HADMÉRNÖK

V. Évfolyam 4. szám - 2010. december

Kuris Zoltán
Zoltan.Kuris@bm.gov.hu

A KOMPLEX INFORMÁCIÓVÉDELEM ÚJ IRÁNYAI A NEMZETI MINŐSÍTETT ADATOK VÉDELMÉVEL ÖSSZEFÜGGÉSBEN

Absztrakt

Jelen közleményben a szerző áttekinti a közelmúltban megjelent minősített adatok kezeléséről szóló törvényt, és a hozzá kapcsolódó három kormányrendeletet, valamint annak hatásait a nemzeti minősített adatok kezelésére. Az elemző értékelés különös figyelemmel vizsgálja a hazai információvédelmi szakma irányelveihez és a nemzetkőzi minősített adatok kezeléséhez fűződő koherenciát. A szerző igyekszik feltárni a szabályozási rendszerben megjelenő anomáliákat és előre jelezni a tovább lépés irányát és lehetőségeit.

In this work, the author analyses the law on the protection of qualified data and the three governmental regulations concerning its execution. The effects of the law on information protection are also analysed. The minor faults and the options of correction are also described as well as the state of domestic information protection. The importance of the formation of the new view and the fact that the event is important for home professional circles are justified, too.

Kulcsszavak: *komplex információbiztonság, minősített adat ~ complex information security, classified information*

BEVEZETÉS

Az információvédelem szakterületén, a közelmúltban történelmi jelentőségű változások következtek be. Hosszú idő után, az Európa Tanács 2002-ben megfogalmazott irányelveivel összhangban 2009. december 14-én az Országgyűlés megalkotta a minősített adat védelméről szóló 2009. évi CLV. törvényt.(a továbbiakban mavtv.) E törvény – az előzőekhez képest – alapjaiban más szemléletmódot tükröz a minősített adatok védelmével összefüggésben. A törvény egységes keretek között szabályozza a nemzeti és a külföldi minősített adatok kezelését. Meghatározza a minősítéssel védhető közérdek fogalmát és tartalmát. Ugyanakkor ezzel összefüggésben bevezeti a kármérték alapú minősítés gyakorlatát is. Rendkívüli jelentőségű az a tény, hogy az mavtv. megjelenését követően, a Kormány három kormányrendeletben szabályozta, a Nemzeti Biztonsági Felügyelet működését, a minősített

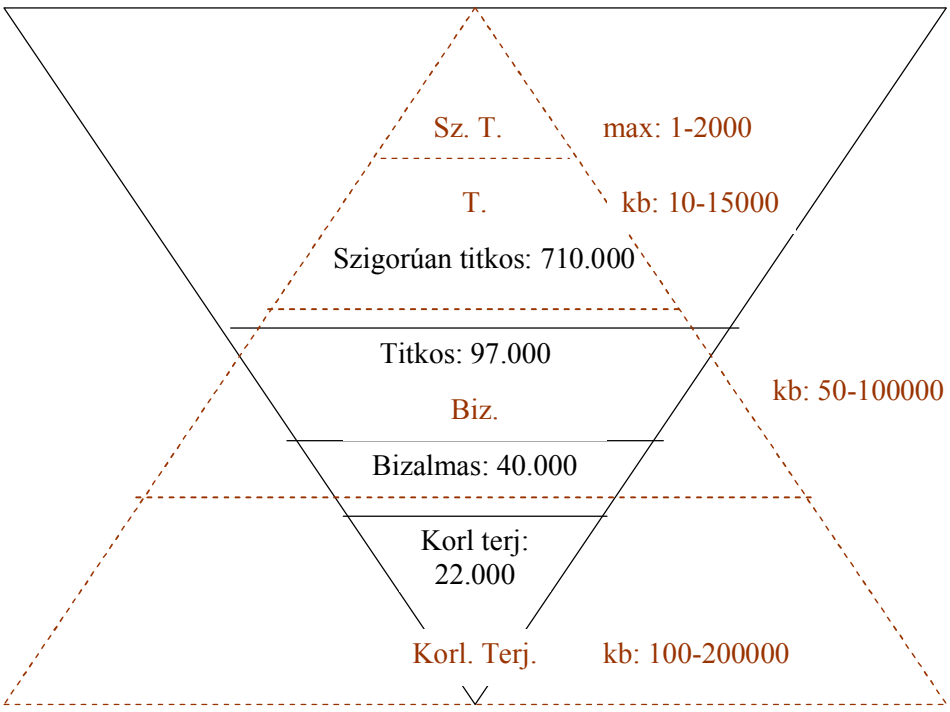
adat kezelésének rendjét, a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység és annak hatósági szabályait, illetve, az ezzel összefüggő iparbiztonsági területet is. Az előző időszakhoz képest megállapítható, hogy a nemzetkőzi szabályozókhoz igazodva, a koherenciára való törekvés egyértelműen nyomon követhető. A minősített adatok kezelésével összefüggő szabályozók között logikai és gyakorlati szinten megjelennek a komplex információvédelmi elvek. Ugyanakkor apróbb szabályozási ellentmondásokat is fel lehet lelni a minősített adatot kezelő szerezet vezetőjének hatáskörét illetően, abban az esetben, ha hierarchikus szervezetben történő szakirányítási szinten elemezzük a gyakorlati megvalósítást. További ellentmondások lelhetők fel az elektronikus információvédelem szabályozásának területén, különösen a kisugárzás védelem megvalósításának szabályozását illetően. Ugyanakkor vitathatatlanul történelmi jelentőségű eseményről van szó az információvédelmi szakmát illetően. Különösen igaz ez a megállapítás akkor, amikor a kritikus infrastruktúra védelmének területén fogalmazódik meg az igény egy olyan infokommunikációs, információs riasztási rendszer, illetve vezetésirányítási, kommunikációs rendszer szükségességét illetően, amely az érzékeny adataik védelmének érdekében információbiztonsági szempontból is megalapozottak. Napjainkban már hazai szektorokból is „figyelemfelkeltő jelzések" érkeznek azzal összefüggésben, hogy infrastruktúrájukat célzó kihívások és kockázatok észlelhető fenyegetések felé hajlanak. Ezekre a figyelmeztető jelekre célszerű odafigyelni és együttműködést kell kialakítani a kritikus infrastruktúrák védelmének érdekében. Ebben a globális környezetben szükségszerűen felértékelődik a minősített információ előállításával, gyűjtésével, tárolásával, feldolgozásával, továbbításával összefüggő információvédelmi tevékenység nemzeti és nemzetközi szintű koherens szabályozórendszer keretei között történő működtetése. Már pedig ha az igény a hazai szektorok felől egyre fokozódik az információvédelmi megoldások irányába, akkor az információvédelmi szakembereknek fel kell készülni az igények szakszerű kielégítésére. Természetesen szükségszerű az, hogy a jelenséget tudományos műhelyekben feltárjuk, elemezzük, modellezzük és hatékony védelmi rendszert tervezzünk és alkalmazzunk a nemzet biztonságát alapvetően befolyásoló szektorokban. Ez tehát az információvédelmi szakemberekkel szemben támasztott alapvető igény, és ennek kielégítése nem egyszerű feladat, ugyanakkor ennek szükségességére fel kell hívni az arra illetékesek figyelmét. Irányadó szakemberek szerint is megállapítható az, hogy a megfogalmazódó igények szakszerű kielégítésének kereteit teremti meg az írásműben ismertetett, értékelő elemzés tárgyát képező szabályozó rendszer.

