztetésre támaszkodva meg kell határoznia a munkakörre vonatkozó személyi biztonsági követelményt, amit meg kell jeleníteni a fontos és bizalmas munkakörök ellátására vonatkozó HM jogszabályban.

Az üzemeltetést végző személyek esetében az egész rendszerre, alrendszerre vonatkozó hozzáférési jogosultsággal rendelkező személyeknél a személyi biztonsági követelmények kialakításánál a minősítési szint mellett figyelembe kell venni a rendelkezésre állással kapcsolatos kockázati tényezőt, így a hozzáféréssel okozható veszélyekkel arányosan emelt szintű követelményeket kell meghatározni, illetve kiegészítő védelmi rendszabályokkal kell ellensúlyozni a véletlen vagy szándékos károkozást. Ezeket az általánostól eltérő rendszabályokat a rendszer-specifikus biztonsági dokumentumokban kell rögzíteni.

Új rendszerek kialakításakor gyakran elfelejtett, de nélkülözhetetlen feladat az üzemeltetői és az információvédelmi szakfeladatok ellátására vonatkozó képzési (továbbképzési) feladatok megjelenítése, és a kötelezően végzendő feladatok közé történő beillesztése. Egyes esetekben a nemzetbiztonsági követelmények szerinti ellenőrzéseken túl a kockázattal arányos mértékben mérlegelni kell az egyéni tulajdonságokat is (pl. felelősségtudat, terhelhetőség, koncentrálóképesség, pánik-tűrő képesség). A biztonsági szempontból kritikus informatikai és információvédelmi munkaköröket betöltő személyek esetében az alkalmasságot rendszeresen felül kell vizsgálni. Ezek azért egyre fontosabb feladatok, mert az

adatkezelő képességek az esetek nagy részében a humán tényezőn keresztül lényegesen egyszerűbben támadhatók (social engeneering). A veszélyességet növeli, hogy gondosan megtervezett akció esetén *az érintett személy nem is sejti, hogy a manipulálás áldozata, és tevékenysége a szervezeti célokkal ellentétes*.

A munkaköri leírásokban, rendszer-specifikus biztonsági dokumentumokban történő feladat-meghatározás elméletileg nem bonyolult feladat. Gyakori eset azonban az egyes munkakörökhöz tartozó *adatkezelési feladatok, felelősségi körök és jogosultságok, információvédelmi feladatok általános megfogalmazása;* vagy *a jelentési, tájékoztatási kötelezettségek hiányos fogalmazása, az események észlelése esetén követendő feladatok* vagy a *helyettesítési kérdések tisztázatlansága*.

A hozzáférési feljogosításkor *csak a munkakörhöz feltétlenül szükséges távhívási, adatkezelési vagy üzemeltetési jogosultságokat kell megadni*, ami az esetek egy részében nehezebb feladat, mint az általános hozzáférések megadása, így célszerű ezeket a folyamatokat is időszakosan áttekinteni. A problémák megelőzése érdekében új belépők esetében általános szabálynak kell tekinteni az általános biztonsági oktatás megtartását a hozzáférési jogosultság érvényesítése előtt, így elkerülhető a „nekem ezt senki nem mondta”, a „nem tudtam, hogy azt is el kell olvasni”, vagy a „másik szervezetnél így csináltuk” típusú védekezés. A képzésen résztvevő személyekkel a későbbi viták elkerülése érdekében aláírásukkal kell igazoltatni az oktatás megtörténtét, és az elhangzottak tudomásul vételét. Az oktatásnak ki kell térnie *az információvédelmi felelősség ismertetésére*, a *más szervezetnél végzett munkavégzés adatkezelési és védelmi feladataira*, az *otthoni munkavégzésre* (amennyiben az engedélyezett), valamint a *más szervezetektől átvett adatok kezelési és védelmi sajátosságaira*.

