Dr. Rajnai Zoltán alezredes- Kerti András őrnagy:

Információbiztonság és rejtjelfelügyelet

Ha valaki végig böngészte az ez évi „Felsőoktatási felvételi tájékoztatót”, megakadhatott a szeme a Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar, Védelmi vezetéstechnikai rendszerszervező mester szak, egyik szakirányán, a rejtjelfelügyeleti szakirányon. Cikkünkben szeretnénk választ adni azokra a kérdésekre, melyek a szakirány specialitásaira, az oktatandó ismeretanyagra vonatkoznak, valamint ismereteket szeretnénk adni arról, hogy milyen munkakörök ellátására lesznek képesek a szakirányt elvégző hallgatók.

Ki minősül rejtjelfelügyelőnek?

Mindenki, akinek titkai vannak, szeretné azokat elrejteni az illetéktelenek elöl, és minél több az elrejtendő információk mennyisége annál kifinomultabb, precízebb a titkos információk elrejtésére használt rendszer. Az állami szervek működése ráadásul különböző jogszabályokon alapul. Megítélésünk szerint ebben a témakörben a legfontosabb jogszabály a 1995. *évi LXV. Törvény az államtitokról és a szolgálati titokról (továbbiakban: Ttv.), valamint* a törvény alapján megalkotott *79/1995. (VI. 30.) Kormány rendelet a minősített adat kezelésének rendjéről.*

A titokvédelmi törvény 18 § (4) pontja alapján:”A Ttv. 3. § (1) bekezdés, valamint a 4. § (1) bekezdés hatálya alá tartozó adatot (államtitok és szolgálati titok) külföldre, vagy külföldről vezetékes és vezeték nélküli adatátviteli rendszerben is - *kizárólag rejtjelezve* - továbbítható.”

Szintén rejtjelzési kötelezettséget ír elő A Kormány rendelet 27 § (7) bekezdése: „Számítástechnikai rendszerben, illetve mágneses vagy más rendszerű adathordozón csak rejtjelezve tárolhatók azok az államtitkot vagy szolgálati titkot tartalmazó adatok, amelyek megbízható védelme más úton nem biztosítható.” Ugyanígy a 31 § kinyilvánítja, hogy „Vezetékes vagy vezeték nélküli adatátviteli rendszerben minősített adatot, ha a továbbított adat a megbízható védelem és felügyelet határain kívülre kerül, így különösen a titokvédelemre kötelezett szervezet megfelelően zárt vagy védett területét elhagyja, csak rejtjelezve szabad továbbítani.”

Tehát azon állami szerveknek, szervezeteknek akik minősített adatokat továbbítanak, a rejtjelzés nem csak jól felfogott érdeküknek, de jogszabályi kötelezettségük is. A rejtjeltevékenység szervezeti kereteit a 43/1994. (III. 29.) „Kormány rendelet a rejtjeltevékenységről” szabja meg, mely kifejezetten rövidek, tömörnek mondható, és kizárólag irányelv jellegű. Például a szervezet vezetőjének feladatául szabja: ”A rejtjeltevékenységet folytató szervezet vezetője a vonatkozó jogszabályok keretei között megállapítja a szervezet rejtjeltevékenységének szabályait, szervezeti rendjét, kiadja az ezeket rögzítő rejtjelszabályzatot;”[1] Könnyen belátható, hogy ez a pár sor is milyen hatalmas munkát jelent, jelenthet a szervezetre nézve. Az is nyilvánvaló, hogy ezt a munkát nem személyesen a szervezet vezetője fogja végrehajtani, hanem a szervezet rejtjelfelügyelője, illetve a rejtjelfelügyelet. A 43/1994. kormányrendelet e téren megállapítja:

[1] 8§ a) bekezdés. A kormányrendelet természetesen még más feladatokat is meghatároz, ezt a pontot csak a példa kedvéért ragadtuk ki.