A létfontosságú infrastruktúra védelmének érdekében használt – információ gyűjtésére, feldolgozására, tárolására és továbbítására – alkalmazott infokommunikációs rendszerek és azok információvédelmi jellemzői alapvetően befolyásolják a védelmi intézkedések eredményességét. Ennek okán célszerű összefoglalni a fentiekben felvázolt új, komplex információvédelmi irány tartalmát és összefüggéseit, illetve annak hatásait, következményeit a kritikus infrastruktúra és információs infrastruktúra védelmével összefüggésben.

AZ ÚJ ÍRÁNY ALAPJA A MINŐSÍTETT ADAT VÉDELMÉRŐL SZÓLÓ TÖRVÉNY

A minősített adatok védelméről szóló 2009. évi CLV törvényt (a továbbiakban Törvény) az Országgyűlés 2009. december 14-i ülésnapján fogadta el. Általános rendező elvek között megjelenik a Magyar Köztársaság érdekeinek védelme, a nemzetközi kötelezettségvállalások teljesítése a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvénnyel, valamint az elektronikus információbiztonságról szóló törvénnyel való összhang. Az törvényben ugyancsak jól kimutatható a külföldi minősített adatkezelési szabályokkal való

koherencia, az egységes elvek terminológiai megközelítés és az egységesített minősítési szintek.
Az is megállapítható, hogy a komplex információbiztonsági alapelvek szintén megjelennek az Törvényben. Ilyen alapelvek: a szükségesség és arányosság elve, a szükséges ismeret elve, a bizalmasság elve, a sérthetetlenség elve, valamint a rendelkezésre állás elve. Az irányelvek már világosan előrejelzik a törvény legalapvetőbb üzenetét, a túlminősítés elkerülése érdekében történő szabályozási elvek érvényesítését (1. ábra). Apróbb értelmezési anomáliát jelenthet a „sérthetetlenség elve" szóhasználat, amely helyett célszerűbb lenne a szakmai körökben elfogadott „sértetlenség elve" kifejezés használata.
A törvény – többek között – rögzíti a nemzeti minősített adat, külföldi minősített adat és az elektronikus adatkezelő rendszer fogalmát, ezzel elősegítve az egységes értelmezést.
Az információvédelmi szakemberek számára igen fontos és figyelemre méltó új elem a minősítéssel védhető közérdek és az ezzel összefüggő alapvetően kár alapú megközelítés (2. ábra). Ezzel összefüggésben a Törvény egyértelműen meghatározza, hogy az adat mely esetekben védhető minősítéssel. A Törvény új minősítési szinteket állapít meg úgymint „Szigorúan titkos" „Titkos" „Bizalmas" és „Korlátozott terjesztésű". Ezek a minősítési szintek megfelelnek a külföldi minősített adat minősítési szinteknek (3. ábra). Ez egy igen fontos lépés az előirányzott koherencia területén. A minősítések érvényességi ideje is lényegesen csökkent, illetve a felülvizsgálatok száma is korlátossá vált (4. ábra). Ez is tükrözi és elősegíti a túlminősítés és a túlzott idejű minősítés fenntartása elleni küzdelmet. Külön szakasz foglalkozik a minősített adat felülvizsgálatának és felülbírálásának szabályaival, egyértelművé téve ezzel a szabályozást. Ugyanakkor – egyes szakemberek szerint – a minősítő számára a melléklet nem ad megfelelően egyértelmű támpontokat a minősítési szint megállapításának vonatkozásában. A törvény újra szabályozza a minősítési szintekhez kapcsolódó nemzetbiztonsági ellenőrzések rendszerét (5. ábra) és a büntetőjogi szankciórendszert is differenciálja az egyes minősítési szintekhez igazodóan (6. ábra).



1. ábra. A túlminősítési piramis talpra állítása [9]

„Szigorúan titkos!”	**rendkívül súlyosan károsítja a minősítéssel védhető közérdeket**
„Titkos!”	**súlyosan károsítja a minősítéssel védhető közérdeket**
„Bizalmas!”	**károsítja a minősítéssel védhető közérdeket**
„Korlátozott terjesztésű!”	**hátrányosan érinti a minősítéssel védhető közérdeket**

2. ábra. Kár alapú megközelítés (1) [9]

„Szigorúan titkos!”	**a Magyar Köztársaság szuverenitásának megsértése, nagyszámú emberi élet veszélyeztetése;**
„Titkos!”	**közvetlen életveszély okozása, ellehetetleníti az állami vagy közfeladatot ellátó szerv rendeltetésszerű működését;**
„Bizalmas!”	**az állam érdekérvényesítő képességeit hátráltatja, gátolja valamely legalább öt évi szabadságvesztéssel büntetendő bűncselekmény felderítését**
„Korlátozott terjesztésű!”	**gazdálkodó szervezetek részére jogtalan előnyszerzést tesz lehetővé;**

3. ábra. Kár alapú megközelítés (2) [9]

	Érvényességi idő	Hosz-szabbítás alapesete	Magánszemély jogos érdekével összefügg. A Magyar Köztársaság - honvédelmi, - nemzetbiztonsági, - bűnüldözési vagy - igazságszolgáltatási érdekére tekintettel
„Szigorúan titkos!”, „Titkos!”	**30 év**	1 x 30 év **∑: 60 év**	2 x 30 év **∑: 90 év**
„Bizalmas!”	**20 év**	1 x 5 év **∑: 25 év**	2 x 20 év **∑: 60 év**
„Korlátozott terjesztésű!”	**10 év**	1 x 5 év **∑: 15 év**	2 x 20 év **∑: 50 év**

4. ábra. Az érvényességi idő új szabályozása [9]

„Szigorúan titkos!”	**„C” típusú kérdőívhez kötött nemzetbiztonsági ellenőrzés**
„Titkos!”	„B” típusú kérdőívhez kötött nemzetbiztonsági ellenőrzés
„Bizalmas!”	„A” típusú kérdőívhez kötött nemzetbiztonsági ellenőrzés
„Korlátozott terjesztésű!”	Nincs szükség nemzetbiztonsági ellenőrzésre

5. ábra.
Az egyes minősítési szintekhez kapcsolódó nemzetbiztonsági ellenőrzések típusai [9]

	„civil” maximum	„hivatalos” maximum
Visszaélés szigorúan titkos minősítésű adattal:	2-8 évig	5-15 évig
Visszaélés titkos minősítésű adattal:	1-5 évig	2-8 évig
Visszaélés bizalmas minősítésű adattal:	- 3évig	1-5 évig
Visszaélés korlátozott terjesztésű minősítésű adattal:	- 1 évig	-3 évig

6. ábra. A büntetőtörvénykönyv változása. [9]

A minősített adat általános biztonságára vonatkozó szabályok

Ebben a fejezetben jelenik meg a szakmai műhelyekben már kialakított komplex információ biztonság rendszere. Jól látszik, hogy az írásmű követi a komplex információvédelmi felosztást – úgymint személyi biztonság; adminisztratív (dokumentum´biztonság; fizikai biztonság; elektronikus biztonság – és annak alrendszereit.