A BEOSZTÁS, MEGBÍZÁS IDEJE ALATTI INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEK

Az elektronikus adatkezelő rendszerhez hozzáférési jogosultsággal rendelkező személyek (felhasználók, üzemeltetők) számára rendszeres időközönként oktatást kell tartani az adatkezelő képesség üzemeltetésével, alkalmazásával vagy felhasználásával kapcsolatos felelősségükről, információvédelmi feladataikról, az információs fenyegetésekről, a biztonsági követelményekről és az általános védelmi rendszabályokról, beleértve a jelentési kötelezettség alá tartozó események ismertetését és a követendő eljárásrendet. Az oktatás elrendelése és végrehajtatása a szervezetileg illetékes vezető felelőssége, melyhez a következő szempontokat célszerű érvényesíteni:

- amennyiben jogszabály más követelményt nem határoz meg, nem minősített és minősített adatkezelő rendszerek esetében az oktatást éves gyakorisággal célszerű végrehajtani;
- az oktatás más foglalkozással összevonható, helyi sajátosságoknak megfelelően csoportokra bontva is végrehajtható;
- az oktatás mellett félévente célszerű önállóan, vagy más kötelező programhoz kapcsolva biztonsági tájékoztatást, ismeretfrissítést tartani;
- a rendszer használata vagy üzemeltetése területén tervezett jelentős változtatások előtt soron kívüli oktatást kell tartani;
- a hiányzó személyek számára pótfoglalkozásokat kell szervezni;
- az oktatás tartalmát, és a résztvevők névsorát a helyi információvédelmi szervezeti elemnél kell megőrizni;
- az általános oktatás mellett egyéni oktatás is elrendelhető.

Projektek, új tevékenységek előkészítésekor a szükséges specializált biztonsági képzést még a feladatok megkezdése előtt, dokumentáltan el kell végezni.

Minősített adatkezelés esetén a hozzáférési jogosultsággal rendelkező személyeknek az üzemeltetés–biztonsági szabályzatot évente át kell tanulmányozniuk. Az áttanulmányozás tényét, és a szabályzatban foglalt feladatok ismeretére és betartására vonatkozó nyilatkozatot minden személynek írásban kell tanúsítania. Az áttanulmányozás történhet egyéni-

leg (beleértve a hálózaton elektronikus formában hozzáférhető szabályzat tanulmányozásának lehetőségét is), vagy csoportosan. A nyilatkozatokat a helyi biztonságért felelős személynek nyilvántartva kell tárolnia.

A minősített elektronikus adatokat kezelő rendszerek hozzáférési jogosultsággal rendelkező személyeiről minden szervezetnél naprakész nyilvántartást kell vezetni.

Nemzetközi beosztásban lévő személyek, akik számára más nemzeti, vagy nemzetközi szervezet biztosít elektronikus adatkezelő szolgáltatást, az információbiztonsággal kapcsolatos rendszer-specifikus képzést a rendszer szempontjából illetékes (vagy a nemzetközi szerződés szerinti) szervezettől kapják, illetve automatizmus hiányában igényeljék.

A munkakörök vagy az adatkezelésre vonatkozó feladatok változása esetén a hozzáférési jogosultság megváltoztatása csak a szükséges ismeretek közlése, és a szükséges adminisztráció megtörténte után hajtható végre.

Nem honvédségi állományba tartozó személyek esetén, amennyiben az elektronikus adatkezelő rendszer teljes biztonsági dokumentumainak megismerése nem indokolt, a szükséges védelmi rendszabályokat tartalmazó kivonatot célszerű készíteni, és rendelkezésre bocsátani. Nyelvismeret hiányában a védelmi rendszabályok ismertetése szóban, más nyelven is megtörténhet, amely tényt az oktatásról szóló jegyzőkönyvben rögzíteni kell.

Az elektronikus adatkezelő rendszerek információvédelmi szakfeladatait ellátó személyeket az információvédelmi szakirányítást támogató HM szervezeti elem által meghatározott általános elektronikus információvédelmi szaktanfolyamra kell beiskolázni. A szaktanfolyamokra a résztvevők csak a szükséges nemzetbiztonsági ellenőrzésre, a személyi biztonsági tanúsítványra vonatkozó feltételek megléte esetén iskolázhatók be.