„A rejtjeltevékenységet folytató szervezet a rejtjelszakmai munka - *különösen a rejtjelzési feladatokat ellátó szolgálatok (a továbbiakban: rejtjelző szolgálatok) munkájának* - irányítása és felügyelete érdekében a feladatok jellegétől és mértékétől függően legalább egy rejtjelfelügyelőt jelöl ki, illetve rejtjelfelügyeletet hoz létre."[2]

Felsőfokú rejtjelző szakemberek képzése utoljára a Zalka Máté Katonai Műszaki Főiskolán volt az 1970-es években. Az akkori technikai színvonalnak megfelelően a képzés főképpen a technikai eszközök üzemeltetésére koncentrált. Az azóta eltelt időszakban a rejtjelfelügyeleteken a szakemberek pótlását más szakterületekről érkezőkkel pótolták, akik a szaktudásuk nagyobb részét már a rejtjelfelügyeleteken dolgozóktól, munkaközben tanulták meg, majd később szakmai továbbképzéseken, átképző tanfolyamokon sajátították el a szükséges ismereteket.[3] A Zrínyi Miklós Nemzetvédelmi Egyetem Híradó Tanszéke – *a korábbi évek, évtizedek tapasztalatai és az említett képzési űrt betöltése érdekében* – célul tűzte ki, hogy a bolognai folyamatnak[4] megfelelően 2007 szeptemberétől Mester (továbbiakban MSc) képzésben, levelező formában korszerű rejtjelfelügyeleti ismeretek megszerzését kínálja a fegyveres erők és a rendvédelmi szervek, valamint polgári érdeklődők részére.

Milyen szaktudásra van szükség?

A tananyag tervezésekor figyelembe vettük a ZMNE-n folyó információvédelmi tanfolyamok tananyagát, a tárgyhoz tartozó jogszabályokat, a tanár kollégák szakmai tapasztalatát, az MH-ban rejtjelzés szakterületén dolgozók véleményét és az egyéb nyílt forrásokban megtalálható ismeretanyagot. Első látásra könnyű dolgunk adódott mivel az egyetemünkön évek óta rendszeresen tartott rejtjelző átképző tanfolyam anyagát, tanáraink ezen a tanfolyamon szerzett tapasztalatát fel lehet (és kell) használni az oktatás alapjául. Azonban ez tényleg csak a látszat, hiszen ezek a tanfolyamok kizárólag a HM és HM alárendeltségébe tartozó rejtjelző beosztást betöltők részére szóltak. A 43/1994. kormányrendelet már említett 8§-a minden szervezet számára kötelezővé teszi saját rejtjelszabályzat megalkotását, és sehol sem olyan fontos a „szükséges, hogy tudja" elv betartása, mint a rejtjelzés területén. Ebből kifolyólag teljesen az elején kellett keresnünk a megoldást: Milyen ismeretekkel kell rendelkeznie egy a rejtjelzés területén tevékenykedő vezető beosztású egyénnek?

Először is mi a rejtjelzés? A kormányrendelet 1§-ban megfogalmazottakon[5] túl a rejtjelzés az elektronikus információvédelem egyik speciális szakterülete, ebből kifolyólag a rejtjelfelügyelőnek tisztában kell lennie az alapvető biztonsági kérdésekkel, mégpedig a fizikai, személyi, és dokumentum biztonság feladataival, lehetőségeivel. Az sem árt, ha rejtjelfelügyelő minél jobban tisztában van az elektronikus információvédelem egyéb szakterületeivel, mint számítógép és hálózatbiztonság, átvitelbiztonság, kisugárzás biztonság.

Másodszor tisztáznunk kell: mi a feladata a rejtjelfelügyelőnek? A kormányrendelet 10§ (1) pont alapján „A rejtjelfelügyelet vezetője a szervezet vezetője által meghatározott körben rejtjel szakmai kérdésekben a szervezet vezetőjének nevében jár el", vagyis a rejtjelzéssel kapcsolatos effektív munkát ő végzi, amire szintén a rendelet így rendelkezik:

„a) a vonatkozó jogszabályok keretei között megállapítja a szervezet rejtjeltevékenységének szabályait, szervezeti rendjét, kiadja az ezeket rögzítő rejtjelszabályzatot;

---

[2] 6§ (1) bekezdés

[3] 2002-től a BJKMF és jogutódján folyamatosan folynak rejtjelző átképzések

[4] Az európai felsőoktatási térség egységes képzési rendszere

[5] Röviden: „Rejtjelezés: minden olyan tevékenység, eljárás, amelynek során valamely adatot abból a célból alakítanak át, hogy annak eredeti állapota a megismerésére illetéktelenek számára rejtve maradjon. A rejtjelzés részét képezi a rejtjelzett adat eredetivé való visszaállítása is."