A biztonság alapvető feltételei a Nemzeti biztonsági Felügyelet – mint hatóság - által kiállított adatkezelési engedély, személyi biztonsági tanúsítvány, nemzetbiztonsági ellenőrzés lefolytatása, a végrehajtási rendeletekben kiadott személyi, fizikai, adminisztratív és elektronikus biztonsági követelmények teljesítése. Ez a komplex megközelítési mód – szakmai körökben elfogadott elvek alapján - teremti meg a minősített adatok hatékony védelmének alapjait.

A minősített adat védelmét ellátó szervezetek és személyek

Ebben a fejezetben fogalmazódnak meg a Nemzeti Biztonsági Felügyelet (A továbbiakban NBF) feladatai. Az NBF önálló feladattal és hatósági jogkörrel rendelkező szervezet. Új megközelítésben a minősített adatot kezelő szervezet vezetője felelős a minősített adat védelmi feltételeinek kialakításáért, ugyanakkor a feladatok végrehajtását és koordinálását a minősített adatot kezelő szerv vezetője által kinevezett biztonsági vezető végzi. A Törvény lehetőséget ad, úgynevezett biztonsági felügyelet kijelölésére is, melyet a kinevezett Biztonsági Vezető irányítja. A felvázolt felső szintű szervezeti struktúra hierarchikus rendszere és a kinevezés intézménye biztosítja a minősített adat védelmének érdekében létrehozott szervezet hatékony működését, úgy hogy már itt, meghatározásra kerülnek az alapvető felelősségi körök.

A MINŐSÍTETT ADATOK VÉDELMÉVEL KAPCSOLATOS VÉDELMI INTÉZKEDÉSEK

A minősített adat védelméről szóló 2009. évi CLV. törvényben meghatározott fő irányokat részleteiben a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet, a minősített adat elektronikus

biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V.6) Korm. rendelet és az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendelet szabályozza.

Az iparbiztonsági ellenőrzés és a Telephely Biztonsági Tanúsítvány (a továbbiakban: TBT) kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendelettel összefüggésben az alábbiak kiemelése szükségszerű és elengedhetetlen annak érdekében, hogy a szabályozási folyamat véglegesítésének lehetőségét és alkalmazhatóságát elemezzük. A minősített adatot kezelő gazdálkodó szervezeteknek 2010. április 01-ét követően TBT-t beszerezniük, melynek előfeltétele a legalább két éves működés. A NATO EU TBT kiállítása csak nemzeti TBT birtokában lehetséges. Az iparbiztonsági ellenőrzés két fázisból áll, nevezetesen a nemzetbiztonsági fázisból és a fizikai és adatbiztonsági fázisból. A nemzetbiztonsági fázis az Alkotmányvédelmi Hivatal és Katonai Biztonsági Hivatal, a fizikai és adatbiztonsági fázis pedig az NBF hatáskörébe tartozó tevékenység.
A kiadott TBT azt igazolja hogy:

- az adott gazdálkodó szervezet iparbiztonsági ellenőrzése befejeződött
- adott szintű minősített információk kezelésére (tárolására, feldolgozására)alkalmas
- minősített projektbe biztonsági szempontból bevonható

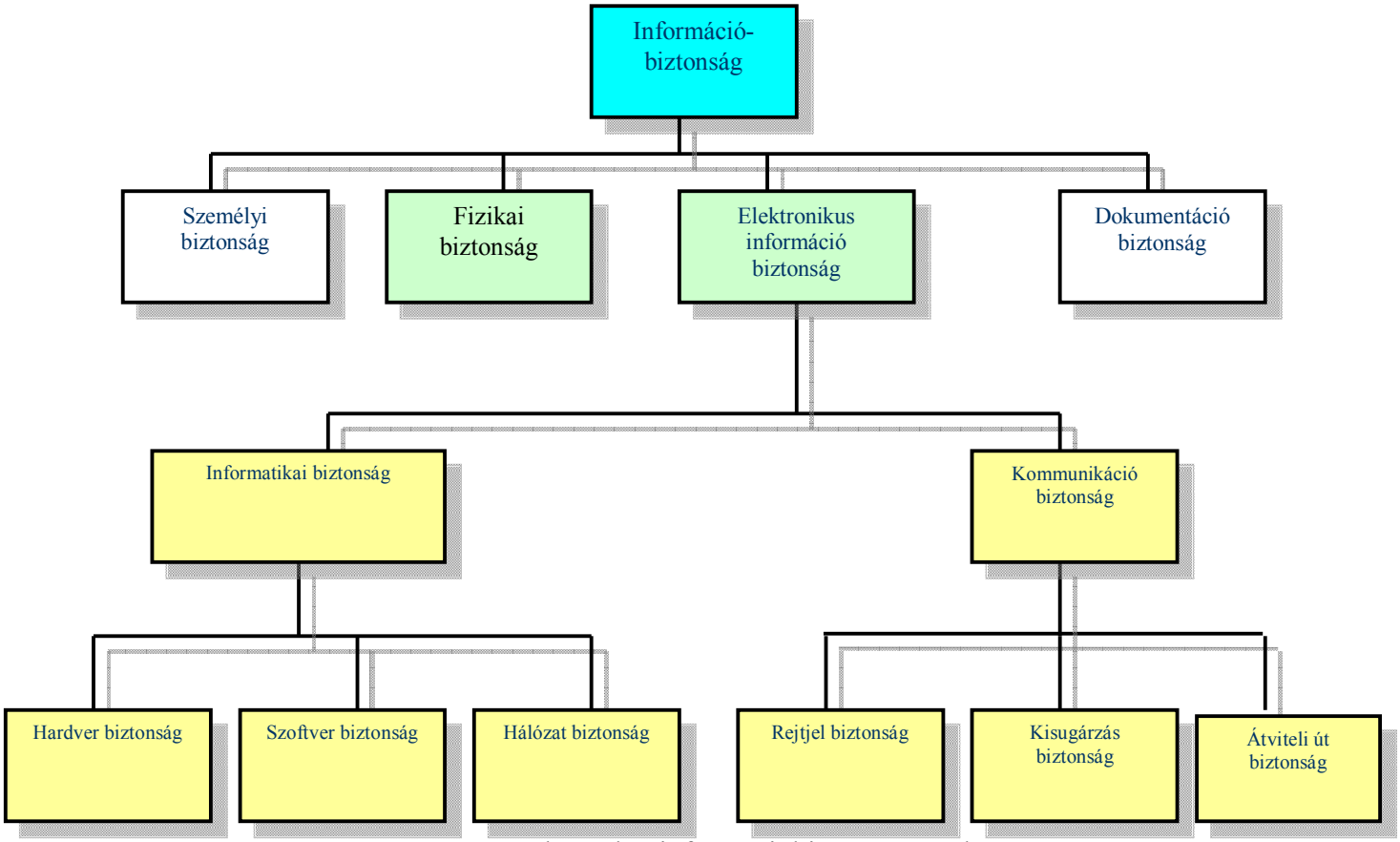
A „Bizalmas" vagy magasabb minősítési szint esetén az érvényes telephely biztonsági tanúsítvány érvényességének igazolását a minősített adatot átadó szerv az NBF-től kéri.
A„Korlátozott terjesztésű" minősítési szint esetén a gazdálkodó szervezet részére a felhasználói engedélyt a minősített adatot átadó szerv vezetője adja ki (előtte meggyőződik, hogy megteremtették-e a KT védelméhez előírt biztonsági feltételeket)
A gazdálkodó szervek a minősített szerződés végrehajtásának biztonsági előírásait Projekt Biztonsági Utasításban szabályozzák.
A Projekt Biztonsági Utasítást a minősített adatot átadó szerv vezetője készíti el a biztonsági vezető bevonásával. A Projekt Biztonsági Utasítás, a minősített szerződés részletes biztonsági előírásait tartalmazza, függeléke a projekt minősítési jegyzék.
A projekt biztonsági utasítás rendelkezik:

- A végrehajtásban részt vevő szervek, a biztonsági szervek és személyek feladat- és hatásköréről,
- a minősített adatok helyszíni tárolásának, bel-és külföldi továbbításának szabályairól,
- a megbeszéléseken, előadásokon történő felhasználás egyedi rendelkezéseiről,
- a minősített adatok alvállalkozónak történő átadásának feltételeiről,
- a minősített szerződés teljesítését követő eljárásrendről (minősített adatok átadónak történő visszaszolgáltatása).

Külföldi gazdálkodó szervezet bevonása esetén a „Bizalmas" vagy annál magasabb minősítési szintű szerződés kötését megelőzően a minősített adatot átadó szerv vezetője az NBF útján be kell hogy szerezze az adott ország nemzeti biztonsági hatóságának igazolását a TBT meglétéről.
Ha a fenti szabályozást összevetjük a jelenleg érvényes szabályozási környezettel és a valós gazdasági környezettel, egyrészt megállapítható, hogy TBT-vel a hazai gazdálkodó szervezetek nagy része még nem rendelkezik, ezért ezen a területen a szabályozás gyakorlati környezetbe való átültetése fontos és elengedhetetlen feladat. Másrészt figyelemmel arra, hogy *az államtitkot vagy szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdeket érintő vagy különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló 143/2004. (IV.29.) Korm. rendelet még mindig hatályos,* ezért annak módosítása a

telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendelettel összhangban szükséges.

Ugyanakkor a fentiekben kifejtett megállapításokkal együtt ki lehet jelenteni, hogy a minősített adat védelméről szóló 2009. évi CLV. törvényben és a hozzá kapcsolódó kormányrendeletek a nemzetközi trendnek megfelelően a védelmi intézkedéseket az eddigi tudományos kutatások alapjaira helyezik (1.ábra) . Az alapelvek és előírt védelmi intézkedések tükrözik a Tanács biztonsági szabályzatának elfogadásáról szóló EU Tanács 2001. március 19-i 2001/264/EK határozatában megfogalmazottakat, azzal összhangban vannak.



7. ábra. A komplex információbiztonság rendszere

Megállapítható viszont az is, hogy a 161/2010. (V.6) Korm. rendelet nem intézkedik kellő részletességgel a hardver és szoftverbiztonsági kérdésekről és a „nemzeti TEMPEST" követelményrendszerével összefüggésben ugyan „az engedélyezési eljárások „fejezetében „a TEMPEST követelmények érvényesítése" [3] megemlíti, de részletes követelményeket nem támaszt. Előirányozza a TEMPEST követelményrendszerének rendelkezésre állását, de ilyen nemzeti követelményrendszer még nem érhető el, illetve az NBF jelenlegi álláspontjára figyelemmel az megegyezik a NATO TEMPEST követelményekkel. Ez alapvetően befolyásolja az elektronikus védelmi intézkedések kisugárzás védelmi alrendszereinek rendelkezésre állását, amely egyben a védelmi rendszer egyenszilárdságát is befolyásoló tényezővé válhat. Irányadó szakemberek véleménye szerint ezen a területen is további szabályozás szükséges.
A minősített adatok kezelésére alkalmas elektronikus rendszer teljes életciklusában a feljogosítás előtti, az adatkezelés alatti és a feljogosítás megszüntetése utáni szakaszokra bonthatók.

Ennek megfelelően a személyi biztonság kérdései is három részre tagolhatók [8]:

- 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 és meghatározása. Az életciklus szerinti megközelítés már megjelenik a nemzeti szabványokban [4], a jelenleg érvényes nemzeti ajánlás is ezt a szemléletet tükrözi [6], illetve az informatikai szolgáltatások szabályozása területén is megfigyelhető [7]. Az említett források feldolgozása az információvédelmi szakemberek munkáját támogathatja, ezzel összefüggésben Kassai Károly Hadtudományi Szemlében megjelent cikke [8] jó példa a szabványok, a civil ajánlások alkalmazhatóságának vizsgálatára.

A 90/2010. (III. 26.) Korm. rendelet előírja, [2] hogy a minősített adatot kezelő szervezetnek el kell készítenie a biztonsági szabályzatát, amelyben leírja a minősített adatok védelmének érdekében felállított szervezet felépítését, működését, a személyi fizikai adminisztratív és elektronikai védelem területén foganatosított védelmi intézkedéseket és a veszélyhelyzeti tervet. Az alábbiakban a kormányrendeletben előírtakra figyelemmel, biztonsági szabályzat ajánlásban célszerű összefoglalni a kormányrendeletekben tükröződő követelményrendszert.
A komplex információbiztonsági elveket szem előtt tartva, fontos kiemelni, hogy az elektronikai biztonsági követelményrendszer – és az ezzel összefüggő szabályzat kialakítása – a biztonsági szabályzaton túl mutató (szabályozási szempontból, a törvény erejéből fakadóan követő) önálló szabályozási ciklusban nyilvánul meg. Ebből eredően ugyan nem szükséges az elektronikus biztonságot a szervezet biztonsági szabályzatában szabályozni, viszont az információs társadalmi fejlődés jelen szakaszában, valós kockázatot jelent ezen a területen a szabályozás hiánya.