Az információvédelmi rendszabályok megsértőivel szemben a jogszabályoknak és a belső rendelkezéseknek megfelelő eljárást kell lefolytatni. A rendszabályok szándékos megsértése esetén az információs veszélyeztetés csökkentése érdekében a hozzáférési jogosultságot haladéktalanul fel kell függeszteni. Az esemény kivizsgálása során, amennyiben bebizonyosodik, hogy a hozzáférési jogosultság a rendszer üzemeltetése szempontjából további kockázatot nem hordoz, a jogosultság a vizsgálat befejezése előtt is visszaállítható.

A szándékos, vagy véletlen események kivizsgálása, értékelése után a tapasztaltakat szükség esetén soron kívül, egyéb esetben a következő oktatáson kell feldolgozni.

Az MH rendszereket érintő esetekben, vagy amikor az egyedi incidensek más szervezetek számára is tanulságosak, célszerű központi, írásos tájékoztatást kiadni a tapasztalatok hasznosítása, a tanulságok levonása érdekében.

A rendszerek felhasználói, üzemeltetői számára biztonsági tudatosságot erősítő, a szervezet feladataihoz illeszkedő akciókat, figyelemfelkeltő programokat kell szervezni.

A BEOSZTÁS, MEGBÍZÁS MEGSZŰNÉSÉVEL KAPCSOLATOS INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEK

A hozzáférési jogosultságokat (beleértve a létesítmények belépésére jogosító felhatalmazást is) a munkaviszony megszüntetésekor (vagy az adatkezelésre vonatkozó megbízás visszavonásakor) azonnali hatállyal vissza kell vonni.

A munkaviszony szüneteltetésekor vagy felfüggesztésekor a hozzáférési jogosultságokat zárolni, vagy törölni kell (belső és külső levelező rendszerek, és egyéb információs szolgáltatások), a mobil adatkezelő eszközöket, adathordozókat be kell vonni, és tárolni.

Bizalmas munkakörnél a munkaviszony változtatására vonatkozó döntés meghozatala előtt meg kell vizsgálni, hogy az adott személy milyen információs szolgáltatáshoz (vagy adathoz) rendelkezik hozzáférési jogosultsággal, mi a munkaviszony változásának (megszűnésének) oka, és azt melyik fél kezdeményezte. A kockázatok függvényében meg kell határozni azokat a kiegészítő védelmi rendszabályokat, amelyekkel biztosíthatók a szervezeti érdekek. Ennek hiányában kritikus funkciók bénulhatnak meg, adatok semmisülhetnek meg egy véletlennek tűnő üzemeltetői beavatkozás következtében, melyre a „bocsánat, tévedtem” vagy „nem tudtam, hogy még nem történt meg a mentés” típusú sablonos válasz már nem ad megoldást.

Munkaviszony megszűnése, vagy annak olyan változása esetén, ami az adatkezelői jogosultság változásával jár, az adott személy a részére rendelkezésre bocsátott elektronikus adatkezelést biztosító eszközökkel köteles haladéktalanul elszámolni. Ennek során célszerű az adatok érzékenységével arányos törlési eljárásokat alkalmazni, mert a korábbi felhasználói adatok visszaélésekre is lehetőséget adhatnak. Az anyagi elszámolás mellett a hozzáférést biztosító egyéni azonosítókat, felhasználói fiókokat is haladéktalanul törölni kell. A változás elrendelése a munkavállaló közvetlen elöljárójának, munkahelyi vezetőjének feladata. A technológiailag szükséges rendszeradminisztrátori hozzáférési jogosultságok törlésével egyidejűleg *gondoskodni kell a funkció azonnali betöltéséről, illetve a szükséges hozzáférési feljogosításról*.