b) megállapítja a szervezet rejtjeltevékenységének tartalmát, terjedelmét, a szervezet rejtjelkapcsolatait;

c) biztosítja a rejtjeltevékenység szervezeti, személyi, tárgyi és biztonsági feltételeit;

d) gondoskodik arról, hogy a rejtjeltevékenységgel kapcsolatos, védelem alá eső információkat csak azok a személyek ismerhessék meg, akiknek a munkájához az feltétlenül szükséges, és arra a megfelelő engedélyekkel rendelkeznek."

A *c)* és *d)* pontok tartalmával más aspektusból de már foglalkoztunk. Az *a)* és *b)* pontokból következik, hogy a rejtjelfelügyelőnek ismerni kell a jogszabályi környezetet. Nagyon jól kell ismernie a szervezete által védendő információk áramlásának rendjét, melyből következik, hogy a saját szervezetét is jól kell ismerni. Tisztában kell lennie az infokommunikációs rendszerek szervezésének elveivel, az alkalmazott, technikai eszközök mind a rejtjelző, mind az infokommunikációs eszközök paramétereivel. Továbbá a 17§-t figyelembe véve megállapíthatjuk, hogy a rejtjelfelügyelőnek tisztában kell lennie az iratkezelés általános és speciális követelményeivel.

Általános vezetői ismeretek
Info-kommunikációs rendszer ismeret
Általános Információbiztonsági ismeretek
Jogszabályi Ismeretek
Ügyviteli ismeretek
Speciális szervezeti ismeretek
Speciális rejtjelző ismeretek

1. ábra: A rejtjelfelügyelő munkájához szükséges ismeretanyag

Az 1. ábra mutatja, hogy a rejtjelfelügyelőnek milyen ismeretanyagokra van szüksége munkája ellátásához.

A tananyag felépítése

A tervezett tananyagot az MSc képzés 4 féléves képzési rendszerében alakítottuk ki, amelynek a felépítését az mutatja:

Tananyag	Félév	Kredit
Természettudományi alapismeretek	1	20
Gazdasági és humán ismeretek	1	10
Szakmai törzsanyag	2	20
Differenciált szakmai anyag	2	10
Differenciált szakmai anyag	3	30
Szabadon választott tantárgyak	4	10
Diplomamunka kidolgozás	4	20

1. táblázat: A infokommunikációs rendszerszervező mester (msc) szak tanterve

A természettudományi alapismeretek és a humán ismeretek olyan alapvető (általános) ismeretek oktatását jelentik amelyek szükségesek egyrészt az MSc végzettségű szakemberek

számára, másrészt megalapozzák szakmai tanulmányaikat. Mint minden Msc képzés, a rejtjelfelügyeleti szakirány is alap- (továbbiakban BSc) képzésre alapoz. Mivel ilyen jelegű alapképzés korábban nem volt, ezért a követelmények kialakításakor a Nemzetvédelmi Egyetem és jogelődjei által *folytatott híradó, villamosmérnök szakok képzési* formáit vettük figyelembe. Amennyiben a jelentkezők nem rendelkeznek az előírt tárgyak mindegyikéből a felelő kredit ponttal (ismeretanyaggal), biztosítunk számukra lehetőséget a különbözeti tananyag elsajátítására. Természetesen ez a beiratkozott hallgatóinknak többlet munkát jelent.

A szakmai törzsanyag a szakra jellemző általános ismeretek oktatását jelenti amelyek szükségesek a szakirány megalapozásához, a szabadon választott tantárgyak pedig a hallgatók érdeklődési körének megfelelő tárgyak tanulását teszik lehetővé. A diplomamunka elkészítésével a hallgatók bizonyíthatják az önálló kutató munkára való kézségüket. A fent leírtak természetesen a védelmi vezetéstechnikai rendszerszerező szak valamennyi választható szakirányára vonatkoztathatóak. Most nézzük meg mitől más a rejtjelfelügyeleti szakirány, vagyis milyen specialitást tartalmaz a differenciált szakmai anyag, amelynek felépítését a tartalmazza:

Tantárgy	**kredit**
Fizikai, személyi és dokumentumbiztonság	2
Informatikai rendszerek biztonsága	2
Elektronikai támadás és védelem	4
Számítógép-hálózatok elleni támadások	2
Kommunikációs rendszerek szervezése	8
Kommunikációs rendszerek biztonsága	8
Rejtjelbiztonság elmélete és megvalósítása	14

2. Táblázat: A rejtjelfelügyelők differenciált szakmai tananyag felépítése

Ha megnézzük a tantárgyak nevét láthatjuk, hogy a kialakításukkor alapvetően az általános információbiztonsággal, és a védelmi szférára jellemző speciális információbiztonsággal foglalkozó tárgyak kerültek a differenciált szakmai törzsanyagba.

A kifejezetten rejtjelfelügyeleti munkával foglalkozó tantárgyunk a „Rejtjelbiztonság elmélete és megvalósítása”. Első pillantásra is szembetűnik a többi tantárgyhoz képest a nagy kredit pontszám. Felmerülhet a kérdés: ez egy tantárgy, vagy több? A tantárgy kialakítása során bennünk is felmerült, hogy több kisebb kredit pontszámú tárgyat kellene kialakítani, de végül is azért döntöttünk így, mert ezzel a megoldással a tantárgy későbbi belső struktúrájának változtatásakor nagyobb oktatói szabadságot kaptunk. A rejtjel felügyeleti szakirány Msc képzésben való megjelenítésekor még járatlan úton haladunk, ami számunkra azt jelenti, hogy legnagyobb igyekezetünk ellenére sem biztos, hogy teljes mértékben elérjük a megfelelő arányokat az oktatott területek között. A reményeink szerinti több évfolyamon keresztül *oktatjuk ezt a szakirányt* és e közben az igényeknek és a megváltozott környezethez igazítva áttervezhetjük, figyelembe vesszük a hallgatói véleményeket és visszajelzéseket, amelyek során a tantárgyak struktúráját módosíthatjuk a kihívásoknak megfelelően.

Magát a tananyagot alapvetően három témakör köré csoportosítottuk, nevezetesen: a rejtjelzés története és a kriptográfiai alapok, a jogszabályi környezet, és a rejtjelző rendszerszervezés és üzemeltetés. Az első részben olyan általános rejtjelző tájékozottság elérése a cél, amely a megítélésünk szerint, a napi általános munkában ugyan nem a fontosabbak közé tartozik, de egy Msc képesítést elérő rejtjelfelügyelőnek hozzá tartozik az

alapműveltségéhez. Ebben a tantárgy csoportban szerepelnek a kriptográfiai alapok, de nem célunk kriptográfus szakemberek képezése[6], mert ez inkább a matematika szakterülete, mint a rejtjelfelügyeleté. Itt alapvetően csak az alapokat adjuk meg ahhoz, hogy szükség, illetve érdeklődés esetén a továbbfejlődés lehetőség biztosítva legyen. Mint azt az 1. ábra mutatja, a rejtjelfelügyelő szakmai tudásanyagának jelentős hányadát a jogi ismeretek teszik ki, ezért a tantárgy második részterülete jogszabályi környezetet mutatja be. Annak ellenére, hogy ennél a résznél sem célunk a hallgatók szakjogásszá történő átképzése, szeretnénk átfogni az információvédelemmel, ezen belül a rejtjelzéssel kapcsolatos jogszabályok teljes skáláját. Ez első látásra nem tűnik nagy tananyag résznek, de aki már foglalkozott a témával tudja, hogy ez a jelenlegi jogszabályi környezetben nem egyszerű feladat. A rejtjelfelügyelőnek azonban a munkája végzése folyamán tisztában kell lennie az előírásokkal és az esetleges szankciókkal is.