BIZTONSÁGI SZABÁLYZAT
(ajánlás)

a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján minősített és a nemzeti minősített adatok védelmére

I. fejezet
ÁLTALÁNOS SZABÁLYOK

Jelen Szabályzat (ajánlás) a minősített adat védelméről szóló 2009. évi CLV. törvényben (a továbbiakban: (Mavtv.) valamint Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendeletben (a továbbiakban: Rendelet) a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V.6) Korm. rendeletben és az iparbiztonsági ellenőrzés és a telephely biztonsági

tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendeletben foglaltak alapján meghatározza:

a) azon kezelési eljárások és módszerek összességét, amelyek kizárják a nemzeti és a külföldi minősített adatok illetéktelen személyek által történő megismerését;

b) nemzeti és a külföldi minősített adathordozók (iratok) készítésének, nyilvántartásának, továbbításának és irattári kezelésének szabályait.

Az alkalmazott biztonsági intézkedések:

- kiterjednek a minősített adatokhoz hozzáférő személyekre, a minősített adathordozókra, a minősített adatoknak helyet adó helyiségekre és berendezésekre;
- kiszűrik azokat a személyeket, akiknek az alkalmazása veszélyezteti a minősített adatok és az azokat tartalmazó adathordozók, berendezések biztonságát;
- megakadályozzák, hogy a minősített adatokhoz, adathordozókhoz és berendezésekhez, illetéktelen személyek hozzáférhessenek;
- a minősített adatok elosztása során a „szükséges ismeret" elvét követik;
- biztosítják a minősített adat integritását, (megakadályozzák a megrongálódást, illetéktelen módosítását, vagy illetéktelen törlését) és rendelkezésre állását (hozzáférést biztosít az arra jogosultak részére).

1. Alapelvek

Szükségesség és arányosság elve a közérdekű adat nyilvánosságához fűződő jogot minősítéssel korlátozni csak az e törvényben meghatározott feltételek fennállása esetén, a védelemhez szükséges minősítési szinttel és a feltétlenül szükséges ideig lehet. *Szükségesség és arányosság elve alapján a zavartalan információáramlás biztosítása érdekében törek*edni kell az indokolatlan szigorú minősítés elkerülésére.

Szükséges ismeret elve: minősített adatot csak az ismerhet meg, akinek az állami vagy közfeladata ellátásához feltétlenül szükséges.

Bizalmasság elve: minősített adat illetéktelen személy számára nem válhat hozzáférhetővé vagy megismerhetővé.

Sérthetetlenség elve: a minősített adatot kizárólag az arra jogosult személy módosíthatja vagy semmisítheti meg.

Rendelkezésre állás elve: annak biztosítása, hogy a minősített adat az arra jogosult személy számára szükség szerint elérhető és felhasználható legyen.

2. A Szabályzat hatálya

2.1. Itt kell megfogalmazni, hogy mely hivatali szervezeti egységekre terjed ki a biztonsági szabályzat hatálya.

3. Értelmező rendelkezések [1] 3.§

2.2. **NATO, illetve NYEU Központi Nyilvántartó:** a Honvédelmi Minisztérium információ- és dokumentumvédelemmel foglalkozó szervének a NATO, illetve a NYEU minősített információk országos szinten történő fogadására, elosztására és kezelésére kijelölt szervezeti egysége;

2.3. **EU Központi Nyilvántartó:** a Külügyminisztériumnak az EU minősített adatok országos szinten történő fogadására, elosztására és kezelésére kijelölt szervezeti egysége;

2.4. **Nemzeti minősített adat:** a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést a Mavtv-ben, valamint a törvény felhatalmazása alapján kiadott,

jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele, a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti, vagy veszélyezteti és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza;

2.5. **Külföldi minősített adat:** az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza.

2.6. **Nyilvántartó:** a minősített adatot kezelő szervhez érkező vagy ott keletkező, külföldi és nemzeti minősített adatok nyilvántartásával kapcsolatos feladatok végrehajtására feljogosított szervezet;

2.7. **Kezelő pont:** a Nyilvántartó felügyelete alatt működő, a nemzeti minősített adatok nyilvántartásával kapcsolatos feladatok végrehajtására létrehozott szervezet;

2.8. **Érvényességi idő:** az az év, hó, nap, szükség esetén óra, perc szerint feltüntetett időpont, ameddig a nemzeti minősített adat nyilvánosságra hozatalát, illetve az arra feljogosítotton kívüli minden megismerhetőségét a minősítő korlátozza;

2.9. **Minősítő:** feladat- és hatáskörében minősítésre jogosult személy;

2.10. **Minősített adatot kezelő szerv:** állami vagy közfeladat ellátása érdekében minősített adat kezelését végző szerv, szervezet vagy szervezeti egység, továbbá a gazdálkodó szervezet.

2.11. **Biztonsági vezető:** a minősített adatok védelmével kapcsolatos feladatok végrehajtását és koordinálását végző, a minősített adatot kezelő szerv vezetője által – a Nemzeti Biztonsági Felügyelet elnökének egyetértésével - kinevezett személy;

2.12. **Titkos ügykezelő:** a nyilvántartó és a kezelő pont iratkezelője;

2.13. **Közreműködő:** az a természetes személy, aki az állami vagy közfeladatot ellátó szerv feladat- és hatáskörébe tartozó ügyben segítséget nyújt, és ehhez minősített adat felhasználása is szükséges.

2.14. **Felhasználó:** az a személy, akinek állami vagy közfeladat végrehajtása céljából a felhasználói engedély kiadására jogosult vezető a minősített adatra vonatkozóan a felhasználói engedélyben rendelkezési jogosultságokat biztosít;

2.15. **Felhasználás:** állami vagy közfeladat végrehajtása érdekében a felhasználói engedély kiadására jogosult vezető által, a felhasználói engedélyben meghatározott, a minősített adatra vonatkozó rendelkezési jogosultságok gyakorlása.

2.16. **Felhasználói engedély:** állami vagy közfeladat végrehajtása érdekében a minősítő, illetve a felhasználói engedély kiadására jogosult vezető által, a minősített adat felhasználására jogosult személy részére írásban adott felhatalmazás, a minősített adattal kapcsolatos egyes rendelkezési jogosultságok meghatározásával.