Adott munkakörökhöz tartozó adatkezelési jog, képviseleti jog megszűnése esetén a közvetlen elöljárónak intézkednie kell az együttműködő szervezet értesítésére a további jogosulatlan adatkezelés (illetéktelen megismerés, megtévesztés) megakadályozása érdekében. Többek között ezért is *szükségszerűen tiltani kell a külső szervezeti kommunikáció nyilvánosan elérhető (például ...@freemail.hu, ..@gmail.com levelező fiókok) vagy magán levelező rendszeren történő folytatását*.

A távozó személy számára célszerű biztonsági tájékoztatást tartani a jogszabályokban foglalt titoktartási kötelezettség fennállásáról, az ezzel kapcsolatos kötelezettségről.

A szervezeten belüli beosztások változását úgy kell kezelni, mint amikor az adott személy beosztásból távozik, illetve új beosztásba lép. Ezzel elkerülhető *a régi hozzáférések „bennragadásának" halmozódó hatása, a magánszorgalomból történő adatgyűjtés kiküszöbölése*.

Szervezeti változások, átszervezések esetében, ha szükséges, külön rendszabályok bevezetésével biztosítani kell (pl. hozzáférési jogok korlátozása), hogy bizalmas adatok illetéktelen felhasználása ne történjen meg (pl. közösen használt könyvtárak tartalmának egyéni mentése, egyéb formájú, az adott munkakörben indokolatlan adatgyűjtés, mobil eszközökről, adathordozókról történő illetéktelen adatmásolás, vagy adatok elektronikus továbbítása).

OKTATÁS, KÉPZÉS, TOVÁBBKÉPZÉS

A szervezeteknél a helyi sajátosságoknak megfelelően a biztonsági oktatásokat felhasználói és üzemeltetői csoportokra bontva célszerű végrehajtani. A biztonsági oktatások témáit a honvédelmi szervezetek által üzemeltetett rendszerek sajátosságainak megfelelően kell kijelölni.

A szakirányítást végző HM szervnek az évek során felhalmozódott ellenőrzési, akkreditálási tapasztalatok, illetve a várható feladatok függvényében célszerű ajánlásokat tenni és oktatási témaköröket kijelölni. Ajánlott lehet például a jelszó biztonság és az egyedi azonosítás szabályai, a vírusok elleni védelem, a levelezés, az engedélyezett és tiltott adatkezelői tevékenységek, mentési feladatok, incidenskezelés, adathordozó szállítás, otthoni munkavégzés, rendezvények speciális adatkezelési igényei, magántulajdonú eszközökkel kapcsolatos rendszabályok, rejtjelzési kötelezettség, hordozható eszközökkel kapcsolatos rendszabályok, látogatók fogadása, információs fenyegetések és rendszer specifikus sebezető pontok.

Az oktatáson mindezek mellett ismertetni kell a szervezetnél szubjektív, objektív okokból bekövetkezett incidenseket a helyes eljárások ismertetése, a tanulságok levonása érdekében.

A másik kiemelt feladat a biztonsági tudatosítás, tájékoztatás. Egy-egy rendezvénnyel, feladattal kapcsolatban képek, rövid felhívások csatolhatók a tájékoztató anyagokhoz a biztonsági tudatosság fokozása érdekében. Folyosókon, közös használatú helyiségekben rövid, figyelemfelkeltő, a biztonsággal kapcsolatos üzeneteket tartalmazó poszterek helyezhetők ki, figyelmeztető feliratok, jelzések vagy hangos tájékoztatás alkalmazható (pl. mobil kommunikációs eszköz használatának tilalma, csomagok tárolására vonatkozó rendszabályok, belépési engedély viselésének kötelezettsége). Körlevelek, hirdetések, elektronikusan küldött emlékeztetők csatolhatók a szervezet előtt álló feladatokhoz, amelyek a biztonsági