A harmadik része a tananyagnak a legterjedelmesebb és kiindulópontját a 43/1994 Kormány rendelet adja, amely szerint – *egyszerű megfogalmazásban* – a szervezetnek meg kell terveznie, szerveznie és üzemeltetnie a rejtjelzést, és fel kell állítania a rejtjelfelügyelete(ke)t. Nem valószínű, hogy a végzett hallgatóink olyan szakmai környezetbe kerülnek ahol még senki nem foglakozott rejtjelzéssel, de elvileg ez sem kizárt. Ebből az aspektusból kiindulva úgy állítottuk össze a tananyagot, hogy a kezdeti lépésektől a folyamatos üzemeltetésig logikailag egységben, folyamatszemléletű megközelítést biztosítson. Mint arról már szó volt, a tananyag kialakításánál nem vehettünk figyelembe, minősített és bizalmasan kezelendő anyagokat[7], ezért – *a jogszabályokon kívül* – az információvédelem területén jelenleg érvényben lévő magyar és nemzetközi szabványokat, illetve a nyílt forrásból elérhető anyagokat vettük alapul. Úgy gondoljuk, hogy a szabványok nem igényelnek különösebb magyarázatot, de mire kell gondolunk a „nyílt forrásoknál", azt egy példán keresztül szeretnénk bemutatni. Az, hogy a rejtjelzés egyik sarkalatos kérdése a kulcs elosztás, szinte minden szakirodalomban megtalálható, és megtalálhatók az elméleti megoldási lehetőségek is Ez egy nyílt forrásból származtatott információ. Azonban az, hogy egy adott szervezet a saját „kerítésén" belül hogyan oldja meg a kulcselosztás problémáját, lehet, hogy – *a szervezettől függően* – államtitoknak minősül. A sort még folytathatnánk további példákkal is.

Összegzés

„Minden diploma annyit ér, amennyit pirulás nélkül elmondunk róla.[8]" Szeretnénk egy olyan diplomát a hallgatóink kezébe adni sikeres végzés után, amelyről elmondható, hogy hasznos a tulajdonos, a szervezet számára. A fentiekből az is megállapítható, hogy amennyiben nem a kezdeti lépésektől alkotja meg szervezete rejtjelzési folyamatait és állítja fel a rejtjelfelügyeletet a friss diplomával rendelkező rejtjelfelügyelőnk, akkor azonnal nem tudja megkezdeni feladatát, mert előtte meg kell ismernie a szervezet struktúráját, specialitásaikat. Ez az ismeretanyag a specialitások sokrétűsége miatt nem oktatható egzakt módon, csupán megoldási alternatívák tanulmányozása segíthet a későbbi munkafolyamatok ellátásában. Reményeik szerint a rejtjelfelügyelői szakirány hallgatói részére olyan ismeretanyagot adunk hallgatóink kezébe, amellyel zökkenőmentesen tudnak be illeszkedni a szervezetek meglévő keretei és munkafolyamatai közé. És ha mégsem fog a végzett hallgató rejtjelfelügyelőként dolgozni? Nos akkor reméljük, hogy olyan elektronikus információvédelmi alapokat szerzett, melyeket akkor is fel tud használni, ha a kommunikációs

[6] És ehhez a képzéshez sem a rendelkezésre álló időt, sem az ez irányú felkészültségünket nem érezzük elegendőnek.
[7] Nem keverendő össze a „Bizalmas" minősítéssel
[8] Dr Nagy László előadása,Vállalati belső auditor képzés, ZMNE 2008. február 11-13.

és informatikai rendszerek szervezésével és tervezésével kapcsolatos munkakörökben lát majd el beosztásokat.

A ZMNE Védelmi Vezetéstechnikai Rendszerszervező szak rejtjelfelügyeleti szakiránya az első, és egyetlen képzési forma és lehetőség a szakterület iránt érdeklődők és az ott dolgozók egyetemi szintű diplomájának megszerzéséhez. Ajánljuk a Honvédelmi Minisztérium, az Igazságügyi és Rendvédelmi Minisztérium, valamint a Katasztrófavédelem szakterületein dolgozók részére. (A felsőoktatási jelentkezés határideje: 2008. március 15.)

Felhasznált irodalom:

1. 1995. *évi LXV. Törvény az államtitokról és a szolgálati titokról*
2. *79/1995. (VI. 30.) Kormány rendelet a minősített adat kezelésének rendjéről.*
3. *43/1994. (III. 29.) Kormány rendelet a rejtjeltevékenységről*
4. *Kérelem a védelmi infokommunikációs rendszerszervező mester (msc) szak indítására ZMNE Budapest 2005*