2.17. **Megismerési engedély:** a minősítő által a jogosult személyazonosító adatainak feltüntetésével, a nemzeti minősített adattal kapcsolatos rendelkezési jogosultságok megjelölésével, a nemzeti minősített adat megismerésére írásban adott felhatalmazás. **Titoktartási nyilatkozat:** a minősített adatot felhasználó vagy megismerő személy nyilatkozata arról, hogy a minősített adat védelmére vonatkozó szabályokat megismerte, és az őt terhelő titoktartási kötelezettséget tudomásul vette.

2.18. **Személyi biztonsági tanúsítvány:** az a tanúsítvány, amely érvényességi idejének lejártáig meghatározza, hogy valamely természetes személy milyen legmagasabb minősítési szintű adat felhasználására kapott felhasználói engedélyt.

2.19. **Elektronikus adatkezelő rendszer:** minősített adat elektronikus, elektromagnetikus vagy optikai úton történő kezelésére alkalmas berendezés, módszer és eljárás együttese;
2.20. **Rendvédelmi szerv:** a rendőrség, a polgári védelem, a polgári nemzetbiztonsági szolgálatok, a büntetés-végrehajtási szervezet, a vám- és pénzügyőrség, valamint az állami és hivatásos önkormányzati tűzoltóság;

4. A külföldi minősítési szint és annak nemzetközi minősítési szintű megfelelője [1] / 2.sz. melléklet

4.1. A NATO által használt minősítési szint és annak nemzeti minősítési szintű megfelelője:
- „COSMIC TOP SECRET" - „Szigorúan titkos!";
- „NATO SECRET" - „Titkos!";
- „NATO CONFIDENTIAL" - „Bizalmas!";
- „NATO RESTRICTED" - „Korlátozott terjesztésű!".

4.2. A NYEU által használt minősítési szint és annak nemzeti minősítési szintű megfelelője:
- „FOCAL TOP SECRET" - „Szigorúan titkos!";
- „WEU SECRET" - „Titkos!";
- „WEU CONFIDENTIAL" - „Bizalmas!";
- „WEU RESTRICTED" - „Korlátozott terjesztésű!".

4.3. Az Európai Unió Tanácsa által alkalmazott minősítési szint és annak nemzeti minősítési szintű megfelelője:
- „TRES SECRET UE/EU TOP SECRET" - „Szigorúan titkos!";
- „SECRET UE" - „Titkos!";
- „CONFIDENTIEL UE" - „Bizalmas!";
- „RESTREINT UE" - „Korlátozott terjesztésű!".

4.4. Az Európai Bizottság által alkalmazott minősítési szint és annak nemzeti minősítési szintű megfelelője:
- „TRES SECRET UE/EU TOP SECRET" - „Szigorúan titkos!";
- „SECRET UE" - „Titkos!";
- „CONFIDENTIEL UE" - „Bizalmas!";
- „RESTREINT UE" - „Korlátozott terjesztésű!".

4.5. Az EURATOM által alkalmazott minősítési szint és annak nemzeti minősítési szintű megfelelője:
- „EURA-TOP SECRET" - „Szigorúan titkos!";
- „EURA-SECRET" - „Titkos!";
- „EURA-CONFIDENTIAL" - „Bizalmas!";
- „EURA-RESTRICTED" - „Korlátozott terjesztésű!".

4.6. Az EUROPOL által alkalmazott minősítési szint és annak nemzeti minősítési szintű megfelelője:
- „EUROPOL TOP SECRET" - „Szigorúan titkos!";
- „EUROPOL SECRET" - „Titkos!";
- „EUROPOL CONFIDENTIAL" - „Bizalmas!";
- „EUROPOL RESTRICTED" - „Korlátozott terjesztésű!".

4.7. AZ EUROJUST által alkalmazott minősítési szint és annak nemzeti minősítési szintű megfelelője:

- „EUROJUST TOP SECRET” - „Szigorúan titkos!”;
- „EUROJUST SECRET” - „Titkos!”;
- „EUROJUST CONFIDENTIAL” - „Bizalmas!”;
- „EUROJUST RESTRICTED” - „Korlátozott terjesztésű!”.

II. fejezet
A BIZTONSÁGI SZERVEZET

5. A minősített adatot kezelő szerv vezetőjének jogköre

5.1. Meghatározza a személyi, fizikai és adminisztratív biztonsági követelményeket, a minősítéssel a minősített adat felhasználásával, megismerésével kapcsolatos jogokat és kötelezettségeket.
5.2. Megállapítja a minősített adat biztonságának megsértése esetén szükséges eljárás, valamint a minősített adatok veszélyhelyzetben történő védelmi intézkedéseinek rendjét.
5.3. Kialakítja a minősített adat védelmének feltételeit.
5.4. Kijelöli az elektronikus biztonságért felelős személyek körét.
5.5. Kiadja az elektronikus rendszer biztonsági dokumentációit.
5.6. Megállapítja rejtjeltevékenység szervezeti rendjét, biztosítja a rejtjeltevékenység végrehajtásához szükséges személyi, tárgyi és biztonsági feltételeket és kiadja a rejtjelszabályzatot.
5.7. Kijelöli a rejtjeltevékenység biztonságáért felelős személyeket.
5.8. Kiadja a rejtjeltevékenységére vonatkozó rejtjel-hozzáférési engedélyeket.
5.9. Kijelöli a felhasználói engedély kiadására jogosult vezetőket.
5.10. A személyi biztonsági tanúsítvány kiadása érdekében kezdeményezi a nemzetbiztonsági ellenőrzések lefolytatását.

6. Helyi biztonsági felügyelet

6.1. A szervezet minősített adatok védelmének érdekében helyi biztonsági felügyeletet működtet.
6.2. A helyi biztonsági felügyelet ellátja a személyi, fizikai, adminisztratív, dokumentum, elektronikai és egyéb biztonsági szabályok alkalmazásának felügyeletét.

7. A biztonsági vezető

7.1. A Biztonsági vezetőt a szervezet vezetője nevezi ki a Nemzeti Biztonsági Felügyelet (a továbbiakban: NBF) elnökének egyetértésével.
7.2. A biztonsági vezető a minősített adatot kezelő szervezet vezetőjének átruházott hatáskörében eljárva – az Mavtv. irányelvei alapján – utasítási joggal gyakorolja a szervezet vezetőjének minősített adat védelmére vonatkozó jogosítványait.
7.3. Ellátja a Rendelet és a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályiról szóló 161/2010. (V.6.) Korm. rendeletben meghatározott szabályok alkalmazásának felügyeletét. Ennek keretében gondoskodik a nemzeti és a külföldi minősítéssel és jelöléssel ellátott adatok védelme érdekében meghatározott feladatok végrehajtásáról.