incidensek szervezeti hatásaira mutatnak rá. A rendezvények, gyakorlatok résztvevőit a helyi sajátosságoknak megfelelően kialakított írásbeli vagy szóbeli tájékoztatásban szükséges értesíteni a helyi sajátosságokról.
Az előző, zömében helyi jellegű feladatokat központi szakági átképző tanfolyamokkal és haditechnikai céltanfolyamokkal, szakmai ismeret-kiegészítő tanfolyamokkal, katonai-szakmai továbbképzésekkel, valamint külföldi és hazai tanfolyamokkal kell erősíteni, támogatni. Ezeken a területeken már jól kialakult rend tapasztalható a honvédelmi tárcánál. A ZMNE bázisán kialakult, folyamatosan fejlődő tanfolyami rendszer, az éves összevonások és konzultációk hatására lassan érzékelhetők a honvédelmi szervezeteknél a szakmai közösség kialakulásának jelei. Ezen a területen komoly lendületet adhat a jogszabályok korszerűsítése és így a nemzeti – NATO, EU térfelekre szakított világ megszűnése, az elektronikus adatkezelő képességek korszerűsítése és ez által új erőforrások, lehetőségek biztosítása a biztonsági menedzsmentek számára.

ÖSSZEFOGLALÁS

A fentiek alapján látható, hogy a személyi biztonság a nemzetbiztonsági ellenőrzés, a minősítési szintnek megfelelő tanúsítványok, valamint nyilatkozatok és feljogosítások mellett még rengeteg feladatot tartalmazó, összetett kérdés.
A honvédelmi tárca a fentieknek megfelelően a személyi biztonság rendszer-specifikus tényezők szerinti meghatározását követeli meg a vezetőktől. Ennek megfelelően szükség van az elektronikus adatkezelő rendszereknél a munkakörök összeférhetetlenségének vizsgálatára, az üzemeltetői és biztonsági állománynál a helyettesítési feladatok meghatározására, valamint a műveletei során a minősített adatkezeléshez szükséges rendkívüli felhatalmazásra. [6.]
A cikkben röviden, tömören ismertetett követelmények segítségével pontosíthatók a szervezeti típusú (pl. Számítástechnikai Védelmi Szabályzat [7.] az Ált/210. szabályzat követelménye szerint) és a rendszer-specifikus biztonsági dokumentumokban [8.] a személyi biztonságra vonatkozó feladatok. Természetesen nem szabad elfelejteni azt az egyszerű tényt, hogy a technikai és a szervezeti változások napjainkban tapasztalható üteme mellett a szabályozók elévülési ideje egyre jobban rövidül. Így szervezeti és rendszer szinten kiemelt vezetői feladatként kell kezelni a szabályozók naprakészen tartását, az elektronikus adatkezelő képességek tekintetében pedig a változások kezelését.
Tárca szinten mindezek mellett az információbiztonság napi aktualitású kérdései közé kell tartozni, hogy létrejöjjön a honvédelmi tárcánál az informatikai biztonsággal kapcsolatos politika támogatására egy tárca szintű rendszer- és szervezet-független követelményrendszer az elektronikus adatkezelés biztonsága érdekében, amelyben helyet kell kapnia a személyi biztonsági kérdéseknek is.

Kulcsszavak: biztonságpolitika, információbiztonság, információvédelem, adatkezelés, személyi biztonság.

Keywords: security policy, information security, protection of information, information handling, personnel security.

FELHASZNÁLT IRODALOM

[1.] 2009. évi CLV. törvény a minősített adat védelméről, 20. §. (2) q)

[2.] MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények; A melléklet, A 8.1- A 8.3. p.

[3.] MSZ ISO/IEC 17799 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002), 8.1 – 8-3. p.

[4.] Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszer (MIBIK), Informatikai Biztonsági Követelmények v 1.1. 2008, p. 76-87.

[5.] ISO/IEC 20000-1 Information technology – Service management - Part 1: Specification; 3.3. p. és 6.6. p.

[6.] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról, 19-21. §.

[7.] A Magyar Honvédség Informatikai Szabályzata (Ált/210), 199. p.

[8.] 179/2003. (XI. 5.) Korm. rendelet a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól, 63. §. (2)-(3); (2010. április 1-től hatályon kívül)