7.4. **Biztonsági vezető feladatai**

- gondoskodik a hivatali szervezeti egységnél a minősített adatok védelmével kapcsolatos feladatok végrehajtásáról és koordinálásáról;
- ellenőrzi a minősített adat védelmére vonatkozó személyi, fizikai, adminisztratív és elektronikus biztonsági rendelkezések megtartását,
- intézkedik a minősített iratforgalmi statisztikák minősítési szintenkénti bontásban történő elkészítéséről;
- intézkedik a nemzeti minősített adatra érvényes személyi biztonsági tanúsítványok kiadásáról, kezeléséről és tárolásáról;
- kezdeményezi a Nemzeti Biztonsági Felügyeletnél a külföldi minősített adatra érvényes személyi biztonsági tanúsítvány kiadását a NATO, NYEU és az EU minősített adatokhoz hozzáférő felhasználók és közreműködők részére;
- felügyeli a titkos ügykezelők tevékenységét;
- elkészíti a titkos ügykezelőre meghatározott tananyagot, vizsgakövetelményt, meghatározza az oktatás szervezeti kereteinek és a vizsgáztatás eljárási rendjét,
- gondoskodik a felhasználói engedély és a titoktartási nyilatkozat kiadásáról, kezeléséről, valamint tárolásáról;
- elkészíti a biztonsági szabályzatot, ellenőrzi az abban foglaltak betartását;
- intézkedik a biztonsági területre telepített biztonságtechnikai eszközöknek és rendszereknek a gyártó előírása szerinti gyakorisággal, de legalább évente egy alkalommal történő karbantartására;
- engedélyezi a személyi biztonsági tanúsítvánnyal rendelkező látogatók azonosító kártya viselése melletti önálló, kíséret nélküli mozgását a biztonsági területen, amennyiben a biztonsági területre érkező látogató biztonsági vezetője írásban igazolja, hogy a látogató személyi biztonsági tanúsítvánnyal rendelkezik;
- kezeli a biztonsági területen használt kódok megváltoztatásának tényét és időpontját rögzítő nyilvántartást;
- ellátja a Nyilvántartó(k) és Kezelő pont(ok) szakmai felügyeletét;
- a minősített adat biztonságának megsértése esetén intézkedik a minősített adat biztonságának megsértése kapcsán felmerülő kár felméréséről és enyhítéséről, valamint – ha ez lehetséges – a jogszerű állapot helyreállításáról;
- tárolja a Nyilvántartók és a Kezelő pontok (irodák, irodabútorok) tartalék kulcsait;
- rendszeresen részt vesz az NBF és a központi nyilvántartók által szervezett továbbképzéseken;
- jelen van a szervezeti egységnél végrehajtott biztonsági ellenőrzéseken;
- vezeti a jogszabályban meghatározott nyilvántartásokat;
- irányítja a helyi biztonsági felügyelet szakmai tevékenységét;
- szakmailag irányítja rendszeradminisztrátor tevékenységét;
- kezdeményezi az elektronikus biztonsághoz, és a rejtjeltevékenységhez előírt engedélyek beszerzését, gondoskodik azok nyilvántartásáról, gondoskodik a rendszerbiztonsági dokumentumok elkészítéséről;
- kivizsgáltatja a rendszerbiztonsági eseményeket;
- kapcsolatot tart a Nemzeti Hálózatbiztonsági Központtal;
- ellenőrzi az elektronikus biztonsági előírások betartását;
- irányítja a rejtjelfelügyelet tevékenységét.

8. Központi rejtjelfelügyelet vezető

8.1. A rejtjelfelügyelet vezetője irányítja a minősített adatokat kezelő szervezet rejtjeltevékenységét.

8.2. A rejtjelfelügyelet rejtjelszabályzatban állapítja meg a minősített adatot kezelő szervezet rejtjeltevékenységének szervezeti rendjét, szabályait, feladat és hatáskörét.
8.3. A rejtjel felügyelet hatáskörét, szervezeti és működési rendjét, feladatait valamint a szervezet rejtjel anyagaira vonatkozó biztonsági követelmények szabályozására a rejtjeltevékenységet végző szervezet vezetője, rejtjelszabályzatot ad ki.

9. Rejtjelző

9.1. A rejtjelző eszközöket a megfelelő szintű, az adott rejtjelző eszközre érvényes rejtjel-hozzáférési engedéllyel rendelkező rejtjelző üzemelteti.
9.2. A rejtjelzők feladatait a minősített adatokat kezelő szervezet vezetője rejtjelszabályzat rögzíti.

10. A titkos ügykezelők

10.1. Titkos ügykezelő feladatai.

11. Rendszerbiztonsági felügyelő

11.1. Rendszerbiztonsági felügyelő feladatai.

12. Személyi és fizikai biztonsági felügyeleti munkatárs

A személyi és fizikai biztonsági szakreferens a helyi biztonsági felügyelet állományába tartozó személy, akinek szakmai tevékenységét a biztonsági vezető közvetlenül irányítja.
12.1. A személyi és fizikai biztonsági szakreferens feladatai .

13. Rendszeradminisztrátor

13.1. A minősített adatok elektronikus kezelésére alkalmas rendszer üzemeltetését a rendszeradminisztrátor végzi.
13.2. A rendszeradminisztrátor feladatai.

III. fejezet
SZEMÉLYI BIZTONSÁG

14. Nemzeti és külföldi minősített adat felhasználása, megismerése és a rendelkezési jogosultság meghatározása.

IV. fejezet
FIZIKAI BIZTONSÁG

15. A fizikai biztonsági követelmények érvényesülése.

16. Fizikai biztonsági védelmi intézkedések.

17. A kulcsok kezelése.

VI. fejezet
ELEKTRONIKUS BIZTONSÁG

18. A minősített adatok elektronikus rendszeren történő felhasználásának és tárolásának (kezelésének) szabályai.

VII. fejezet
ADMINISZTRATÍV BIZTONSÁG

19. A minősítési eljárás és a minősítés szabályai.

20. A minősített adatot tartalmazó adathordozó nyilvántartásba vétele.

21. A más szervtől érkezett minősített küldemény átvétele.

22. A küldemény felbontása.

23. A minősített adathordozó továbbítására vonatkozó rendelkezések.

24. A minősítés felülvizsgálata, felül bírálata.

25. A minősített adat átadása közreműködő részére.

26. Minősített adathordozó sokszorosítása, fordítása, kivonatolása .

27. Minősített adathordozók átadása megbízás megszűnése esetén.

28. A minősített adathordozó megsemmisítése.

29. A titoktartási kötelezettség alóli felmentés.

VIII. fejezet
ELLENŐRZÉS

30. Az ellenőrzés

30.1. A minősített adatok védelmére vonatkozó szabályok megtartásának ellenőrzésére jogosultak:
a) a minősített adatok kezelésére jogosult szervezet állományából:
- a minősített adatot kezelő szervezet vezetője;
- a biztonsági vezető;
- a minősített adatot kezelő szervezet vezetője által írásban felhatalmazott személy;

b) a jogszabályban erre feljogosított más szervezet.

30.2. Az ellenőrzésről jegyzőkönyvet kell készíteni, amelyet az ellenőrzött személynek is alá kell írnia. Az ellenőrzött személy kérésére az ellenőrzéssel kapcsolatos megállapításait a jegyzőkönyvben rögzíteni kell.

30.3. Az ellenőrzés során megállapított hiányosságokról haladéktalanul írásban tájékoztatni kell a minősített adatok kezelésére jogosult szervezet vezetőjét, aki soron kívül intézkedik a feltárt szabálytalanságok megszüntetéséről, a felelősség megállapításáról.

30.4. Évente, január 02. és február 20. között e feladatra kijelölt bizottságnak ellenőrizni kell a minősített adathordozók meglétét, valamint az biztonsági szabályainak betartását. Az ellenőrzés eredményét jegyzőkönyvben kell rögzíteni, azt 10 évig meg kell őrizni.

30.5. A tikos ügykezelők és felhasználók a kezelésükben lévő minősített adathordozókat negyedévente egyszer kötelesek tételesen ellenőrizni és ennek tényét dokumentálni. Adathordozó esetleges hiányának észlelése esetén a biztonsági vezető felé jelentést kell tenni.

30.6. A tikos ügykezelők és a felhasználók, tételes ellenőrzést kötelesek végrehajtani az 50 napot meghaladó távollét esetén is a távolét (szabadság stb.) megkezdése előtt.

30.7. Az NBF elnöke, a biztonsági vezető valamint a NATO, EU, NYEU Központi Nyilvántartó vezetője – ha súlyos szabálytalanságot vagy működési zavart észlel – soron kívül is bármikor elrendelhet tételes bizottsági ellenőrzést.

IX. fejezet
A MINŐSÍTETT ADAT BIZTONSÁGÁNAK MEGSÉRTÉSE ESETÉN SZÜKSÉGES ELJÁRÁSOK, A MINŐSÍTETT ADATOK VESZÉLYHELYZETBEN TÖRTÉNŐ VÉDELME

31. Veszélyhelyzeti terv

A „Veszélyhelyzeti Terv”-ben meghatározott szabályok, feladatok és tevékenységek, alkalmazására akkor kerül sor, ha fennáll annak a veszélye, hogy a nemzeti és külföldi minősített adat illetéktelen kezekbe kerül vagy megsemmisül.

A minősített nemzeti és külföldi minősített adat biztonságának bármely módon történő megsérülését a biztonsági vezető haladéktalanul köteles dokumentálni és jelenteni az NBF-nek.

31.1. A minősített információ biztonságának megsértése esetén

32. A nemzeti és külföldi minősített adathordozóhoz való hozzáférésre kijelölt személy - különösen a titkos ügykezelő - igazolatlan távolléte esetén szükséges intézkedések

33. Az elektronikus védelmi berendezés indokolt és indokolatlan működése esetén követendő eljárás

33.2. <u>Elektronikus rendszer indokolt működésbe lépése esetén:</u>
a) A reagáló erő köteles :

33.3. Elektronikus védelmi berendezés <u>Indokolatlan működés esetén</u>
a) A reagáló erő köteles :

b) A riasztás okának kiderítése után vissza kell állítani az eredeti helyzetet.

34. A biztonsági kulcsok és tartalék példányaik, valamint a kódok lezárt borítékjai kezelésére vonatkozó szabályok.

35. Tűz, elemi csapás bekövetkezése esetén szükséges intézkedések.

35.1. Eljárásrend munkaidő alatt keletkező tűz esetén:
35.2. Eljárásrend munkaidőn kívül keletkezett tűz esetén:
35.3. Eljárásrend munkaidőben történt vízvezeték törése esetén:
35.4. Eljárásrend munkaidőn kívül történt vízvezeték törése esetén:

36. Eljárás természeti katasztrófa esetén

37. Eljárás szükségállapot esetén

37.1. Az adminisztratív zóna evakuálásának rendje:

38. Eljárás az iratkezelés szabálytalanságából adódó sérelem esetén

39. További biztonsági intézkedések

X. fejezet
ZÁRÓ RENDELKEZÉSEK

ÖSSZEFOGLALÁS

Irányadó szakemberek egyetértenek abban, hogy a minősített adatok kezelésével összefüggő szabályozás újragondolása időszerű volt. Különösen időszerűvé tették ezt az Európai Unió által megfogalmazott direktívák és az Uniós soros elnökségi feladatok is. A szabályozásban jól érzékelhetőek a komplex információvédelmi alapelvek és a komplex védelmi intézkedések alkalmazásának igénye.
A személyi, adminisztratív és a fizikai biztonsági követelményrendszer egyértelműen megfogalmazott, az akkreditációs folyamatba jól beilleszkedő, számon kérhető pontrendszeren alapuló alrendszereket alkotnak. Az viszont tapasztalati tény, hogy a közigazgatás nincs felkészülve a fizikai biztonsági követelmények teljesítésére, annak ellenére sem, hogy a szabályozás haladékot ad a szervezetek számára a megvalósítást illetően.
Az elektronikus védelem területén viszont irányadó szakemberek szerint is további egységes és világos követelményrendszer megfogalmazása szükséges, különösen a minősített adatok elektronikus rendszereken történő kezelésével és továbbításával összefüggésben.
Ezt különösen fontos kiemelni, hiszen napjainkban szinte minden minősített adat, elektronikus adathordozón kerül előállításra, tárolásra, feldolgozásra és többnyire aminősített adatok elektronikus továbbításával összefüggésben fogalmazódnak meg a felhasználói igények. Ugyanakkor a közigazgatás nem tudja értelmezni – és nem is érti – az elektronikus védelmi intézkedések kialakításának szükségességét és rendszerint a túlzott anyagi erőforrásokra (illetve annak hiányára) hivatkozva vonakodik teljesíteni az ezzel összefüggő beruházásokat.

FELHASZÁLT IRODALOM

[1] A minősített adat védelméről szóló 2009 évi CLV. törvény

[2] A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010.(III.26.) Korm. rendelet. (58.§ (1),(2))

[3] A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Korm. rendelet. 49§-51§

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

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

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

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

[8] Kassai Károly Az elektronikus adatkezelés során szükséges személyi biztonság kérdései.(Hadtudományi Szemle 3. évfolyam 3. szám 2010. 1. oldal)

[9] A Nemzeti Biztonsági Felügyelet elnökének (*NBF bemutatása biztonsági vezetőknek.ppt 2010.11.12)* előadása.

[10] A telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendelet.