Óbudai Egyetem

Doktori (PhD) értekezés

Az emberi tényező szerepe az információbiztonság megvalósítása és erősítése terén. Az információbiztonsági kultúra fejlesztésének lehetőségei a Magyar Honvédségben

Mógor Tamásné

Témavezető:
Prof. Dr. Rajnai Zoltán

Biztonságtudományi Doktori Iskola

Budapest, 2017

Szigorlati Bizottság:

Elnök: Prof. Dr. Berek Lajos egyetemi tanár, ÓE

Tagok: Dr. habil. Farkas Tibor docens, NKE

Dr. Tóth András adjunktus, NKE

Nyilvános védés bizottság:

Elnök: Prof. Dr. Berek Lajos egyetemi tanár, ÓE

Titkár: Dr. Szűcs Endre adjunktus, ÓE

Tagok: Dr. Magyar Sándor adjunktus, NKE

Dr. Bérczi László tű. dandártábornok,

Dr. Horváth Zsolt László adjunktus, ÓE

Bírálók: Dr. Bozsó Zoltán c. r. dandártábornok,

Dr. habil. Michelberger Pál docens, ÓE

TARTALOMJEGYZÉK

BEVEZETÉS

A tudományos probléma megfogalmazása

Doktori értekezésem az információbiztonság megteremtésének, erősítésének humán vonatkozásaival foglalkozik, különös tekintettel az információbiztonsági kultúra kialakításának és fejlesztésének lehetőségeire. Disszertációmban vizsgálom az EMBER szerepét az információbiztonság megteremtésében és fenntartásában. Gyakorlati tapasztalataimra, többéves megfigyeléseimre és információgyűjtő tevékenységemre építve megállapítom, hogy az EMBER – mint az információbiztonság megteremtésének „alappillére" – csekély figyelmet és támogatást kap e területen. Fontosnak tartom kihangsúlyozni azt a tényt, hogy az információbiztonsági incidensek legnagyobb része emberi mulasztás miatt következik be. Az emberi tényező vizsgálatának és értékelésének az elhanyagolása miatt már évek óta foglalkoztat a kérdés: hogyan, mely módszerekkel fejleszthető a biztonsági kultúra, milyen lehetőségek állnak rendelkezésre a biztonságtudatos viselkedés kialakítására, motiválására.

Meggyőződésem, hogy a biztonsági kultúra fejlesztésének kiindulópontja az oktatás, ezért értekezésemben nagy hangsúlyt fektetek az információbiztonsági képzés jelenlegi helyzetének bemutatására, fejlesztésének lehetőségeire. Az oktatás mellett tanulmányozom és kutatom azt, hogy egy alkalmassági vizsgálat bevezetése mennyiben járulna hozzá az információbiztonság színvonalának emelkedéséhez a Magyar Honvédségben (a továbbiakban: MH).

A témaválasztás indoklása

2008–tól 2012–ig a Zrínyi Miklós Nemzetvédelmi Egyetem (továbbiakban: ZMNE), majd 2012–től 2013–ig a Nemzeti Közszolgálati Egyetem (a továbbiakban: NKE) Híradó Tanszéken dolgoztam gyakorlati oktatóként. Az oktatói munka mellett rejtjelanyagok titkos ügykezelője, minősített adatok feldolgozására feljogosított számítógép rendszerbiztonsági felügyelője voltam, valamint több mint 5 éven át szerveztem a Honvéd Vezérkar Híradó, Informatikai és Információvédelmi Csoportfőnökség (a továbbiakban: HVK HIICSF) felkérésére szakmai tanfolyamokat. A HVK HIICSF jóvoltából számos akkreditáláson és Nemzeti Biztonsági Felügyeleti (a továbbiakban: NBF), valamint NATO szintű szakmai ellenőrzéseken is lehetőségem volt tapasztalatot szerezni.

Az évek folyamán több tanfolyamot magam is elvégeztem, valamint számos tanfolyamon oktatóként is részt vettem. Az évente megrendezett konferenciákon és továbbképzéseken is jelen voltam, hogy szakmai tudásomat fejlesszem, naprakész legyek a szakmai újdonságokat és jogszabályi változásokat illetően. Ezeken a rendezvényeken és az általam lebonyolított tanfolyamok alkalmával a szakterületen dolgozó személyek nagy részével megismerkedtem, az

évek során kiváló szakmai és emberi kapcsolatokat sikerült kialakítanom. A disszertáció elkészítése során figyelmet fordítottam arra, hogy a megszerzett tapasztalatok, összegyűjtött információk felhasználásra kerüljenek. Az információbiztonság területén dolgozó szakemberekkel folytatott szakmai beszélgetések, személyes interjúk és megfigyelések eredményei megerősítették bennem azt az elhatározást, hogy az információbiztonság humán tényezőivel foglalkozzak.

Témaválasztásom egyik oka a humán biztonság felé irányuló érdeklődésem. Témaválasztásom másik oka, hogy az információbiztonság kérdése – benne a humán biztonság – napjainkban egyre fontosabb és kiemeltebb szerepet kap, tehát ez a téma rendkívül aktuális.

Kutatási célok

1. Célként fogalmaztam meg, hogy olyan értekezést készítsek, amely elősegítheti az információbiztonsági kultúra fejlesztésének lehetőségeit az MH – ban, ezzel együtt célom volt, hogy kutatásom megfelelő alapot teremtsen a terület további tudományos elemzéséhez és vizsgálatához.

2. Kulcscélként jelöltem meg azt, hogy igazoljam az EMBER meghatározó szerepét az információbiztonság elleni mulasztások bekövetkezésének okai között.

3. Kiemelt célként határoztam meg az információbiztonsági kultúra fejleszthetőségének vizsgálatát, ezzel egyidejűleg az információbiztonsági tudatosság erősítésének támogatását.

4. Ugyancsak célként fogalmaztam az információbiztonsági képzés jelenlegi helyzetének a bemutatását az MH–ban. Hangsúlyozni kívánom az oktatás kiemelkedő szerepét az információbiztonsági tudatosság fejlesztése terén.

5. Speciális célként jelöltem meg egy új, többlépcsős tanfolyami rendszer lehetőségeinek bemutatását.

6. Sajátos célom volt annak bizonyítása, hogy az információbiztonsági munkaköröket betöltő, vagy minősített adatokkal dolgozó személyek előzetes speciális alkalmassági vizsgálata hozzájárulhat az információbiztonsági incidensek számának és mértékének csökkenéséhez.

7. Végül pedig személyes célom az volt, hogy be tudjam mutatni a dolgozatban megjelenő tudományterületek közötti összefüggéseket, és ezek egymásra gyakorolt hatását.

Hipotézisek

1. Feltételezem, hogy az információbiztonsági incidensek gyakori előfordulásához jelentős mértékben hozzájárul a humán faktor, ezért kiemelt figyelmet kell fordítani az emberi tényezőre.
2. Feltételezem, hogy az információbiztonsági kultúra és az információbiztonsági tudatosság fejlesztésének a kérdése nem kap elég hangsúlyt az MH–ban.

3. Feltételezem, hogy a biztonságtudatosság erősítésének elengedhetetlen tényezője a színvonalas oktatás, szakmai képzés és ezek előtérbe helyezése.

4. Feltételezem, hogy az információbiztonsági képzések követelményrendszerének és tematikájának átdolgozása, frissítése elősegítené az eddiginél hatékonyabb és könnyebben alkalmazható képzés megvalósítását.

5. Feltételezem, hogy a Magyar Honvédségen belüli általános alkalmassági kiválasztási rendszeren túl egy szakma specifikus szűrőrendszer hozzájárulna az információbiztonság szintjének emelkedéséhez, az információbiztonsági kockázatok csökkentéséhez és az információbiztonság elleni incidensek megelőzéséhez.

Kutatási módszerek

A téma jellegéből, összetettségéből adódóan a kutatási módszerek tekintetében szükségszerű az interdiszciplináris megközelítés alkalmazása. Ez abból következik, hogy az információbiztonság témakörét több tudományterület szempontjából vizsgáltam. Ilyen releváns társadalomtudomány a pszichológia, a jog a pedagógia és a didaktika. Mindezek figyelembevételével lényegesnek tartottam az interdiszciplinaritás elvének megfelelő megközelítést és feldolgozást.
Kutatómunkám során törekedtem az elméleti összefüggések és a gyakorlati alkalmazás komplex vizsgálatára. Elméleti kutatásomban a hatályos jogszabályok figyelembevételével közelítettem meg a kérdéseket, amelyek végén a gyakorlati megvalósíthatóság elvét tekintettem célként.
A forrásanyagok feldolgozása, saját kutatásomban történő felhasználása, integrálása, tapasztalatainak leszűrése érdekében felhasználtam az analízis és a szintézis nyújtotta módszereket.
A dokumentum – és kutatáselemzéseket minden esetben saját kutatási témámhoz kapcsolódóan végeztem. Célom volt egy – az ok-okozati összefüggéseket láttató – átfogó munka megalkotása.
A személyes interjúk és megfigyelések hozzájárultak ahhoz, hogy a végkövetkeztetések pontosan tükrözzék az információbiztonsági kultúra jelenlegi helyzetét az MH – ban.
Kérdőívet készítettem biztonsági vezetők részére, amelynek tapasztalatai a kutatásomhoz kiindulási alapot nyújtottak.

Különös figyelmet fordítottam a gyakorlati tapasztalatok elemzésére, az értékelhető következtetések megfogalmazására.

1. AZ INFORMÁCIÓBIZTONSÁG, MINT A BIZTONSÁGTUDOMÁNY RÉSZTERÜLETE

Bevezetés

Az 1. fejezetben a biztonságtudomány egyik fontos területét, az információbiztonságot ismertetem.

Az információbiztonság a biztonságtudomány részterülete, az a folyamat, melynek során az információkat megvédjük a nem engedélyezett hozzáféréstől, használattól, kiszivárgástól, megsemmisítéstől, módosítástól és megzavarástól. Az információbiztonság megvalósulása természetes számunkra, de hiánya azonnal feltűnik. Ezért nagyon fontos, hogy ne csak akkor fordítsunk rá kellő figyelmet, amikor az információbiztonság sérül, hanem biztosítsunk komplex, megelőző védelmet.

1.1 Történelmi áttekintés

Az információ megszerzése és védelme, vagyis az információbiztonság évezredek óta foglalkoztatja az emberiséget. A történelem vizsgálata során megfigyelhetjük, hogy a XX. század közepéig a társadalmak politikai, gazdasági és egyéb mozgásait két fontos tényező motiválta: egyrészt a terület megszerzése és megtartása, másrészt a nyersanyagokhoz való hozzáférés, ezek birtoklása és elzárása.

A kezdetleges számítógépek megjelenésekor, majd később a fejlett, adatkezelő rendszerek kifejlesztésével az információ megszerzésének és védelmének jelentősége, módja is megváltozott.

A 19. század végétől kezdve olyan dinamikus változások kezdődtek az egész világon, melyek az élet minden területén gyors fejlődést, átalakulást eredményeztek. Gondoljunk csak a közlekedés, híradás, energetika területére, melyek rendkívüli előrelépést hoztak az emberiség életében, ugyanakkor sérült az egyén, a közösségek, országok, földrészek, vagyis az egész világ biztonságérzete. Az 1900–as évek közepétől az ember már nem tudta felvenni azt a dinamikát, amit az információs fejlődés diktált. Ettől az időszaktól kezdve az energia vált fő értékké, a stratégiák célkeresztjébe az energiaforrások birtoklása, és a technikai fölény megszerzése került. Mérföldkövet jelentett, hogy a változások mozgatórugói az információ, a kommunikáció, a humán erőforrás, a jogalkalmazás és a globalizáció lettek. Ennek következtében az 1900–as évek közepétől egyre jelentősebb szerepet kapott a biztonság kérdése. [1]

Az információbiztonság történeti fejlődésének vizsgálatakor hangsúlyt szükséges fektetni a kriptográfiára és annak átalakulására. A kriptográfia[1] gyökerei tulajdonképpen egészen az ókorig nyúlnak vissza, de általánosságban elmondható, hogy a kriptográfia egészen a XX. századig inkább művészet volt, ami olyan fejlődésen ment keresztül, amely nem volt tudatos. Már ie. 800 körül megfigyelhető volt a Káma Szútra szerelmeseinek kommunikációjában a titkosírás. Az arab világban 1000 körül fedezték fel a kriptoanalízist,[2] az 1400-as években pedig egyre elterjedtebbé vált a titkosírás a diplomáciai levelezésekben. Az első kriptográfiával foglalkozó nyomtatott könyv 1518-ban jelent meg, melyet Johannes Trithemius spanheimi apát írt Poligraphiae címmel. 1586-ban kriptoanalízis segítségével Sir Frencis Walsingh I. Erzsébet királynő államminisztere rábizonyította a Babington – összeesküvés[3] résztvevőire bűnösségüket. 1793-ban Claude Chappe[4] létrehozta az első nagytávolságú szemaforjelzéseket használó kommunikációs vonalat. 1795-ben Thomas Jefferson[5] megalkotta a Jefferson korongok rejtjelző szerkezetet és módszert, melyet egy évszázad múlva Etienne Baseries[6] újra felfedezett.

1837-ben Samuel Morse[7] megtervezte és szabadalmaztatta az elektromos telegráfot, és megalkotta a Morse kódot[8].

1917-ben történelmi fordulatot jelentett, hogy a brit hírszerzés elfogta, és megfejtette Arthur Zimmermann táviratát, ami miatt az USA belépett az I. Világháborúba. Jelentős előrelépést hozott Arthur Scherbius 1918-ban ENIGMA néven szabadalmaztatott titkosító gépe és Hugo Alexander Koch rotor alapú titkosító gépe 1919-ben.

A kriptográfia igazi áttörése azonban csak a II. Világháborúhoz köthető, amikor az információszerzés a hadműveleti, harcászati siker elérése érdekében minden korábbinál fontosabbá vált. A II. Világháború tapasztalatainak levonása után 1948-ban Claude E. Shannon[9] kezdeményezésére kialakult az információelméletnek nevezett tudományág.

Az Amerikai Egyesült Államokban már az 1970-es években teret hódított az információbiztonsági értékelés hatékony rendszerének kidolgozása, előtérbe helyezése. A szakemberek belátták, hogy a biztonság magas szintje csak korszerű védelmi, biztonságtechnikai rendszerekkel valósítható meg. Elismerték azt is, hogy az integrált, komplex biztonság, és a

[1] Görög eredetű szó; kriptos = eltitkolt, elrejtett + graphein = írni
[2] Kriptográfiai rendszerek elemzése, és feltörésének kutatása
[3] A második legnagyobb összeesküvés I. Erzsébet királynő ellen, ami Stuart Mária kivégzéséhez vezetett
[4] Francia feltaláló, 1763 és 1805 között élt.
[5] Az USA harmadik elnöke, 1743 és 1826 között élt, szakterülete többek között a kriptográfia volt.
[6] Kriptoanalízissel foglalkozó feltaláló, 1890-től az I. Világháborúig a francia hadseregben tevékenykedett.
[7] Amerikai feltaláló, 1791 és 1872 között élt
[8] Olyan kommunikációs kód, amely szöveges információ átvitelét teszi lehetővé vezetékes és vezeték nélküli kommunikációs csatornán.
[9] Matematikus, hírközlési szakember

magas biztonsági szint elérésének alapvető követelménye, hogy figyelemmel kell kísérni az adott rendszert, feltárni, elemezni a kockázatokat, amelyek veszélyeztetik annak működését. Ezek figyelembevételével lehetséges a kockázatok szintjét és mennyiségét úgy lecsökkenteni, hogy a lehető legbiztonságosabb működés valósulhasson meg.

Hatalmas előrelépésnek könyvelhetjük el, hogy mindez még az ezredforduló előtt átterjedt Európára, ezen belül Magyarországra is. Ennek következtében a Miniszterelnöki Hivatal 1996-ban hazai ajánlást adott ki *Informatikai Rendszerek Biztonsági Követelményei* címmel.

Az információbiztonság tudománya 2001. szeptember 1-től óriási hangsúlyt kapott az amerikai terrortámadások következtében. Elmondható, hogy ez a dátum és a hozzá kapcsolódó események a nyugati társadalmak és a szakma információbiztonság iránti „feleszmélésének" kezdetét jelentették. Ettől kezdve rohamosan megnőttek az információbiztonságra fordított költségvetések. Az országok politikai és katonai vezetői belátták, hogy a biztonságnak kiemelt szerepe van egy ország, egy szervezet működésében.

Az ezredforduló után hazánkban is sürgetővé vált a biztonságtudománnyal kapcsolatos elvek, eszmék, követelmények meghatározása, melyet az Óbudai Egyetemen a következőképpen írtak le:

„Magyarországon az ezredfordulóra megszületett a jövő globális tudománya, a biztonságtudomány. Ma a biztonságnak a társadalom által elvárt magas szintje a gyakorlatban csak korszerű védelmi, biztonságtechnikai rendszerekkel valósítható meg. Az elvárt biztonsági szint egyre növekszik, s az ennek eléréséhez szükséges műszaki megoldások, rendszerek egyre bonyolultabbakká válnak." [2]

A korábban említett 2001. szeptember 11-én történt események és a napjainkban világszerte „tomboló" terrorizmus megerősítették azt az elvárást, hogy az információvédelmi szakembereknek a biztonság minden területén fel kell készülniük a legváratlanabb eseményekre. Egyre több vészjósló, szakértők által megfogalmazott kijelentés tükrözi azt, hogy nagyon nagy kihívásokkal kell az információs társadalomnak felvenni a harcot. Amikor a következő mondatokat [3] halljuk, mi laikus emberek is jogosan érezzük veszélyben magunkat:

„Kiberháború – a hadviselés ötödik dimenziója"

„A következő Pearl Harbour egy számítógépes támadás lesz"

„Láthatatlan ellenség a digitális térben"

A felmerülő veszélyek és kockázatok növekedése egyre hangsúlyosabb szerepet szán olyan tevékenységeknek, mint a megelőzés, védelem, biztonság előtérbe helyezése. Minden ország

törekszik arra, hogy információs oktatási kampányokat indítson annak érdekében, hogy az információbiztonság egységessé, nemzetközileg elfogadott szabályozáson alapulóvá váljon.
Magyarország 1999 – es NATO csatlakozása az MH egészét illetően óriási változást hozott. Ez az információbiztonság területén is új kihívásokat jelentett, de a szakemberek gyorsan felismerték, milyen fontos NATO tagállamaként a szervezet jogszabályi – és szakmai hátterét úgy alkalmazni, hogy nemzeti érdekeink ne sérüljenek.
A 2001 szeptemberében Amerikában elkövetett támadásokkal új korszak kezdődött a védelem területén, melyben kiemelt szerepet kap a NATO, ezáltal az MH is. Ennek keretében az utóbbi másfél évtizedben a NATO tagállamok számos gyakorlatot bonyolítottak le, amely során a résztvevő szakemberek a számítógépes rendszerek elleni támadások elhárításával foglalkoztak. Ezek közül a Cyber Coalition gyakorlatot emelem ki, mely minden évben megrendezésre kerül[10]. Ezeknek a gyakorlatoknak kiemelkedő szerepet tulajdonítottak a szakemberek, mivel a ballisztikus rakétákkal elkövetett támadás és a terrorfenyegetettség mellett a számítógépes rendszerek elleni támadás veszélyezteti leginkább a tagállamokat.
2001 – ben az Egyesült Államok az ellene intézett terrortámadások után nem sokkal átadta a NATO-nak azt a listát, amely tartalmazza, hogy a kollektív segítség jegyében mit kér szövetségeseitől, s ezzel a NATO alapokmányának 5. cikke életbe lépett[11]. A NATO-szerződés szóban forgó cikke a tagállamok kölcsönös szolidaritását írja elő, vagyis azt, hogy bármelyikük megtámadását a többi tagállam saját maga elleni támadásként kezeli.
A NATO főtitkár ebben az időszakban interjút is adott a német Bild hetilapnak, melyben kijelentette, hogy *„Egy tömeges, a NATO információs, kommunikációs- és vezetés-irányítási hálózatait ért támadás kiválthatja a NATO egységes válaszlépését, mivel ez a támadás akár az V. cikkely szerinti eseményként is értékelhető. Ez esetben a NATO akár hagyományos fegyverekkel is válaszolhat egy cyber támadásra."* A NATO védelmi miniszterek a „cyber teret" hivatalosan hadműveleti térként határozták meg, egyenértékűvé tették a légi, szárazföldi, vízi dimenziókkal. [4]
Néhány év elteltével 2010-ben újabb stratégiai koncepció került lefektetésre "Aktív Elkötelezettség, Modern Védelem"[12] néven, amely nagyon világosan és egyértelműen meghatározza a NATO alapfeladatait, szabályait, és értékeit, valamint a fejlődő biztonsági környezet és a Szövetség stratégiai célját a következő évtizedre vonatkozólag.

[10] www.nato.int
[11] Oszama bin Ladennek a szeptember 11.-i eseményekért való felelősségének bebizonyítása volt a feltétele az 5. cikk életbe lépésének
[12] Active Engagement, Modern Defence

A “Active Engagement, Modern Defence” három fő részt tartalmaz: [5]

- Kölcsönös védelem – Collective Defence
- Krízis menedzselés – Crisis Management
- Együttműködő biztonság – Cooperative Security

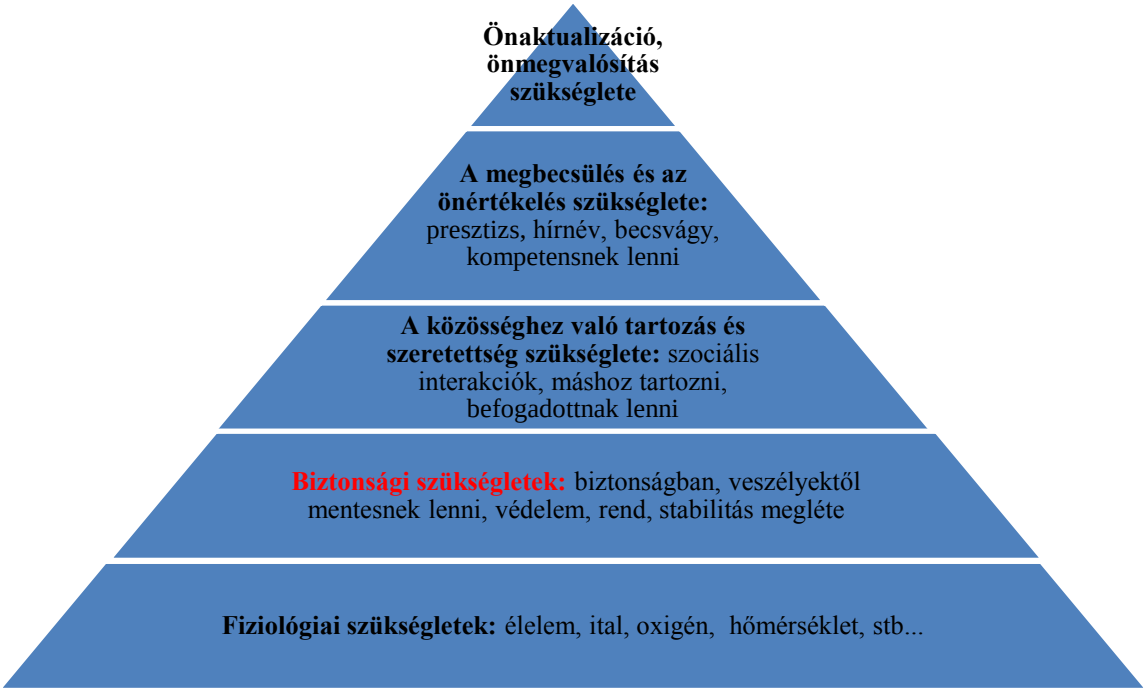
Jens Stoltenberg a Die Welt című német lapnak adott interjújában arról nyilatkozott, [6] hogy 2016-ban hatvan százalékkal nőtt a NATO elleni kibertámadások száma, és több tagállamban attól tartanak, hogy hackerek választási kampányok befolyásolásával próbálkozhatnak. A NATO főtitkára azt is elmondta, hogy tavaly havonta átlagosan 500 olyan informatikai támadás érte a NATO intézményeit, amely “szakértőink intenzív beavatkozását tette szükségessé”. *„A legtöbb támadást nem magánszemélyek, hanem állami intézmények finanszírozták”* – tette hozzá Jens Stoltenberg. Elmondta azt is, hogy a szövetségnél új eljárást vezettek be, válságkezelő szakértői csoportokat állítanak össze, amelyek készen állnak arra, hogy segítsék a tagállamokat hálózataik védelmében. Hozzátette azt is, hogy az informatikai támadások azért is nagyon veszélyesek lehetnek, mert kárt tehetnek az energiaellátó rendszerben vagy más kritikus infrastruktúrában, és azért is, mert ma már minden katonai aktivitás adatok átvitelén alapul.
A NATO tagjaként az MH – ra nézve is sokrétű tennivalókat jelentenek a főtitkár szavai, fontos tehát, hogy az információbiztonság kérdése központi része legyen a Szervezet mindennapjainak.

1. 2. A biztonság meghatározása

Az ember életében számos olyan tényező van jelen, amely veszélyt jelent számára. Az egyén biztonságát veszélyeztető források lehetnek például a természeti veszélyek, az ember teremtette környezetből származó veszélyek, a szervezet belső veszélyei valamint az ember és környezete találkozásából eredő veszélyek. Az ember, hogy nagyobb biztonságban érezhesse magát folyton arra törekszik, hogy minimalizálni tudja a veszélyeket. Egyszerű példákkal szemléltetve: biztonságot teremt magának azzal, hogy bezárja házának ajtaját, óvatosan közlekedik, hogy elkerülje a balesetet, megelőző orvosi szűrésre jár egészsége megőrzése érdekében, vagy nem költözik olyan helyre, ahol természeti katasztrófák gyakran előfordulhatnak.
A biztonságnak az ember életében betöltött szerepét Abraham Maslow amerikai pszichológus nevéhez fűződő piramis szemlélteti, amely a különböző motivációk egymáshoz való viszonyát mutatja. A piramis alján az alapszükségletek helyezkednek el. A létfenntartás szükséglete magában foglalja a biztonsági szükségletek kialakulását, melyek a következők: fizikai védettség, megszerzett javak védelme, rend, stabilitás, komfortérzés, veszélyektől mentes állapot elérése.

Ez a kategorizálás alapvetően az emberi pszichikumra, valamint fizikumra vonatkozik, de a történelem és napjaink eseményei is alátámasztják azt a tényt, hogy a biztonság megteremtése az élet minden területén alapvető, és fokozott figyelmet érdemlő feladat.

A motívumok hierarchiája Maslow[13] szerint [7]



1. sz. ábra: *A motívumok hierarchiája – saját szerkesztés*

A XX. század utolsó évtizedében és az új évezredben a biztonság még ennél is komplexebben értelmezhető. A társadalmi élet minden szféráját átfogó, a korábbiaknál lényegesen gyorsabb fejlődés az egész világ, a földrészek, a régiók, a kis közösségek, de az egyén életét is gyökerestől megváltoztatja. A biztonságot legjelentősebben befolyásoló tényezők: a terrorizmus, a környezetrombolás, a katasztrófák – köztük az ökológiai katasztrófa veszélye – az egész emberiség elpusztulásának veszélyét is magában hordozhatja. Megalapozottan kijelenthető, hogy a biztonság egy „széles sávban" értelmezett komplex fogalom.

A Magyar Értelmező Kéziszótárban a biztonság:

„1. veszélyektől vagy bántódástól mentes (zavartalan) állapot.

2. építmény, szerkezet szilárd volta.

3. bizonyosság, határozottság."

A témánk szempontjából fontos 1. meghatározás alapján a biztonság tehát – **állapot**.[8] Mivel disszertációmban az információbiztonságot az MH–ra fókuszálva vizsgálom, ezért a biztonság definiálását a hadtudomány oldaláról is megközelítem:

[13] Abraham Maslow (1908 - 1970) amerikai pszichológus, a Maslow-piramis kidolgozója.

A Hadtudományi Lexikon szerint „a biztonság: az egyéneknek, csoportoknak, országoknak, régióknak, szövetségi rendszereknek a maguk reális képességein és más hatalmak, nemzetközi szervezetek hatékony garanciáin nyugvó olyan állapota, helyzete és annak tudati visszatükröződése, amelyben kizárható vagy megbízhatóan kezelhető az esetlegesen bekövetkező veszély, illetve adottak az ellene való eredményes védekezés feltételei."
A biztonság kérdésének vizsgálata során azonban nagyon lényeges kihangsúlyozni, hogy a biztonság az **érzésről** és a **valóságról** szól. Különbséget kell tenni a ***biztonság érzése***, és a ***valós biztonság*** között. Nagyon sokszor kerülünk olyan helyzetbe, amikor a hamis biztonságérzetünk, valamint hamis veszélyérzetünk következményeként, akár sztereotípiák hatására ítélünk valamit biztonságosnak vagy veszélyesnek. Néhány példával szeretném bemutatni, hogy sokszor nem vagyunk tisztában a biztonság kockázatával, mégis kompromisszumot kötünk: [9]

- A repülőgépet veszélyesebbnek érezzük, mint az autót annak ellenére, hogy a statisztikák ennek az ellenkezőjét mutatják.
- Az ismeretlen embert kockázatosabbnak hisszük, mint az ismerőst, ezért idegen emberre nem bízzuk olyan szívesen gyermekünket, mint családtagra.
- Ma Magyarországon a dohányzás miatt sokkal nagyobb esélyünk van meghalni, mint terrortámadás miatt, ennek ellenére nem érezzük a dohányzást olyan veszélyesnek, amilyen valójában.

Weisz János a kancellár.hu alapítója az MVM[14] Zrt. Biztonsági Igazgatósága 2017. május 24-én megrendezett Energia az információbiztonságban című konferencián kihangsúlyozta, hogy *„…két nagyon fontos feladata van a szakembereknek: egyrészt meg kell érteni a valós kockázatokat, másrészt a szakembereknek el kell érniük, hogy a biztonság érdekében megtörténjenek a megfelelő változtatások, fejlesztések"*.

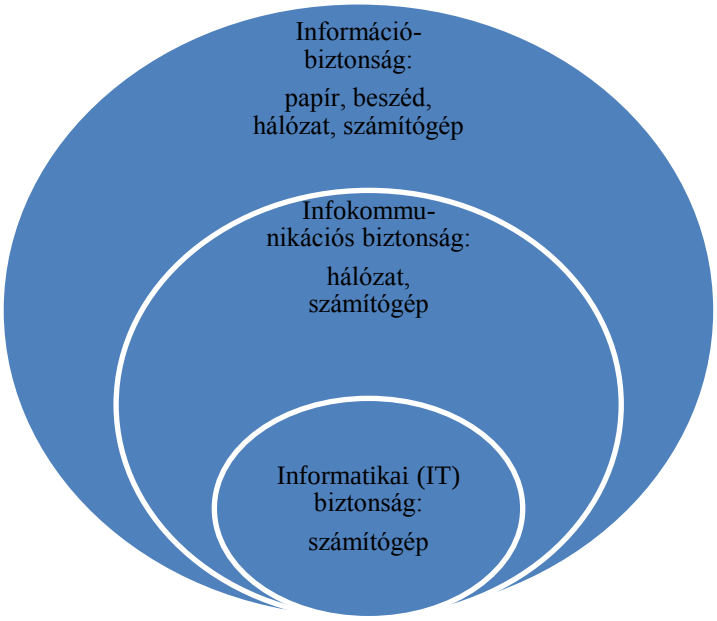
1.3 Az információbiztonság és az informatikai biztonság meghatározása

Disszertációmban az „információbiztonság" szóösszetétel igen sokszor szerepel. Az információbiztonság tartalmazza az információ minden megjelenési formáját, az információs szolgáltatásokat és az ezeket biztosító információs rendszerek védelmét. A mindennapi életben azonban igen gyakran azonosítják az információbiztonságot az informatikai biztonsággal.
„Az információbiztonság a biztonságtudomány részterülete, amely „az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb

[14] Magyar Villamos Művek

tulajdonságok, mint a hitelesség, a számon kérhetőség, a letagadhatatlanság és a megbízhatóság szintén ide tartozhatnak." [10]

Az információbiztonság és az informatikai biztonság közötti különbséget a következő ábra szemlélteti:



2. sz. ábra: *A biztonság különböző szintjei – saját szerkesztés*

Az információ védelmének területe kihat egy szervezet minden erőforrásának, az embereknek, az eszközöknek, az információs rendszereknek, és más vagyontárgyaknak a szabályozására, használatára, és egyben annak az ellenőrzését is jelenti.

Az informatikai biztonság pedig az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága,[15] sértetlensége[16] és rendelkezésre állása,[17] valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. [11 Ezt az összetett védelmet CIA elvnek[18] nevezzük.

„Az informatikai biztonság alapvetően függ az információs rendszerek elemeiből integrált komplex rendszerek biztonsági megfelelőségétől, és az információs rendszereket működtető szervezet folyamatainak érettségétől, a szakemberek, és az irányítást végzők szakképzettségétől, és a belső kontroll rendszer minőségétől. Az információbiztonságot a tágabb és szűkebb környezetre szabva kell kialakítani, megvalósítani, működtetni és fejleszteni." [12]

[15] Confidentiality
[16] Integrity
[17] Availability
[18] Confidentiality, Integrity és Availability együttes megvalósulása

Napjainkban folyamatos a verseny a hackerek és a biztonságot védő szervezetek, csoportok, személyek között. A támadó sokszor egy lépéssel előbbre jár, ugyanis neki van ideje felkészülni, míg az áldozatot váratlanul éri a hacker támadás.

Az informatikai biztonság megteremtésére való törekvés terén a leghatékonyabb fegyver a tudás, vagyis tudni azt, hogy milyen veszélyek leselkednek ránk a világhálón, tudni azt, vajon hogyan előzhetjük meg az információs rendszerünk elleni támadást. Fontos tisztában lenni azzal is, hogy mit tehetünk az ellen, hogy károsultak legyünk, és mit kell tennünk, ha mégis bekövetkezik egy incidens.

Sajnos az elmúlt másfél évtizedben egyre nőtt az informatika és a világháló veszélyeinek mennyisége és összetettsége, valamint nőtt az általuk okozott kár mértéke. Ezért fontos fokozott figyelmet fordítani a károk megelőzésére.

Az informatikai biztonságot meghatározó összetevők jelentésének lényege a következő:

A **bizalmasság** azt jelenti, hogy csak az arra jogosultak ismerhetik meg az információt.

Az informatikai rendszer **sértetlensége** akkor valósul meg, ha az információ tartalma és formája az elvárttal megegyezik, megfelelő forrásból származik, hiteles, igazolható, hogy megtörtént, vagyis letagadhatatlan, valamint egyértelműen azonosítható, elszámoltatható az a személy, aki az információval kapcsolatos műveleteket végzi.

Rendelkezésre állás alatt azt a tényleges állapotot értjük, amikor egy informatikai rendszer szolgáltatásai az arra jogosultak számára rendelkezésre állnak, és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva.

A rendszer **zártságáról** akkor beszélhetünk, ha a védelem az összes releváns veszélyt, fenyegetést figyelembe veszi.

A **teljes körűség** a rendszer minden elemére kiterjedő védelmet biztosítja.

A **folytonosság** azt jelenti, hogy időben folyamatosan megvalósul a védelem.

A **kockázatokkal arányos védelem** akkor valósul meg, ha a rendszer várható működésének időtartamában a védelem költsége arányban van a lehetséges kárral, vagyis a kockázatmenedzsmentet úgy kell kialakítani, hogy a bekövetkezendő kár mértéke és a védekezésre költött befektetés egyenesen arányos legyen.

Ehhez ad segítséget a COBIT[19] 5-ös verziója, [13] amely több mint 15 év fejlesztési tapasztalataira épít. Kialakításának egyik legfontosabb célja az volt, hogy az üzleti és az informatikai oldalt közelebb hozzák egymáshoz a hatékonyabb együttműködés érdekében. Többek között olyan fontos kérdésekre keresi a választ, hogy milyen hasznot eredményez az

[19] Controll Objectives for Information and Related Technology

információ és a technológia használata a vállalatoknál. A COBIT 5 támogatja a vállalatokat az IT optimális értékének előállításában a hasznok realizálásán, a kockázatok kézbentartásán és az erőforrások megfelelő használatán keresztül.

A COBIT 5 olyan átfogó keretrendszert biztosít, amely támogatja a vállalatokat céljaik elérésében, valamint értéket közvetít az IT eredményes irányításán és menedzsmentjén keresztül. Lehetővé teszi az IT irányítását és menedzsmentjét a teljes vállalatra vonatkozóan.

A COBIT 5 keretrendszer 5 irányelvre épül:

- Az érintettek igényeinek kielégítése.
- Integrált keretrendszert biztosítása.
- A teljes vállalatot lefedő end – to end megoldások adása.
- Irányítás és menedzsment folyamat elkülönítése.
- Holisztikus[20] szemlélet követése.

A COBIT 5 holisztikus szemlélete alapján hét nagyobb kategóriát ad meg azokra a tényezőkre, amelyek a vállalati informatika irányításában és menedzsmentjében meghatározóak.

Ezek a kategóriák:

- a folyamatok;
- a szervezeti struktúra;
- a vállalati kultúra, etika és magatartás;
- az irányelvek, szabályzatok, keretrendszerek;
- az információ;
- a szolgáltatások, infrastruktúra és alkalmazások;
- a humán erőforrás, kompetenciák és a szakértelem.

1.4 Információbiztonság és minősített adatvédelem

A minősített adatvédelem az információbiztonság – tudománynak egy olyan komplex ága, amely négy részterületre bontható. [14] Ezek a következők:

A **személyi biztonság** magába foglalja a felforgató tevékenység és a terrorista akciók veszélyének felismerését, a mozgási lehetőségek korlátozását. Az információhoz való hozzáférés szempontjából is értelmezhető a személyi biztonság, vagyis, hogy a minősített információ csak olyan személynek juthat birtokába, aki a megfelelő szintű személyi biztonsági követelményeknek igazoltan megfelel, illetve az adott minősítésű információ megismerése számára munkavégzéséhez kapcsolódóan szükséges. A személyi biztonság megteremtésének alap eljárása

[20] Teljességre törekvő

a nemzetbiztonsági ellenőrzés. A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény rendelkezik az ellenőrzés jogalapjáról, annak menetéről és a nemzetbiztonsági ellenőrzéssel kapcsolatos egyéb tudnivalókról.
A 90/2010. (III. 26.) Kormányrendelet nagy hangsúlyt fektet a **fizikai védelem** megvalósítására, melynek főbb részei a következők: mechanikai védelem, elektronikai jelzőrendszer, élőerős védelem, beléptető rendszer, biztonsági kamera rendszer, villám és túlfeszültség védelem, valamint a tűzvédelem. A minősített adat felhasználására és tárolására szolgáló helyszín fizikai biztonsági rendszerének több egymásra épülő elemből kell állnia. Ez az ún. mélységi védelem elve, amely meghatározza, hogy a minősített adatok fizikai védelmét külső, közbenső és belső fizikai biztonsági elemek együttese kell, hogy biztosítsa.

Az **adminisztratív biztonsági** intézkedések körébe tartoznak azok a követelmények, melyek a minősített adat nyomon követhetőségét, bizalmasságát, sérthetetlenségét valamint rendelkezésre állását biztosítják. Ennek alapját egy hiteles, a felelősség megállapítására alkalmas nyilvántartási rendszer képezi. A nyilvántartás jelenleg két féle módon valósul meg: a legtöbb szervnél még mindig a papíralapú nyilvántartást alkalmazzák, de már több helyen megjelentek a számítógépen vezetett nyilvántartások, elektronikus iktatókönyvek.

Az **elektronikus biztonság** (TEMPEST[21]) megteremtésének alapszabályait a 179/2003. (XI. 5.) Elektronikus kormányrendelet tartalmazza, amely a NATO és az EU biztonsági szabályzatainak előírásait szem előtt tartva, a minimális követelményeket állapítja meg. Ezzel kellő rugalmasságot tesz lehetővé ahhoz, hogy a minősített adat, valamint a minősített adatot kezelő rendszer védelme a konkrét veszélyeztetettséghez igazodva, a költséghatékonyság figyelembevételével biztosítsa a szükséges és elégséges védelem szintjét. Az elektronikus biztonság integrált részeként szabályozza a rejtjeltevékenységet, de a nemzetközi gyakorlatnak megfelelően e szakterület viszonylagos önállóságát megőrizve. Az Elektronikus kormányrendelet részletesen meghatározza az elektronikus biztonság helyi szervezeti, személyi elemeit és azok feladatkörét. Az elektronikus biztonsági rendszerben a NBF látja el az elektronikus biztonság tekintetében a nemzeti engedélyező, a kommunikációbiztonsági és a kompromittáló kisugárzás biztonsági hatóság feladatait.

1.5 Az információbiztonság megvalósítását szabályozó jogi háttér

A 2000-es évek elején alapvető és lényeges változások következtek be az információbiztonság jogi vonatkozását illetően. A minősített adatvédelem nagyon fontos része az információbiztonság

[21] Kompromittáló kisugárzás elleni védelem

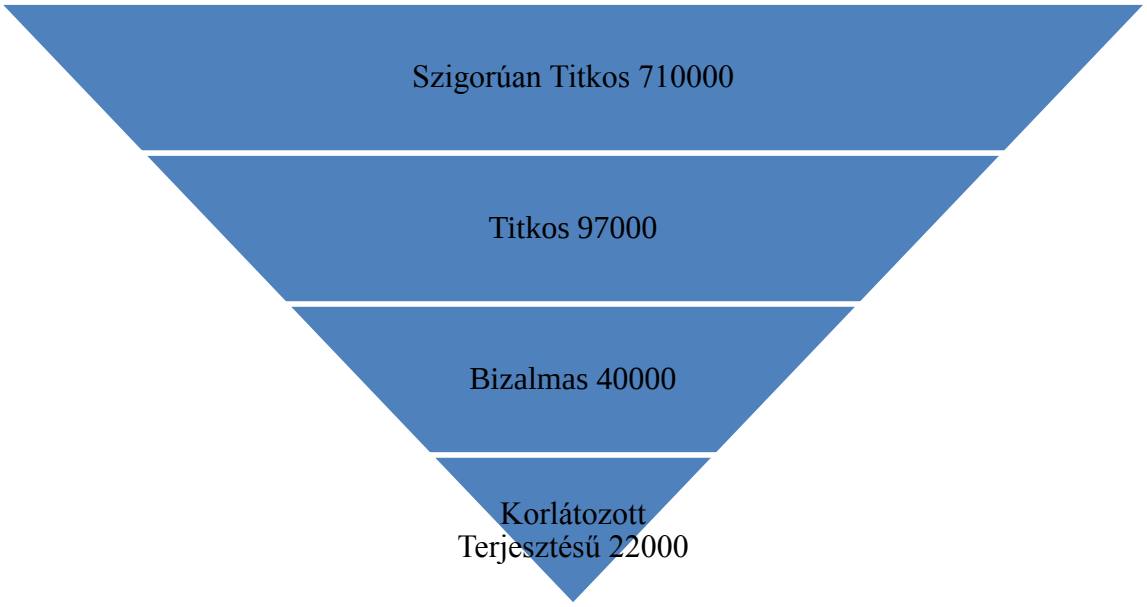
megteremtésének, így komoly előrelépést jelentett, amikor a Kormány 2004-ben elfogadta az egységes minősített adatvédelmi rendszer megteremtésével kapcsolatos feladatokról szóló 2094/2004. (IV. 27.) Korm. határozatot[22], mely alapján az új törvény megalkotására 2009 decemberében kerülhetett sor. A törvény létrehozásával nemcsak a NATO illetve EU követelmények átvétele volt a terv, hanem a nemzeti minősített adatvédelmi szabályozás felállítása valamint hatósági felügyelet létrehozása. A cél egy olyan egységes adatvédelmi rendszer kialakítása volt, amely egyrészt védi nemzeti minősített adatainkat, másrészt alkalmas a minősített adatok védelmével összefüggő nemzetközi kötelezettségvállalásaink teljesítésére is. A törvény 2010.április 1-jén lépett hatályba. A Mavtv. felhatalmazása alapján, a törvény végrehajtása érdekében a Kormány az alábbi három rendeletet alkotta meg:

- 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;
- Az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III.31.) Korm. rendelet.

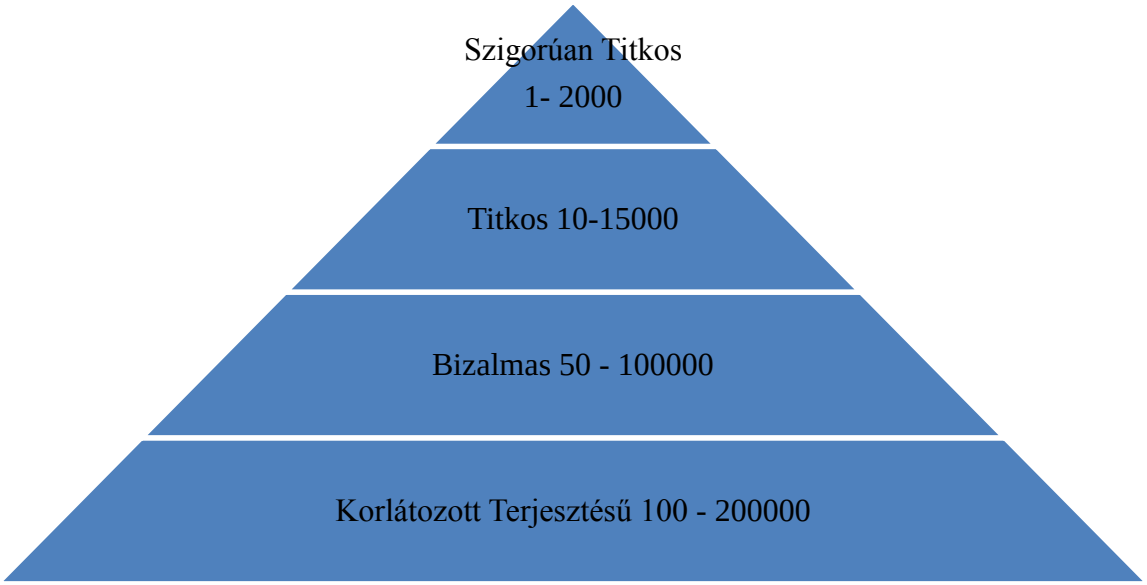
A minősített adat védelméről szóló Mavtv. illetve az annak végrehajtásáról rendelkező három kormányrendelet jelentősen megváltoztatta a minősített adatok védelmének magyarországi rendszerét. Általánosságban szólva az új törvényről elmondható: a jogszabály számos olyan változtatást hozott, amely nem csupán a minősített adat kezelésével foglalkozó személyek, hanem a hétköznapi emberek számára is szemléletesen érzékeltethető.

A Mavtv. által meghatározott minősítési eljárás tovább erősíti a káralapú minősítési rendszert, azaz az okozható kármértéknek megfelelő védelemben kell részesíteni a minősített adatot. Míg a törvény megjelenéséig évente a NATO és az EU szervezeteiben és intézményeiben néhány „Szigorúan titkos!”, százezres nagyságrendű „Bizalmas!” és „Korlátozott terjesztésű!” adat keletkezett, addig hazánkban a „Szigorúan titkos!” minősítésű adatok száma meghaladta az évi 700.000 darabot, és csupán néhány tízezer alacsonyabb minősítési szintű adat jött létre. Az új törvény ezen az aránytalanságon is változtatni kívánt. A magasan minősített adatok számának csökkentésével hosszabb távon a magas költségvetési ráfordítások mérséklése is elérhető lesz. Az alábbi ábrákon látható két piramissal az eddigi, illetve az optimálisnak gondolt állapotot mutatom be. [15]

[22] njt.hu



3. sz. ábra: *A minősített adatok száma a 2009. évi CLV törvény bevezetése előtt - saját szerkesztés*



4. sz. ábra: *A minősített adatok számának alakulása a 2009. évi CLV törvény bevezetése után – saját szerkesztés*

A büntető törvénykönyvről szóló 2012. évi C törvényben (a továbbiakban: Btk.) a minősített adattal visszaélés bűncselekményének büntetési tételei módosításra kerültek. A minősített adat feldolgozására törvény alapján feljogosított személyre vonatkozóan szigorúbb büntetési tételt állapít meg. Az alábbi ábrán jól látható, hogy már korlátozott terjesztésű adattal való visszaélés esetén is szabadságvesztést kaphat az a személy, aki törvény alapján minősített adat

feldolgozására jogosult. Az alábbi saját készítésű táblázatban a büntetési tételeket szemléltetem. [16]

Visszaélés minősített adattal:	Minősített adat feldolgozására nem feljogosított személy	Minősített adat feldolgozására törvény alapján feljogosított személy
Visszaélés szigorúan titkos minősítésű adattal:	1-5 évig terjedő szabadságvesztés	2-8 évig terjedő szabadságvesztés
Visszaélés titkos minősítésű adattal:	maximum 3 évig terjedő szabadságvesztés	1-5 évig terjedő szabadságvesztés
Visszaélés bizalmas minősítésű adattal:	vétség miatt 1évig terjedő szabadságvesztés	maximum 2 évig terjedő szabadságvesztés
Visszaélés korlátozott terjesztésű minősített adattal	vétség miatt elzárás	vétség miatt 1évig terjedő szabadságvesztés

Annak érdekében, hogy a törvényben leírtak jól érthetőek és könnyebben betarthatóak legyenek, a jogalkotók öt alapelvet fogalmaztak meg, melyek alapvetően a NATO illetve az EU Biztonsági Szabályzatai mintájára kerültek be a minősített adatvédelmi törvénybe.

Az alapelvek a következők:

„2. § (1) 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.
(2) Szükséges ismeret elve: minősített adatot csak az ismerhet meg, akinek az állami vagy közfeladata ellátásához feltétlenül szükséges.
(3) Bizalmasság elve: minősített adat illetéktelen személy számára nem válhat hozzáférhetővé vagy megismerhetővé.
(4) Sérthetetlenség elve: a minősített adatot kizárólag az arra jogosult személy módosíthatja vagy semmisítheti meg.
(5) Rendelkezésre állás elve: annak biztosítása, hogy a minősített adat az arra jogosult személy számára szükség szerint elérhető és felhasználható legyen.” [17]

Nagy előrelépést jelentett Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban. Ibtv.) bevezetése, amely új helyzetet teremtett többek között az MH számára is.

Ez az első magyar hivatalos szabályzó, amely országos szinten határoz meg biztonsági követelményeket, a hálózati biztonságért felelős szervezeteket és koordinációért felelős tanácsot alapít, és alacsonyabb szintű követelmények meghatározását rendeli el a szükséges mértékű számítógép és hálózati biztonság érdekében. Az Ibtv. egyaránt vonatkozik a minősített és nem minősített elektronikus adatkezelő rendszerekre, szolgáltatásokra.

Az MH rejtjeltevékenységének szabályozásában jelentős előrelépést hozott az új rejtjelszabályzat, melynek kiadásáról a Honvédelmi Közlöny rendelkezik. [18]

Az alábbiakban felsorolt – az információbiztonság megvalósulását elősegítő – jogszabályok a következők:

- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről
- 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről
- 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről
- 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat – és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenység vizsgálat lefolytatásának szabályairól
- 186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

1.6 A minősített adatvédelmi rendszer működtetésében részt vevő személyek

A 2009. évi CLV. törvény 23§ – a határozza meg a minősített adat védelmi feltételeinek kialakításáért felelős személyek kinevezését valamint a felügyeleti rendszer létrehozását. A

90/2010. (III. 26.) Kormányrendelet III. fejezete részletesen leírja a biztonsági vezető és a titkos ügykezelő foglalkoztatásának feltételeit, feladatait. A minősített adatvédelem helyi működtetéséhez szükséges, megfelelő képesítési követelményekkel és szakmai ismeretekkel is rendelkező személyzet létszámának meghatározása és folyamatos biztosítása a minősített adatot kezelő szerv vezetőjének a felelőssége.

A minősített adatot kezelő szervnél a minősített adat védelmével kapcsolatos feladatok végrehajtását és koordinálását a minősített adatot kezelő szerv vezetője által kinevezett **biztonsági vezető** végzi, aki az egyszemélyi felelősség elvének érvényesülésével látja el feladatát. A gyakorlat azt mutatja, hogy az MH – ban a feladatokat nem önálló munkakörben, hanem kinevezéssel, más munkaköri tevékenység mellett látják el a biztonsági vezetők.

A biztonsági vezető foglalkoztatásának feltételeiről a 90/2010. (III. 26.) Kormányrendelet III. fejezet 1. pontja rendelkezik, miszerint biztonsági vezető csak az a személy lehet, aki a minősített adatok kezelésének területén legalább 1 évet eltöltött, a szervezetnél kezelt legmagasabb szintű minősített adat kezeléséhez szükséges személyi biztonsági tanúsítvánnyal rendelkezik, és titoktartási nyilatkozatot ír alá. A feladat ellátásához arra is szükség van, hogy az adott személy a szervezeti hierarchiában mindenképpen magasabb vezetői tevékenységet lásson el annak érdekében, hogy felügyeleti tevékenységét minél magasabb szinten tudja érvényesíteni. Ez azért is fontos, hogy a szerv vezetőjétől kapott jogkörben eljárva a minősített adat védelmével kapcsolatos döntéseinek, akaratának akár utasítási joggal érvényt tudjon szerezni. Erre megfelelő „súllyal", a minősített adatot kezelő szerven belül hatékony érdekérvényesítő képességgel, nyilvánvaló vezetői tekintéllyel rendelkező munkatársnak van esélye.

A minősített adatot kezelő szerv vezetője által kiadott biztonsági szabályzatban kell rendelkezni a helyi biztonsági felügyeletnek a minősített adatot kezelő szerv területi, helyi szerveinél kinevezett biztonsági vezetőkkel kapcsolatos szakmai felügyelet tartalmáról, a biztonsági vezetők feladat – és hatásköréről.

Összefoglalva: a biztonsági vezető szabályalkotási, szabályozási és ellenőrzési feladatokat lát el, valamint gondoskodik az adott szervezetnél a minősített adatok védelmével kapcsolatos személyi, fizikai, adminisztratív és elektronikus teendők végrehajtásáról, végrehajtatásáról.

A rendszerbiztonsági felügyelő, a rendszerbiztonsági felügyelet és a központi rendszerbiztonsági felügyelet

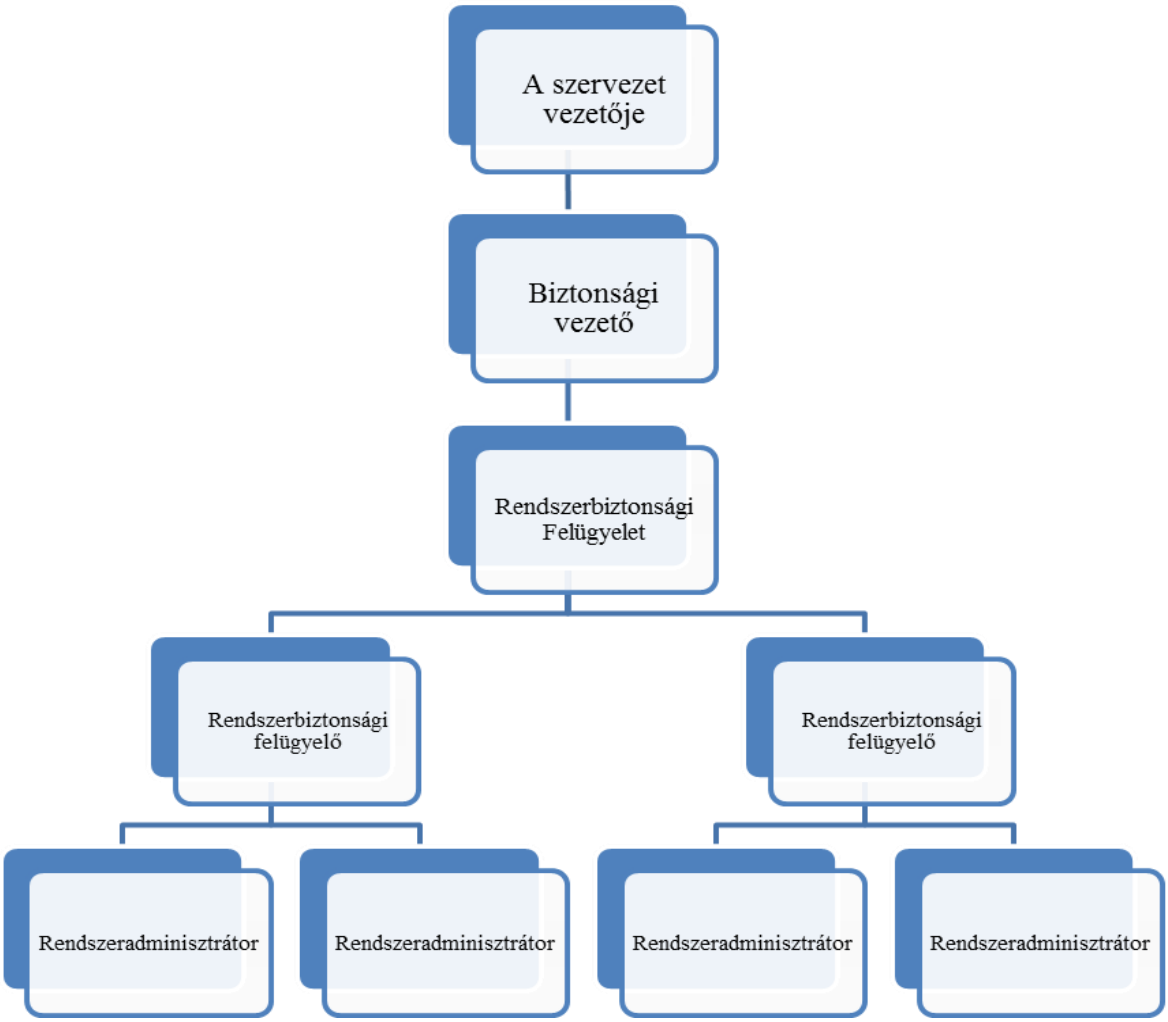
A 161/2010. (V. 6.) Kormányrendelet 3. pontjának 6. §. – a rendelkezik arról, hogy a minősített adat elektronikus rendszeren való kezelése esetén a szerv vezetőjének a biztonságért felelős személyeket kell kijelölnie. A rendszerbiztonsági felügyelő a biztonsági vezető irányítása alatt a

rendszer alkalmazási területén felelős a minősített adatot kezelő **elektronikus rendszer** személyi –, fizikai –, adminisztratív – valamint rendszerbiztonsági feltételeinek teljesüléséért, a biztonsági beállítások és hozzáférési jogosultságok naprakészen tartásáért.

Több elektronikus adatkezelő rendszer működtetése során rendszerbiztonsági felügyelet létrehozására van lehetőség, melyet a biztonsági vezető irányít.

A minősített adatot elektronikus rendszeren kezelő szerv vezetője rendszeradminisztrátort jelöl ki. A rendszeradminisztrátor a rendszerbiztonsági felügyelő irányítása mellett az üzemeltetéséért, karbantartásáért felelős személy.

A biztonsági felügyeleti rendszert az alábbi ábrák szemléltetik:



5. számú ábra: *Minősített adatkezelő rendszerek biztonsági felügyelete – saját szerkesztés*

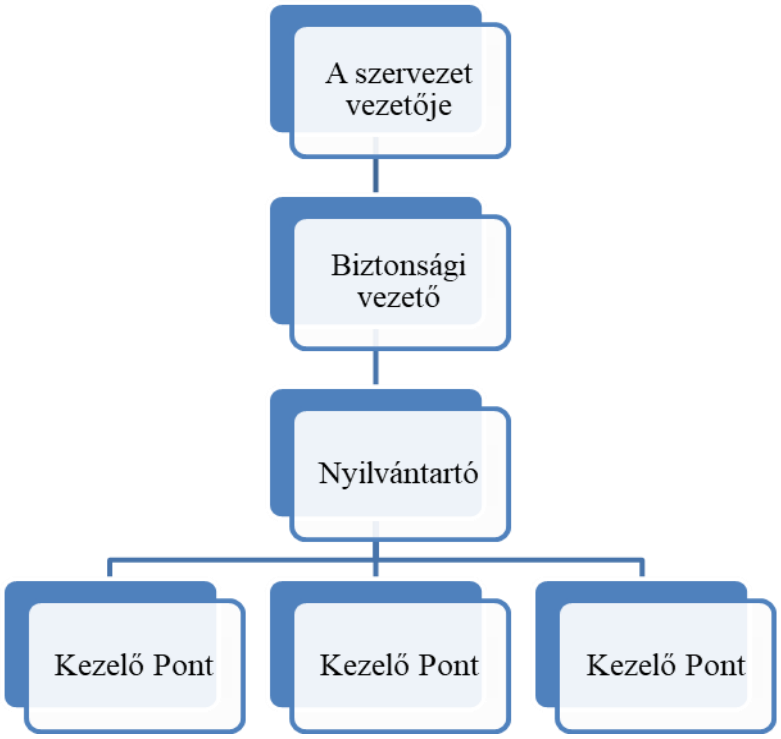
A rejtjelfelügyelő és a (központi) rejtjelfelügyelet

Rejtjeltevékenységet folytató szerv vezetője köteles rejtjelfelügyelőt kijelölni vagy – amennyiben a minősített anyagok mennyisége indokolja – rejtjelfelügyeletet létrehozni.

6. számú ábra: *A rejtjeltevékenység biztonsági felügyelete – saját szerkesztés*

A Nyilvántartó és Kezelő Pont működése

A Nyilvántartó és Kezelő Pont a minősített adatot kezelő szerv olyan szervezeti egysége, amely a minősített adatot kezelő szervhez érkező vagy ott keletkező minősített adatok nyilvántartásával kapcsolatos feladatokat hajtja végre, tevékenységét a biztonsági vezető szakmai alárendeltségében végzi.



7. számú ábra: *A nyilvántartó és kezelő Pont felépítése – saját szerkesztés*

Az ábrákon bemutatott felelősségi körök alá –, fölé – és mellérendeltségi, viszonyban állnak egymással. A humán kockázatok csökkentése érdekében a jogszabályok *összeférhetetlen felelősségi köröket* is meghatároznak a nagyobb biztonság érdekében.

A biztonsági vezető a minősített adatot kezelő szervnél egyidejűleg titkos ügykezelői munkakörben nem foglalkoztatható.[23]

Egy rendszerbiztonsági felügyelő nem tölthet be rendszeradminisztrátori szerepkört ugyanazon adatkezelő rendszeren.

Magas kockázatú tevékenységek esetében pedig gyakran alkalmazzák a „négy szem elvét". Ennek bevezetése nagyobb biztonságot jelent, mert így egyetlen felhasználó nem tud bizonyos folyamatokat egyedül elvégezni a rendszerben, hanem csak résztevékenységeket. A további lépések végrehajtására egy másik felhasználó van feljogosítva.

Összegzés

Az 1. fejezetben **az információbiztonság** történelmi hátterét áttekintve megállapítom, hogy a biztonságtudománynak ez a részterülete **egyre fontosabb szerepet tölt be, különösen az ezredforduló után.**

Ebben a fejezetben kihangsúlyoztam, hogy **Magyarország NATO csatlakozása** kollektív védelmet nyújt az ország, és az MH számára, de egyben **új kihívásokat is jelent a katonai védelem terén, melynek egyre hangsúlyosabb területe az információbiztonság.**

Ebben a fejezetben szemléltettem az információbiztonság jelentését, összevetettem az informatikai biztonsággal. Bemutattam továbbá a minősített adatvédelem szabályozását, amely az információbiztonság megvalósulása tekintetében jelentős szerepet tölt be.

[23] 90/2010. (III. 26.) Kormányrendelet III. fejezet 1. pontja

2. AZ INFORMÁCIÓBIZTONSÁG ELLENŐRZÉSI RENDSZERE A MAGYAR HONVÉDSÉGBEN

Bevezetés

Disszertációmban kiemelt figyelmet fordítok annak vizsgálatára, hogy mely eszközökkel, módszerekkel erősíthető a katonai szervezeteknél az információbiztonság. Ehhez elengedhetetlen az ellenőrzési rendszer vizsgálata, mert egy katonai szervezet információbiztonsági szintjének mérésére az ellenőrzés az egyik legeredményesebb módszer.

2.1 A Magyar Honvédség információvédelmi ellenőrzési rendszerének hierarchikus felépítése

Az alábbi ábra bemutatja, hogy a Magyar Honvédségen belül az ellenőrzés hierarchikus rendszer szerint valósul meg. A legfőbb, információbiztonságot ellenőrző szerv a Honvéd Vezérkar Híradó, Informatikai és Információvédelmi Csoportfőnökség (a továbbiakban HVK HIICSF), amely felett az NBF külső szakmai felügyeleti, és ellenőrzési joggal rendelkezik. A HIICSF szakmai irányítása alatt az Összhaderőnemi Parancsnokság (a továbbiakban ÖHP) látja el az alárendeltségében működő végrehajtó szervek ellenőrzését. A Nemzeti Közszolgálati Egyetem (a továbbiakban NKE) Hadtudományi és Honvédtisztképző Karára az új egyetem megalakulása óta az alábbi hierarchikus ellenőrzési szabályozás nem vonatkozik. Míg korábban a HVK rendelkezett ellenőrzési joggal az intézmény felett, jelenleg az információbiztonság ellenőrzését az NBF látja el.

8. sz. ábra: *Példa a Magyar Honvédség információbiztonsági ellenőrzési hierarchiájáról – saját készítésű ábra*

2.2 Az információbiztonság ellenőrzés szabályozása az MH–ban

A honvédelmi tárca ellenőrzési rendjéről az 52/2007 (HK 11.) HM utasítás rendelkezik, melynek néhány pontját a 86/2011 (VII. 29.) HM utasítás módosítja. Ezen kívül a Magyar Honvédség Biztonsági Szabályzata meghatározza az ellenőrzés menetét, és az ellenőrzéssel kapcsolatos szabályokat, feladatokat. Mielőtt ezt a témát vizsgálom, szükségesnek tartom meghatározni magát az ellenőrzés fogalmát:

„Az ellenőrzés a vezetés folyamatának egyik alkotóeleme, a vezetői tevékenység szerves része, az elöljáró és az alárendeltek közötti kapcsolat fontos láncszeme, amely megmutatja, tényekkel, adatokkal alátámasztja, hogy az alárendelt mit tett (és mit nem) az elöljáró által megszabott feladatok végrehajtása érdekében és milyen eredménnyel." [18]

Egy ellenőrzés nem csupán az ellenőrzött személyekről ad visszacsatolást egy vezető vagy egy elöljáró, ellenőrző tevékenységet lebonyolító szerv részére, hanem képet ad a vezetés biztonságtudatosságának szintjéről, valamint a szervezet biztonsági kultúrájáról is. Az ellenőrzés során az ellenőrző szerv megbizonyosodhat arról, hogy a szabályzatokban előírt feladtok betartásán túl reális volt-e a követelménytámasztás a beosztottakkal szemben. A felmerülő problémák, hiányosságok pedig támpontot adnak ahhoz, hogy a szervezet vezetője mérlegelje és eldöntse, hogy szervezetén belül a munkavégzés módszerei változtatást igényelnek vagy sem.

Az ellenőrzésnek nem csupán a számonkérés és a felelősségre vonás a célja, hanem fontosabb a hibák felszínre kerülése, ezek kijavítására, megszüntetésére tett kezdeményezések megtétele az illetékes vezető részéről.

A híradókatonák és híradó alegységek kiképzésének szakmódszertana összefoglalja, hogy melyek azok az általános rendező elvek, amelyeket az ellenőrzések tervezése, szervezése, végrehajtása során követni érdemes. Ezek az alábbiak:

„Az ellenőrzés:

- *komplex módon, objektíven tárja fel a helyzetet, a helyzet megítéléséhez, a tendenciák felismeréséhez szükséges tényeket, az okokat és az okozati összefüggéseket,*
- *legyen rendszeres, szakszerű, következetes, megelőző és szükség szerint váratlan,*
- *időben derítse fel a hibákat, torzulásokat, segítse elő megismétlődésük elkerülését,*
- *fejlessze a feladat végrehajtásáért érzett személyes felelősséget, a kritikai érzéket, a vezetőkészséget, a kölcsönös bizalmat és a pozitív vezetői tulajdonságokat,*
- *szilárdítsa a törvényességet, a katonai rendet és fegyelmet, biztosítsa a tulajdon védelmét,*
- *hozza felszínre az általánosítható tapasztalatokat,*

- *állapítsa meg az eredményeket, a személyes érdemeket, illetve a mulasztásokat és az azért felelős személyeket, a felelősség mértékét."* [19]

Az ellenőrzések alapját a jogszabályi háttér biztosítja. Ezek törvények, kormányrendeletek, utasítások, rendelkezések, intézkedések, követelmények, szabályzatok, normagyűjtemények, valamint kiképzési programok előírásainak formájában jelennek meg. Az 52/2007 (HK 11.) HM utasítás az ellenőrzés típusait a következőképpen határozza meg:

- komplex ellenőrzés
- átfogó ellenőrzés
- témavizsgálat
- célellenőrzés
- utóellenőrzés.

A komplex információvédelmi ellenőrzések alapvető okmánya az Ellenőrzési terv.

Az ellenőrzés módszerei függenek az ellenőrzések jellegétől, tartalmától, céljától. Az ellenőrzések során felhasznált módszerek a következők lehetnek:

- okmányok, nyilvántartások, egyéb adatok és dokumentumok tanulmányozása, elemzése;
- helyszíni vizsgálat, beszámoltatás;
- jelentés bekérése, meghallgatás;
- személyek kikérdezése, vizsgáztatása szóban, vagy írásban;
- tevékenységi folyamatok, technikai eszközök működésének, működőképességének kipróbálása;
- eszközök, anyagok, anyagi készletek részleges, vagy teljes leltározása.

Az információbiztonsági ellenőrzések részét képezi a minősített iratkezelés ellenőrzése. Az ügyviteli ellenőrzést felügyeleti és szervezeti belső ellenőrzés keretein belül valósítják meg. A minősített iratkezelés tárca szintű felügyeleti ellenőrzéseit a nyílt iratkezelés ellenőrzésével egy időben a MH információbiztonsági tevékenységének szakmai irányításáért felelős HVK szerv tervezi, és bonyolítja le.

Az éves terv szerinti ügyviteli ellenőrzés tapasztalatait összegezni, értékelni, hasznosítani kell. Az ellenőrzés eredményéről jegyzőkönyvet kell felvenni, melyet meg kell küldeni az ellenőrzött szerv felügyeleti hatóságának, valamint az MH információvédelmi tevékenységének szakmai irányításáért felelős HVK[24] szerv vezetőjének.

[24] HVK HIICSF

A minősített elektronikus adatkezelő rendszerek ellenőrzésére vonatkozóan néhány évvel ezelőtt adták ki a 10/2012 (HK 14.) HVK HIICSF szakutasítást, amely a minősített adatkezelő rendszerek ellenőrzésére szolgál. A szakutasítás kihangsúlyozza, hogy az ellenőrzés során különös figyelmet fordítsanak a teljes életcikluson át tartó állandó védelemre, a személyi, fizikai, adminisztratív és elektronikus információbiztonsági követelmények megvalósítására. A szabályzó kijelöli, hogy az ellenőrzés gyakoriságát és mélységét a szervezet feladatrendszeréhez kell alakítani oly módon, hogy a szervezeti működés felesleges zavarását elkerüljük. Az ellenőrzés során kialakított észrevételeket, javaslatokat úgy kell megfogalmazni, hogy a hiányosságok, hibák felszámolásra kerüljenek, és a rendszer a szabályzókban megfogalmazott előírások szerint működhessen Az ellenőrzésben a következő személyek vesznek részt: az ellenőrzött szervezet biztonsági vezetője (biztonsági szervezete), az ellenőrzött rendszer rendszerbiztonsági felügyelője valamint rendszeradminisztrátora. Az ellenőrzés során a szakutasítással együtt egy kérdőívet is használnak az ellenőrök, melyet az ellenőrzések alkalmával kötelező az ellenőrzött szervnek előre kitölteni, és az ellenőrzés megkezdése előtt a bizottság részére át kell adni. A kérdőív az alábbi fejezetekből áll:

1. A biztonság adminisztrációja és szervezete (19 pontban)
2. A híradó és informatikai rendszer jellemzője (3 pontban)
3. Fizikai biztonság (4 pontban)
4. Személyi biztonság (7 pontban)
5. Adminisztratív biztonság és az elektronikusan tárolt adatok védelme (7 pontban)
6. Elektronikus információvédelem (19 pontban)

2012. decemberben a HVK HIICSF jóvoltából részt tudtam venni több NATO ellenőrzésen, ahol ezt a kérdőívet első ízben alkalmazták. Már az első tapasztalatok[25] is azt mutatták, hogy a kérdőív használata megkönnyítette mind az ellenőrök, mind az ellenőrzött személyek dolgát. Részletes, átfogó támpontot nyújtott az ellenőrzötteknek az ellenőrzésre való felkészülés során, ugyanakkor megkönnyítette az ellenőrök munkáját az ellenőrzés végrehajtása közben.

Az ellenőrökkel készített személyes interjúk alapján az ellenőrzések során a következő hiányosságok merültek fel:

- Az okmányok nyilvántartása pontatlanságot mutatott;
- A minősített számítógép jelszavainak borítékolása, nyilvántartása nem az előírásoknak megfelelően történt;
- Nem állt rendelkezésre telepítő CD;

[25] Az ellenőrzés befejezése után interjút készítettem az ellenőrökkel és az ellenőrzött személyekkel

- A jogtiszta szoftver nem volt nyilvántartva;
- Hiányosságok mutatkoztak a számítógépek beállítása terén: kiemelték az ellenőrök, hogy a minősített számítógépen mindent úgy kell beállítani, ahogy az ÜBSZ-ben le van írva;
- Az ÜBSZ frissítésével egyidejűleg a gépet is frissíteni kell;
- A szoftverlista nem volt pontos;
- A hardver frissítések egy része nem az NBF jóváhagyásával történt.

Az ellenőrzés tapasztalatai összességében azt mutatták, hogy a katonai szervezetek az ellenőrzésre megfelelően felkészültek, az alapvető előírásoknak meg tudtak felelni.

2.3 A katonai szervezetek minősített adatainak ellenőrzése [20]

A katonai alakulatoknál a nem minősített adatok ellenőrzésével összhangban a szervezet biztonsági vezetője intézkedik a minősített adat védelmére vonatkozó személyi, fizikai, adminisztratív biztonsági rendelkezések betartásának éves ellenőrzéséről, melyet minden év február 28 – ig, jegyzőkönyv felvétele mellett kell végrehajtani. A biztonsági vezető gondoskodik a szervezethez érkezett és ott készített minősített adatok iratforgalmi statisztikájának minősítési szintenkénti bontásban történő elkészítéséről. A belső ellenőrzés alkalmával sor kerül az ügyviteli szervnél és az ügyintézőknél nyilvántartott minősített iratok, hivatalos bélyegzők és személyi pecsétnyomók meglétének átvizsgálására, a kezelt minősített adatok felhasználásának és tárolásának ellenőrzésére. Az ellenőrzést követően a biztonsági vezető március 20 – ig gondoskodik a lefolytatott éves ellenőrzés eredményéről készített jegyzőkönyv, valamint az ellenőrzést megelőző évben a szervezetnél készített és oda érkezett minősített adatok iratforgalmi statisztikáját tartalmazó jelentés elkészítéséről. A jelentés és jegyzőkönyv az MH információvédelmi tevékenység szakirányítását ellátó állami vezető részére kerül továbbküldésre.

A középszintű vezető szerv az alárendelt szervezetei tekintetében összesített iratforgalmi statisztikát készít, és azt az alárendelt szervezetek jelentéseivel együtt megküldi a HVK HIICSF vezetője részére. Az MH – szintű összesített iratforgalmi statisztikai kimutatás, valamint a jelentéseknek az elkészítése és az NBF részére történő megküldése a HVK HIICSF vezetőjének a feladata.

A minősített iratok munkaidőn túli tárolására vonatkozó szabályok megtartását a biztonsági vezető a szervezeten belül évi 2-3 alkalommal külön bizottsággal előzetes bejelentés nélkül köteles ellenőriztetni. Az ellenőrzés kiterjed az iratok, rontott lapok elzárására, a

számítástechnikai eszközök szabályos használatára, a biztonsági tárolók zárására és pecsételésére, valamint a kulcsdobozok és a helyiségek kulcsainak kezelésére és tárolására.
A bizottsági ellenőrzésről jegyzőkönyv készül, melyet a biztonsági vezető – az ellenőrzést követő munkanapon – bemutat a szervezet parancsnokának. Az ügyviteli szerv vezetőjének váltásakor a minősített iratok meglétét az ügyviteli szervnél tételesen, bizottság útján ellenőrizni kell.
A közvetlen szolgálati elöljáró folyamatosan ellenőrzi beosztottjainál az ügykezelés szabályainak betartását, és félévenként egyszer tételesen a minősített iratok meglétét. Az ügyintézők a kezelésükben lévő minősített iratokat negyedévente kötelesek tételesen ellenőrizni. Ha irat hiányát észlelik, azt jelentsék közvetlen szolgálati elöljárójuknak. Az ellenőrzés végrehajtását jegyezzék be a belső leírásukba.
Az ügyintézők a minősített irataik tételes ellenőrzését kötelesek végrehajtani huzamosabb távollét (szabadság, vezénylés stb.) megkezdése előtt is.
Az ügyviteli szerv vezetője – belső ellenőrzés keretében – folyamatosan ellenőrzi az ügyviteli szerv munkáját, a nyilvántartások vezetését, az iratok kezelésének, tárolásának és őrzésének rendjét.

2.4 Az információbiztonság erősítése, fokozása az informális ellenőrzés lehetőségeinek kihasználásával

Egy szervezet irányítása során a vezetést olyan tevékenységként kell felfogni, amely célokat tűz ki, a célok elérése érdekében erőforrásokat biztosít. A vezetés nem más, mint egy tudomány, szakma, egy olyan folyamat, amely során a vezető befolyásolja és motiválja a beosztottakat a kívánt célok elérése érdekében. A szervezet vezetője mozgósítja a szervezet tagjait, tehát a szervezet parancsnoka nem csak vezetői szerepet tölt be, hanem egyúttal menedzsere is saját szervezetének. A menedzsment feladata pedig a tervezés, szervezés, utasítás, koordinálás, valamint az ellenőrzés is.
Az előző oldalakon nagyrészt jogszabályokon alapuló ellenőrzésekről ejtettem szót, melyek az MH ellenőrzési rendszerének formális részét képezik. Emellett kiemelkedően fontosnak tartom a nem hivatalos, informális módon megjelenő ellenőrzési módszereket is. Kétféle módszert tartok hasznosnak és hatásosnak, amik igen jelentős információkat adhatnak egy vezető részére a beosztottakról, munkájukról.
Az egyik módszer az alkalmazottak személyes megfigyelése. Mivel a szervezet vezetője a jogszabályokban leírtakon túl bármikor ellenőrizheti a szervezetében munkát végző személyt, jogában áll munkaidőn belül, és munkaidőn túl is belépni az alkalmazott irodájába, és meggyőződni arról, hogy beosztottja az információbiztonsági előírásoknak megfelelően tárolja a

dokumentumokat, vagy a szabályokban meghatározottak szerint működteti a minősített adatkezelő rendszert. Az illetékes parancsnokok tájékoztatása szerint a legtöbb szabálytalanságot munkaidőben követik el az emberek azáltal, hogy például nem zárják el az iratokat arra az időre, amíg kimennek az irodájukból, vagy a számítógépet bekapcsolva hagyják.

A másik informális ellenőrzési lehetőséget a kommunikáció adja. A szervezetben kialakított úgynevezett „kommunikációs csatornák" biztosítják a vezetői tájékozódást. A parancsnokok a kommunikáció révén visszajelzést kapnak a szervezet keretében folyó tevékenységekről, személyekről, melyeket az információk informális áramlásának is nevezhetünk. A kommunikáció két részre osztható: a formális kommunikáció egy hivatalos forma, amely általában a vezetőtől a beosztottak felé áramlik. Ilyen lehet például célok közlése, utasítások, elvárások megfogalmazása, nevelő szándékú üzenetek, visszajelzés a teljesítményről, stb. A beosztottak részéről gyakran fordul elő probléma közlése, javaslat felterjesztése, vita indítása, stb. Az informális kommunikáció többnyire nem tudatos, kötetlen, legtöbb esetben a szervezetet irányító személy kezdeményezi. A jó vezető megtalálja annak módját, hogy hogyan használja fel céljainak elérése érdekében ezt a lehetőséget. Az így szerzett információk legnagyobb része rendkívül hasznos, nagymértékben hozzájárul a szervezet hatékonyságához. Általánosan elfogadott, hogy egy menedzser típusú vezető az informális kommunikáció – és ellenőrzés révén sokkal inkább tud valós képet kapni beosztottjairól, mint a jogszabályokban meghatározott ellenőrzések során. Itt arra gondolok, hogy egy kötetlen beszélgetés alkalmával egy parancsnok olyan szabálytalanságokat is feltárhat vagy megelőzhet, ami egy hivatalos ellenőrzés során esetleg a felszín alatt marad. Jellemző ugyanis az, hogy hivatalos ellenőrzés alatt kevésbé kommunikatívak az ellenőrzöttek, de egy főnök – beosztott kötetlen beszélgetése alatt nyíltabban beszélhet problémákról, gondokról, hiányosságokról egyaránt.

2.5 A minősített adat biztonságának sérülése során végrehajtandó feladatok

A biztonsági vezető a minősített adat biztonságának megsértése esetén haladéktalanul intézkedik az incidens kapcsán felmerülő kár enyhítéséről valamint a jogszerű állapot helyreállításáról. A biztonság megsértése esetén az esemény körülményeit bizottságnak kell kivizsgálni, melynek egyik tagja a biztonsági vezető. A minősített adat biztonságának megsértéséről a biztonsági vezető jelentést készít. A minősített adat védelméről szóló 2009. évi CLV. törvény 19.§ (2) bekezdése alapján az NBF kizárólag a „Szigorúan titkos!", a „Titkos!", valamint a „Bizalmas!" minősítési szintű adat biztonságának megsértésével kapcsolatban kap tájékoztatást, azonban ezen esetekben is csak akkor, ha a megjelölt minősítési szintű minősített adatok illetéktelen személyek részére válhattak hozzáférhetővé vagy annak veszélye fennállt. A 2009. évi CLV. törvény

hatályba lépését követően Magyarországon a minősítési gyakorlatban jelentős változás figyelhető meg. Dolgozatom 1. fejezetének 5. pontjában már illusztráltam a 2009. évi CLV. törvény hatályba lépése előtti állapotot. Az új törvény hatályba lépésével az addigi magasan minősített adatok számának radikális csökkentése következtében a korábbiaktól eltérően jóval nagyobb mennyiségben „Korlátozott terjesztésű!" minősítési szintű adatok jöttek létre. Az új szabályozás szerint a minősített adat biztonságának megsértése esetén azonban – a hatályos szabályozás szerint – a NBF felé a minősített adatot kezelő szervek vezetőinek nem áll fenn tájékoztatási kötelezettsége. Nem hagyható figyelmen kívül az sem, hogy azon minősített adatot kezelő szerv vezetőjének, ahol a minősített adat biztonságának megsértése bekövetkezett, az NBF részére kizárólag az NBF működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Kormányrendelet 60.§ (2) bekezdésében meghatározott tartalmú tájékoztatást kell elkészítenie és megküldenie. Idézem:

„60. § (1) A biztonsági vezető 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.

(2) A minősített adat védelméről szóló törvény alapján a minősítő és a Nemzeti Biztonsági Felügyelet részére a minősített adat biztonságának megsértéséről adott tájékoztatás tartalmazza:

a) a veszélyeztetett minősített adatok azonosításához szükséges adatokat,

b) a biztonság megsértésének körülményeit,

c) a veszélyeztetettség idejét (ismert vagy vélelmezett időhatárait) és helyét,

d) a veszélyeztetettség kialakulásának elsődleges okait,

e) ha ismert, a biztonság megsértéséért felelőssé tehető személy nevét,

f) a megtett intézkedések felsorolását."

Az MH–n belül nem jutottam hozzá olyan információhoz, amely arra utalt, hogy a vezetők alkalmaznak szabályzókon kívüli szankcionálást, felelősségre vonást. Azt vallom, hogy egy találékony vezető olyan módszert is sikeresen alkalmazhat az előírások betartatása érdekében, amely a szabályzókban nincs leírva, viszont a vétkes beosztottat hátrányosan érinti. Nagyon fontosnak tartom az emberi mulasztás okozta incidensek szankcionálása esetében a „zéro tolerancia" elvének megvalósítását az illetékes parancsnok részéről. Elengedhetetlen, hogy a vezető megvizsgálja azokat az okokat, amelyek az információbiztonsági incidenshez vezettek. Fontos tényező például az, hogy szándékos volt – e az elkövetés, ha igen, előre eltervezett, vagy előre nem eltervezett mulasztás – felelőtlenség, hanyagság, megbízhatatlanság – következett-e be. Nem szándékos bekövetkezés esetében érdemes azt is mérlegelni, vajon milyen tényezők

idézhették elő az eseményt. Szabálysértés bekövetkezése során ne maradjon semmi kivizsgálatlanul, ne maradjon hátra „elvarratlan szál”. Lényeges kihangsúlyozni, hogy a szabálysértésnek jól kommunikált következménye kell, hogy legyen,

A szervezetek vezetői sokszor érzik úgy, hogy ha az ellenőrzés során nem kerülnek felszínre nagyobb hiányosságok, akkor minden rendben van a biztonsággal, pedig ez nem feltétlenül van így, ezért az ellenőrzés terén szemléletváltásra is szükség lenne. Ennek egyik formája lehet a szabályzókban előírtak mellett az informális ellenőrzés előtérbe helyezése.

Az MH–ban szerzett ellenőrzési tapasztalataim azt mutatják, hogy az ellenőrzéseket pontosan, a jogszabályokban leírtak szerint végzik. Az ellenőrzések tapasztalatainak még hatékonyabb felhasználásával mód és lehetőség lenne az információbiztonság szintjének emelésére és az MH információbiztonsági kultúrájának fejlesztésére.

Összegzés

Az MH információbiztonsági ellenőrzési rendszerének vizsgálata során megállapítottam, hogy az ellenőrzések a jogszabályokban leírtak szerint, körültekintően történnek. Az éves kötelező ellenőrzések a határidők pontos betartásával zajlanak. A katonai alakulatoknál szerzett és saját munkahelyi tapasztalataim alapján az információbiztonsági kultúra szintjének növelése érdekében a következő javaslatokat teszem:

1. A katonai szervezeteknél a jogszabályokban nem előírt, „informális” ellenőrzéseket javaslom rendszeresen alkalmazni.

2. Az ellenőrzések eredményeit, tapasztalatait hatékonyabban fel kell használni.

3. Ezeket a tapasztalatokat a vezetők egymás között osszák meg, a beosztottakat pedig a szükséges mértékben tájékoztassák.

3. AZ INFORMÁCIÓBIZTONSÁG MEGVALÓSULÁSÁNAK HUMÁN VONATKOZÁSAI

Bevezetés

Disszertációm bevezetőjében a témaválasztásom indoklása című részben kitértem arra, hogy az információbiztonság humán vonatkozásainak vizsgálatát kiemelten fontos feladatnak tartom.
Ezt megerősíti az a tény, hogy – az én személyes, tapasztalatokon alapuló véleményem mellett – a szakma képviselői is hangoztatják: az információbiztonsági incidensek bekövetkezésének oka legtöbb esetben emberi tényezőre vezethető vissza. Erre a tényre alapozva azt kutatom, vajon a személyiség, a személyiséget alkotó emberi tulajdonságok figyelembe vétele csökkenteni tudja-e a humán biztonsági kockázatokat?

3.1 Az személyi biztonság megvalósításának jelenlegi feltételei a minősített adatok tekintetében

Dolgozatom 1. fejezetének 4. pontjában már meghatároztam a személyi biztonság fogalmát, mint az információbiztonság egy fontos részterületét. A személyi biztonság feltételeinek jogi hátterét a 2009. évi CLV. minősített adatvédelmi törvény biztosítja, mely alátámasztására rendelkezésre áll a 90/2010. (III.26.) Kormányrendelet 4. fejezete, valamint a 161/2010.(V.6.) Kormányrendelet 3. fejezete. Míg előbbi a minősített adat kezeléséhez szükséges személyi feltételeket határozza meg, az utóbbi jogszabály a minősített adatkezelő rendszerre és adathordozóira vonatkozó követelményeket írja elő. A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény és az azt módosító 2014. évi CIX. törvény (a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény, valamint egyes törvényeknek a nemzetbiztonsági ellenőrzéssel összefüggő módosításáról) a nemzetbiztonsági ellenőrzés jogi alapját teremti meg.

A jogszabályok alapján minősített adatokhoz személyi biztonsági tanúsítvány és felhasználói engedély kiállítása után jogosult hozzáférni a minősített adatot kezelő személy. Amíg a „Korlátozott terjesztésű!” minősítési szintű adatokhoz a törvény nem ír elő nemzetbiztonsági ellenőrzést, addig a „Bizalmas!”, „Titkos!”, és „Szigorúan titkos!” minősítési szintű adatok eléréséhez a személyi biztonsági tanúsítvány és felhasználói engedély kiállítását nemzetbiztonsági ellenőrzés előzi meg. Az ellenőrzést mindig a munkaadó kezdeményezi, és az MH állományára a Honvédelmi Miniszter rendeli el.
A nemzetbiztonsági kérdőívben a vizsgált személynek nyilatkoznia kell az alábbiakkal kapcsolatosan: [21]
I. Általános személyi adatok;

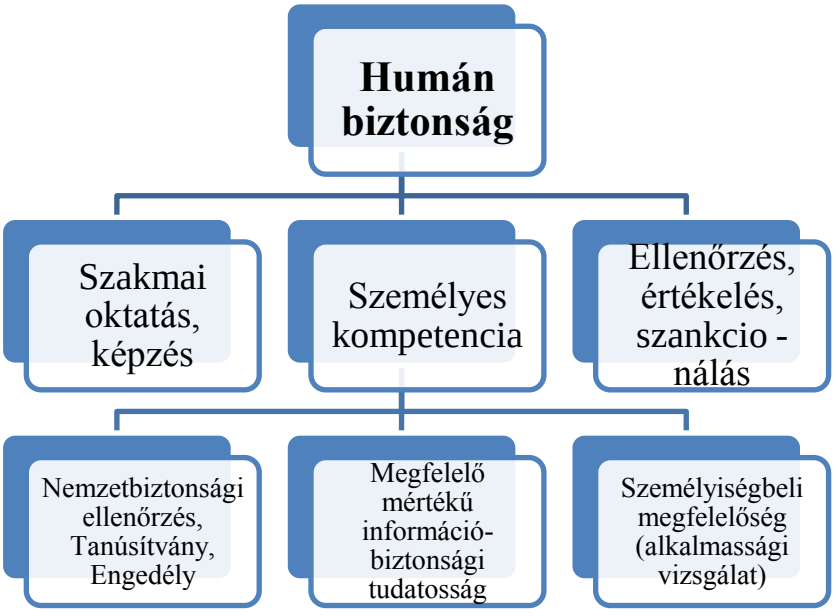
II. Állampolgársági adatok;
III. Családi állapot, gyermekekre, hozzátartozókra vonatkozó adatok;
IV. Lakcímek, tartózkodási helyek adatai;
V. Iskolai végzettségre vonatkozó adatok;
VI. Foglalkozással kapcsolatos adatok;
VII. Katonai adatok;
VIII. A vizsgált személy, házastársa, és élettársa jövedelmi viszonyával, anyagi helyzetével összefüggő adatok;
IX. A vizsgált személy, és a vele közös háztartásban élő hozzátartozója vagyoni helyzete (ingatlan, ingóság), valamint pénzintézetekkel fennálló tartozása;
X. Büntető és szabálysértési eljárások adatai;
XI. Speciális adatok (például: Megkereste-e korábban valamilyen hírszerző szolgálat?);
A vizsgált személy és házastársa/élettársa külföldi állampolgárságú személlyel fenntartott magánjellegű kapcsolata. Életvitelre valamint hivatalos, közösségen kívüli partnerkapcsolat fenntartására vonatkozó kérdések is szerepelnek ebben a pontban. A teljes nemzetbiztonsági kérdőív a NBF honlapján (nbf.hu/dokumentumok/iratmintak) található.
Összességében a kérdőív a vizsgált egyén személyes adataira vonatkozó kérdéseket tesz fel, az illetővel kapcsolatos büntetési és szabálysértési eljárásokat vizsgál, valamint életviteli és életmódbeli feltérképezést készít az illetékes Nemzetbiztonsági Szolgálat. A vizsgálat lezárásával a Szolgálat egy szakvéleményt ad ki, amely a vizsgált személy kockázatmentességét bizonyítja. A munkaadó szerv ezután állítja ki a Személyi Biztonsági Tanúsítványt (nbf.hu/dokumentumok) és a Felhasználói Engedélyt (nbf.hu/dokumentumok). Rejtjeltevékenység végzése esetén ehhez Rejtjelhozzáférési – engedély (nbf.hu/dokumentumok) is szükséges. Ezek után az egyén bevizsgált olyan munkakör betöltésére, amelyben minősített adattal való munkavégzésre feljogosítható.
Kutatásaim egyik fő kérdése, vajon a nemzetbiztonsági ellenőrzés folyamata és az engedélyek kiadása elegendő-e ahhoz, hogy egy személy olyan súlyú minősített információkhoz juthasson hozzá, amik esetleg embertömegek vagy védelmi szervezetek és kritikus infrastruktúrák biztonságát veszélyeztetik?
Feltételezésem szerint a jelenleg használt hivatalos protokoll a humán biztonság megvalósításának csak egy része, amely oktatással, szakmai felkészítéssel kell, hogy párosuljon. Mindezek mellett elengedhetetlen tényezőnek tartom az egyén személyiségvonásainak, emberi tulajdonságainak vizsgálatát, az információbiztonsági

kultúra kialakítását és fejlesztését, valamint az ellenőrzést és a korrekt, következetes szankcionálást.

A fentiek alapján humán kockázatnak minősülnek azok az alkalmazottaknál fennálló személyi körülmények – különösen a negatív személyiségjegyek, konfliktusokkal terhelt környezeti vagy élethelyzetekből származó fenyegetettségek, életviteli és mentális problémák –, amelyek fennállása önmagukban nem, de az adott, fokozott kockázatú, bizalmi elvre is építő munkakörökben végzett munkavégzéssel összefüggésben fenyegetettséget jelenthetnek egy szervezet számára.

Ritkán esik szó még egy, általam fontosnak tartott tényezőről: a munkavégzés feltételeinek megteremtéséről[26]. Ezek az összetevők hozzájárulnak a kockázatok csökkentéséhez, az információbiztonság megvalósulásához.

A humán biztonság szemléltetése céljából egy olyan ábrát készítettem, amely tartalmazza azokat az alapvető összetevőket, amelyek feltétlenül szükségesek ahhoz, hogy információbiztonsági munkakörben minősített adatokkal, minősített adatkezelő rendszerekkel egy adott személy munkát végezhessen. Ezek figyelembe vételével elérhető lenne a kockázatok mértékének csökkentése a humán biztonság területén.



9. sz. ábra: *A humán biztonság összetevői – saját szerkesztés*

[26] Összetevők: előírások szerinti munkakörnyezet, releváns szabályzók, tisztázott alá – fölérendeltségi viszonyok, korrekt vezetés - irányítási struktúra, rugalmas, biztonságos informatikai rendszer

A személyes kompetencia olyan adottságokat, jellemvonásokat, értelmi és érzelmi viszonyulásokat jelent számomra, amelyek lehetővé teszik a hatékony és eredményes munkavégzést.

3.2 Az emberi tényező szerepe a biztonság megteremtésében és megtartásában

Az információbiztonság mozgatórugója az ember, ennek ellenére az érintettek nem fordítanak kellő figyelmet az emberi tényező jelentőségére. A biztonsági rendszer kockázatainak elemzése során egyértelműen kijelenthető, hogy még mindig a humán faktor (emberi tényező) a leggyengébb láncszem. [22] Nehéz ennek a pontos okát megmondani, de talán az fontos szerepet játszik, hogy vannak olyan emberi tulajdonságok, amelyek kockázatot jelenthetnek az információbiztonsággal szemben. Az ember nem „gépként" működik, hibázhat, befolyásolhatóvá válhat, megtéveszthető és megzsarolható, nem utolsó sorban a fizikai – adminisztratív –, és elektronikus biztonság megteremtése is az ő feladata, vagyis az egyén felelőssége óriási. Fontos figyelembe venni azt is, hogy az ember biztonságot veszélyeztető tulajdonsága a bizalomra épülés, a kommunikációs hajlam és a dicsekvés.

Az információbiztonság megteremtése tehát olyan komplex feladattal terheli meg az egyént, amely számos kockázati tényezőt von maga után. Dolgozatom megírása folyamán most értem el ahhoz a pillanathoz, amikor a biztonság témakörében kiléphetek a jogszabályi keretekből[27]. A továbbiakban arra keresem a választ, vajon van-e összefüggés a személyiségjegyek, a pszichológiai vizsgálatok, a személyi alkalmasság, a biztonságtudatosságra való törekvés és a biztonságtudatosság fejlesztése között?

3.3 Személyiségvizsgálatok

A személyiség fogalmának meghatározása rendkívül összetett. A meghatározást filozófiai és világnézeti kérdések is befolyásolják. Jelentős mértékben függ attól is, hogy éppen melyik pszichológiai irányzathoz tartozó elméletalkotó határozza meg a jelentését. A személyiség kifejezés az ókori latin persona (maszk) szóból ered. Ez azt sugallja, hogy a klasszikus korban a hangsúly egy ideig a külső megjelenésen volt, majd fokozatosan a belső tulajdonságokkal is kezdtek foglalkozni. A személyiség a személy viszonylag stabil tulajdonságainak összessége, amelynek együttese csak az adott egyénre jellemző. Ez a tulajdonsághalmaz különbözteti meg az egyes embereket.

[27] A korábbi fejezetek – Az információbiztonság jogi szabályozása az MH – ban; A minősített adatvédelmi rendszer működtetésében részt vevő személyek; Az információbiztonság ellenőrzési rendszere az MH – ban – teljes mértékben jogszabályi háttérre alapulnak.

Allport[28] [23] szerint: „A személyiség azoknak a pszichológiai rendszereknek a dinamikus struktúrája az egyénben, amelyek a környezethez való egyéni alkalmazkodást meghatározzák. Ez a „szerkezet" egy viszonylagos állandóságot feltételez, ugyanakkor az emberek nagyon lassan és fokozatosan, de változnak. Mivel ez a folyamat lassú, ezért megítélésünk egy időszakra vonatkoztatva megbízható lehet".

A személyiség meghatározottságának vizsgálata régóta foglalkoztatja a szakembereket. Ugyanakkor szeretném hozzáfűzni, hogy a személyiség alapvető összetevőinek kutatására tett kísérletek nem látszanak nagyon eredményesnek. Az amerikai pszichológia inkább a környezet meghatározottságára esküszik, ezzel szemben az európai irányzatok inkább arra helyezik a hangsúlyt, ami az emberi természetben veleszületett, és viszonylag változatlan. Vizsgálati eredmények azonban azt is bizonyítják, hogy egy adott szituáció – mint például a kulturális környezet is jelentős befolyást gyakorol a személyiségre.

Az emberi pszichikum vizsgálatakor általánosan kijelenthető, hogy az emberek nem csupán nemükre, korukra, külső adottságaikra nézve különböznek egymástól, hanem személyiségjegyeik is eltérőek.

Éppen ezért a biztonság fogalma is szubjektív, ugyanis az egyik ember számára valamely körülmény biztonságos, a másik ember pedig ugyanazon körülmények között a biztonság hiányát érzi. Személyiségünk tulajdonságai meghatározóak lehetnek abban, hogy a bennünket ért hatásokra milyen módon reagálunk. Személyiségünket tehát azok a tulajdonságok határozzák meg, amelyekkel rendelkezünk.

A pszichológiai kutatások eredményét felhasználva utalni szeretnék arra, hogy az egyes emberek személyisége mennyire különböző lehet, és ez milyen mértékben határozza meg az egyén életét. A pszichológiai kutatások közül Carl Gustav Jung[29] személyiségtípus elméletét emelem ki, amely kiválóan bemutatja az egyének különbözőségeit. [24]

Jung könyve, a Lélektani típusok 1921-ben jelent meg németül. Ebben Jung személyiségtípus – felfogását, és ennek részletes értelmezését írta le.

Jung *általános beállítódás szerint* vizsgálta az embereket. Azt akarta megtudni, hogy a személyiségük belső ösztönző ereje (libidó) önmaguk vagy a környezetük felé irányul – e. Ez alapján két típust nevezett meg:

Introvertált – befelé forduló (megfontolt, töprengő, a külső kapcsolatokat nem kereső, érzelmileg nehezen kötődő és szorongásra hajlamos).

[28] Gordon Willard Allport (1897-1967) amerikai szociológus és szociálpszichológus, a személyiségelméleti kutatások klasszikusa, a pszichoanalitikus és a behaviorista lélektan határozott ellenfele.
[29] Carl Gustav Jung (1875 – 1961) svájci pszichiáter, pszichológus, analitikus.

Extrovertált – kifelé forduló (vidám, tetterős és gyorsan reagál mindenre, szívesen keresi az emberi kapcsolatokat).

A két típus gyakran konfliktusban állhat egymással, és hajlanak egymás lebecsülésére. Tisztán ritkán fordulnak elő, inkább speciális vagy funkciótípusa segítségével alkalmazkodik, és tájékozódik a külvilágban az egyed.

Négy nagy *funkciótípus* van:

- gondolkodás
- érzelem, érzés
- érzékelés (tapasztalat)
- intuíció.

Ez a négy funkciótípus mind a két beállítottsági típusra jellemző lehet. Ennek értelmében minimálisan nyolc jól elkülöníthető típus áll elő[30]. Ezek variációi összesen 16 típust adnak, melyek közül a kutatók szerint az ENTJ[31] (extrovertált, iNtuitív, gondolkodó, megítélő) képes a biztonsági kultúra követésére, azonban fontos kihangsúlyozni, hogy képzéssel más személyiség esetében is fejleszthető ez a képesség. **Az ENTJ személyiségek kifejezetten igénylik, hogy egy szabályozott, minden választási lehetőségre választ adó szabályrendszer kötöttségei között, rendszeresen ismétlődő, kiszámítható tevékenységeket végezzenek, ahol a csoport vezetője meghatározott rendszerességgel ellenőrzi a munkájukat, és visszajelzést ad. Feltételezhető, hogy ez a típus az információbiztonság területén kisebb biztonsági kockázatot jelent a személyiségjegyek szempontjából.**

Jung mellett érdemes figyelmet fordítani egy másik híres szakemberre Hans Jürgen Eysenckre[32], aki a XX. század végén a leggyakrabban idézett pszichológus a tudományos folyóiratokban. Munkássága során az intelligenciával és a személyiséggel kapcsolatban végzett kutatásokat, de számos területen is kiemelkedő szerepe volt.

Eysenck 1947-ben 700 neurotikus katona megvizsgálása után 39 személyiségjellemző[33] statisztikai vizsgálatát végezte el. A vizsgálat módszere a faktoranalízis[34] volt, amely segítségével számos jellemzőt, tulajdonságot néhány csoportba – faktorba – rendezhetünk,

[30] Beszélhetünk, tehát extrovertált gondolkodóról, introvertált gondolkodóról, extrovertált érzőről, introvertált érzőről, extrovertált érzékelőről, introvertált érzékelőről, extrovertált intuitív és introvertált intuitív típusokról.
[31] ENTJ Extraverzió+iNtuíció+Thinking+Judging
[32] Hans Jürgen Eysenck (1916 - 1997) német-angol pszichológus
[33] Lásd: 12. számú ábra
[34] A módszer a pszichológiában a személyiség szerkezetének, modelljének vizsgáló többváltozós kutatások alapjául szolgál, de azokon a területeken alkalmazható leginkább, ahol nagy mennyiségű adattal dolgoznak. A faktorelemzés módszerét alkalmazzák a pszichometriában, a viselkedés- és társadalomtudományokban, használja a szociológia, a marketing, a termékmenedzsment és az operációkutatás is.

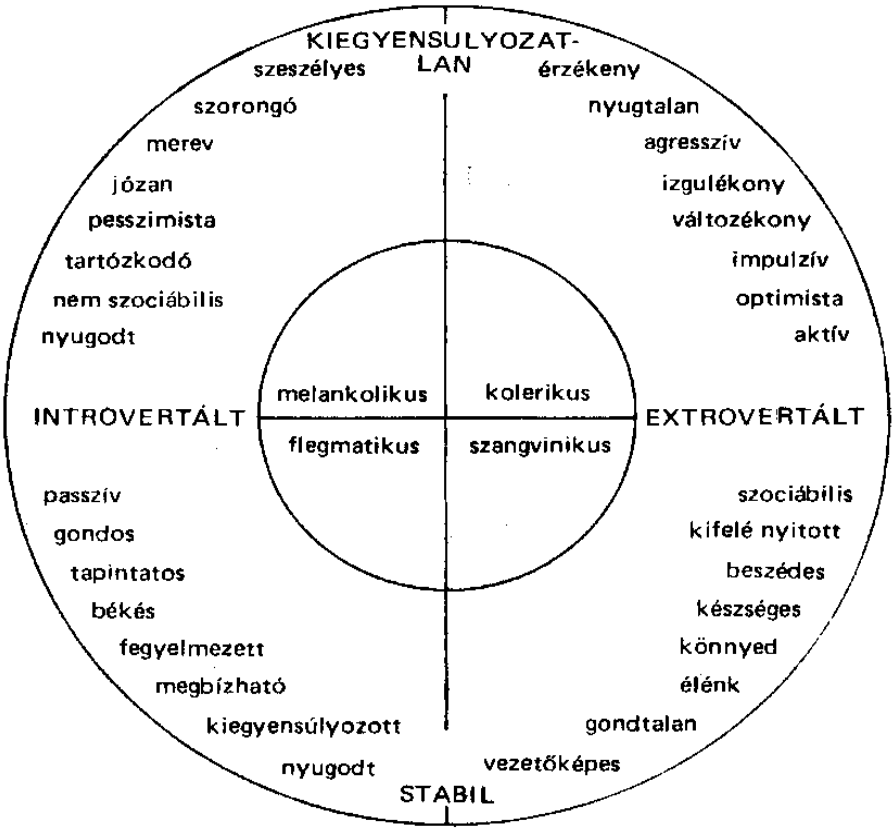
egyszerűsíthetünk. Eysenck a faktoranalízis segítségével arra az eredményre jutott, hogy két alapdimenzió különíthető el: extroverzió – introverzió (Jung), illetve a neurotikusság – stabilitás (Pavlov).

Eysenck elméletében [25] az ember érzelmi labilitása vagy stabilitása abban mutatkozik meg, hogy a személy milyen könnyen és gyakran borul ki, keseredik el, lesz rosszkedvű, szorongó és levert.

Az instabil személyek: kiegyensúlyozatlanok, érzelmeik múlóak, változékonyak, gyakran szorongással küszködnek.

A stabil személyek: kiegyensúlyozottak, optimisták, érzelmeik tartósak. Nyugodt személyek, fegyelmezettek, munkájukat gondosan végzik.

Eysenck vonáselméletét az alábbi ábrával szemléltetem.



10. sz. ábra: *Eysenck vonáselmélete*

Az elmélet szerint négy típus különböztethető meg: extrovertált érzelmileg stabil, extrovertált érzelmileg labil, introvertált érzelmileg stabil és introvertált érzelmileg labil. **A négy típus közül az extrovertált érzelmileg stabil típus alkalmas leginkább információbiztonsági munkakör betöltésére.**

Az előbbi elméletek választ adnak arra a kérdésre, hogy érdemes – e a személyiséggel foglalkozni abban az esetben, amikor a humán biztonság kérdéskörét vizsgáljuk. A fenti személyiségvizsgálatok bizonyítják, hogy az eltérő személyiségjegyek óriási szerepet játszanak abban, hogy a különböző feladatok elvégzésére egyes emberek jobban alkalmasak, mások pedig kevésbé. Természetesen utóbbiak egy más jellegű feladatkör betöltésére, tökéletesen megfelelőek lehetnek.

Összegzés

Ebben a fejezetben a humán biztonság összetevőinek kutatásával foglalkoztam, különös figyelmet fordítva a minősített adatkezelés esetén. A jogszabályi háttér vizsgálatával arra jutottam, hogy **a kockázatok csökkentése érdekében egy kiterjedtebb, sokoldalúbb szűrésre volna szükség, ami a munkavállalók személyiségbeli vonásait is figyelembe veszi.** Megvizsgáltam, hogy **az ember bizalomra épülése**, az információbiztonság megvalósítása során betöltött összetett szerepe, **és személyiségbeli tulajdonságai jelentik a legnagyobb információbiztonsági kockázatot.**

4. INFORMÁCIÓBIZTONSÁGI STRATÉGIA. AZ INFORMÁCIÓBIZTONSÁGI KULTÚRA FEJLESZTÉSE A BIZTONSÁGTUDATOSSÁG KIALAKÍTÁSÁVAL ÉS NÖVELÉSÉVEL

Bevezetés

Az utóbbi évek statisztikái szerint naponta megközelítőleg a Föld népességének 40% – a használ internetet. 1993 óta a felhasználók száma folyamatosan növekszik. 2010–ben 2 milliárd, 2014–ben 3 milliárd, 2015–ben 3,2 milliárd, 2016–ban pedig már több mint 3,4 milliárd felhasználó kapcsolódik naponta az internethez [26]. Átlagban másodpercenként 57.000 keresés történik a Google – ben [27], a 2015 márciusi állapot szerint a filmkészítők a youtube–on több mint 10000 videót töltöttek fel, amit 1 milliárdan néztek meg 70 millió óra alatt [28]. 2014 és 2016 között 15%–kal nőtt a letöltött alkalmazások száma, amely számokban kifejezve 90 milliárd feletti mennyiséget jelent [29]. A Facebook 500 millió aktív felhasználót könyvelhet el, akiknek fele naponta csatlakozik a közösségi hálóhoz [30].

2013–ban több mint 100 milliárd e–mail került elküldésre illetve fogadásra [31], és az Amazon[35] nettó negyedéves bevétele 2016–ban 252 millió dollár volt [32]. 2013–ban 1,8 millió kártékony és nem kívánt programot azonosítottak a kutatók [33]. Ezen kártékony programok célpontjai az informatikai rendszerek, eszközök és nem utolsó sorban a felhasználók „virtuális élete”. Ezek a riasztó adatok az embereket nem csupán „civil” felhasználóként érintik, hanem munkájuk és hivatalos – online bankolás, kapcsolattartás állami szervekkel–tevékenységük során egyaránt.

A fenti adatok rávilágítanak arra, hogy a virtuális térben mind az eszközök, a rendszerek, mind azok felhasználói rengeteg támadásnak vannak kitéve. A szakembereknek nem maradt más lehetőségük, mint kísérletet tenni a minél magasabb szintű biztonság megteremtésére, és felvenni a harcot a támadásokkal szemben.

Annak érdekében, hogy egy adott szervezetnél az információbiztonsági kockázatokat csökkenteni tudjuk, nagyon fontos tényezőnek tartom az információbiztonsági stratégia, az információbiztonsági kultúra kialakítását és fejlesztését.

4.1. A biztonságtudatossági szint növelésének lehetőségei

A szakemberek elsődleges feladata a minél magasabb szintű biztonság megteremtése, amely a biztonsági kockázatok minimális szintre való csökkentésével érhető el. Az információbiztonsági kockázatok növekedését azonban elősegíti az emberek természetes, bizalomra való hajlamának

[35] Online Shopping for Elektronics, Apparel, Computers, Books, DVDs and more…

kihasználása. Ezt a folyamatot – vagyis az emberek pszichológiai manipulációját – a megtévesztés „tudományának”, vagy más néven *Social Engineeringnek* is nevezzük [34]. A támadó a befolyásolás, rábeszélés és a meggyőzés módszerével ráveszi áldozatát, hogy együttműködjön vele, ezáltal esetleg olyan információt adjon ki, amely alapjául szolgálhat informatikai rendszerek, technológiai eszközök elleni támadásra.

A Social Engineering fogalom megalkotója – és nagy gyakorlati megvalósítója – Kevin Mitnick ex-hacker volt. Mitnick szerint ez a támadási forma az emberek hiszékenységére és együttműködő képességére alapozó támadási forma [35]:

„Így a felhasználókat a következőkre kell külön felkészíteni:

- *Keltsen bennük gyanakvást, ha bárki a jelszavunk, vagy a bejelentkezési procedúráink iránt érdeklődik.*
- *A szabadon hagyott gép, szabadon hagyott préda. Egyfelől látják, hogy nem dolgozunk, másfelől ezek a gépek szabad prédák az adatrablók számára.*
- *Bárki, aki informatikusként „csak úgy” felhív minket, hogy segítséget nyújtson, fogadjuk azt kétkedéssel (informatikusok nem szoktak csak úgy segíteni).*
- *Ha szervezet-idegen személy sokat „legyeskedik” az információkat kezelő eszközök közelében, az keltse fel a gyanakvásunkat, esetleg vonjuk őt kérdőre.”*

Az adatvédelem előtérbe kerüléséről a Nemzetbiztonsági Szolgálatok is készítettek értékelést:

„A felhasználók sok esetben nincsenek tisztában azzal a ténnyel, hogy az ingyenes alkalmazások legtöbbször azért tudnak díjmentesek maradni, mert bizonyos adatokat gyűjtenek a használóról (pozíció, látogatott weboldalak, névjegyzék, stb.). A gyűjtött adatok létrehozóiknak úgy tudnak profitot termelni, hogy harmadik fél számára tovább értékesítik azokat, akár úgy is, hogy ennek nincs tudatában a felhasználó. Fontos, hogy minden esetben tisztában kell lenni adataink értékével – amelyek például marketing és kiberbűnözés szempontjából egyre nagyobb értéket jelentenek – így az adatvédelem kérdése egyre inkább előtérbe kerül.” [36]

Az Internet feltalálása, kifejlesztése és továbbfejlesztése óriási előnyt jelent az ember életében azzal, hogy olyan lehetőséget biztosít a felhasználók számára, amely segítségével megszámlálhatatlan mennyiségű információhoz és személyhez férhetnek hozzá világszerte. Azonban ami a legnagyobb előnye az egyben hátránya is, hiszen károkat, rombolást, teljes megsemmisülést is okozhat az emberek életében. Erre napjainkban komoly bűnözői ipar épült. Ezért nagyon fontos, hogy a biztonság területén mindig szkeptikusak maradjunk. Sosem szabad megbízni kizárólag a technikában vagy az adminisztratív szabályozásban. Mivel nincs totális biztonság, törekedni kell a minél komplexebb védelem kialakítására. Pusztán azért, mert erős

tűzfalat vagy kódolást használunk, valamint nincs vezeték nélküli hálózat a rendszerben, még nem szabad biztonságban érezni magunkat.

Az utóbbi évtizedekben az információ biztonsága, a hivatalok, a cégek és magánszemélyek adatainak védelme egyre inkább központi kérdéssé válik. Az adatok véletlen vagy szándékos kompromittálódása, sérülése, ellopása vagy rossz szándékú manipulálása komoly erkölcsi károkat okoz az érintett szereplőknek, elveszíthetik jó hírnevüket. E mellett sokszor anyagi –, kártérítési – és büntetőjogi következményei is lehetnek az adatok helytelen kezelésének. Az adatvesztés, adat – kompromittálódás legtöbbször emberi tényezőkre vezethető vissza. Az ember szándékos vagy nem szándékos károkozásával tönkreteheti a „bombabiztos" technikai megoldásokat is.

Egyre több olyan kezdeményezést fedezhetünk fel, amelyek az információbiztonság tudatosság[36] fejlesztésére tesznek lépéseket. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. L. törvény a védelemhez számos feltételt szab, többek között rendelkezik a felhasználók biztonságtudatossági képzéséről. A 41/2015. (VII. 15.) BM rendelet pedig a következőket határozza meg:

„Biztonság tudatosság képzés - Az érintett szervezet annak érdekében, hogy az érintett személyek felkészülhessenek a lehetséges belső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést nyújt az elektronikus információs rendszer felhasználói számára." [37]

Ezeket a képzéseket nem csak belépéskor kell lebonyolítani, hanem az ismeretek frissítése, aktualizálása érdekében rendszeresen (évente) meg kell tartani.

Az MH vonatkozásában a biztonságtudatosság stratégiájának kialakításához hasznos támpontot ad az MH Kibervédelmi Szakmai Koncepciójának megjelenése [38]. A jogszabály formai vagy tartalmi követelményt nem határoz meg, így a stratégiai szintű szabályozásra vonatkozó általános követelmények szerint kell az alkalmazó szervezeteknek eljárnia, és az „intézményi stratégia" kialakítására vonatkozó általános feladatokat kell figyelembe vennie, kiegészítve a honvédelmi sajátosságokból adódó eltérésekkel.

A biztonságtudatosság kialakítását és fejlesztését célzó szakmai kihívás rendkívül összetett, és az egész MH–ra vonatkozik. A feladat sikeres megoldásához szükség van a végrehajtás központi támogatására, a szervezetek vezetőinek aktív együttműködésére és a beosztott állomány közreműködésére is.

[36] A szervezet tagjainak tudása és attitűdje a szervezet tulajdonában, vagy kezelésében lévő információs javak védelmével kapcsolatban. MVM Zrt. Konferencia 2017. 05. 24. Tarján Gábor: Az információbiztonsági tudatosság mérése gazdálkodó szervezeteknél.

4. 2. A biztonságtudatos szervezet jellemzői

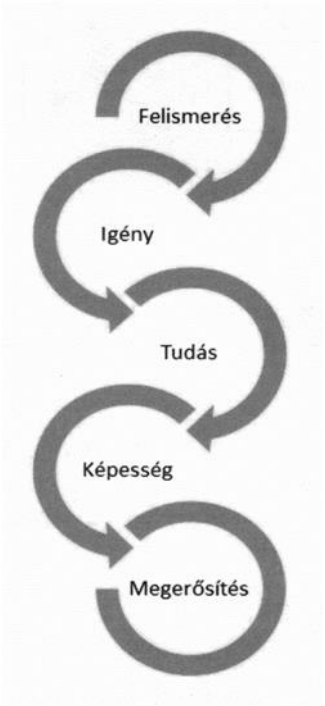
„*A szervezet biztonságáért vállalt felelősség, a szervezet vezetése által meghatározott biztonsági szintnek, mint követelménynek elfogadása és a hiánya következményeinek elismerése, valamint a biztonsági szempontból erkölcsös, etikus magatartási kultúra együttesen jellemzi a biztonság tudatos szervezetet."* [39]

Fejlett biztonsági kultúráról akkor beszélhetünk, amikor az ismeretek elsajátítása és a megvalósítás együttesen érvényre jutnak. Ha felkészítjük a szervezet alkalmazottait arra, hogy felelősen, a biztonságot veszélyeztető tényezők ismeretében végezzék munkájukat, valamint a munkavégzéshez szükséges munkaeszközöket és információs rendszereket biztonságtudatosan használják, akkor bizonyosak lehetünk abban, hogy kisebb anyagi ráfordítással érjük el az információbiztonsági kockázatok csökkenését. Itt elsősorban arra gondolok, hogy a szervezet dolgozói megfelelő oktatásban, képzésben részesülnek, és az ott elsajátított ismereteket alkalmazni tudják, alkalmazni akarják. Az *akarat* szót szándékosan hangsúlyoztam ki, mert véleményem szerint biztonságtudatos magatartást csak abban az esetben tudunk tanúsítani, ha mi magunk is fontosnak tartjuk ezt. A biztonságtudatos viselkedésnek alapja, hogy mi magunk felismerjük egyrészt azt, hogy a tudatosság hiánya veszélybe sodorhat minket vagy szervezetünket, másrészt pedig képesek vagyunk átlátni, hogy ilyen helyzetben mit kell tennünk, hogyan cselekedjünk. Ez azonban egy bonyolult, sok lépcsős, komplex folyamat, amely az egyén információbiztonsággal kapcsolatos gondolkodását alapvetően megváltoztatja. Ennek sikeres megvalósításához nyújthat támpontot az ADKAR[37] modell, amelyet 1999-ben mutattak be.

Ez az egyik legsikeresebben alkalmazott, egyénekkel foglalkozó célorientált módszer. A módszer alkalmazásával felmérhető, hogy a változtatásmenedzsment lebonyolításának milyen nehézségei, buktatói vannak. E módszer segítségével képet kaphatunk arról is, vajon milyen a munkatársak változásokhoz való viszonya, hozzáállása. Jelen esetben a változtatásmenedzsment alatt a szervezet biztonsági kultúrájának fejlesztését, és a biztonságtudatosság erősítését értem.

A modellt Molnár Imre doktori értekezésében bemutatott saját készítésű ábrájával szeretném szemléletesebbé tenni:

[37] Ábra és ismertetés a következőkben



11. sz. ábra: *ADKAR modell*

A modell neve mozaikszó, amely az alábbi szempontok szerint értelmezendő:
Awareness – felismerés;
Desire – igény;
Knowledge – tudás
Ability – képesség
Reinforcement – megerősítés.
A szervezetek vezetése által kialakított és támogatott magas szintű biztonsági kultúra elősegíti azt, hogy az egyén maga is biztonságtudatosabbá akar válni, és ezt képes is megvalósítani.
Akkor lehetünk sikeresek, ha felkeltjük az emberekben az igényt arra, hogy késztetést érezzenek a változásra. Jelentős előrelépést jelenthet, ha az alkalmazottak megértik, hogy a biztonsági rendszabályok őket és a szervezetet védik, és nem csak egy adminisztratív szabályozás, aminek be nem tartása büntetést von maga után. Ennek a folyamatnak a megvalósítása olyan erős motivációt adhat a szervezetek munkatársainak, amely az információbiztonsági kultúra fejlesztésének alapját képezheti. Ehhez iránymutatást adhat, és segítséget nyújthat a jogszabályi háttér valamint a szervezet vezetése, a humánpolitikája és a belső szabályozás.

A biztonsági kultúra kialakításához és fejlesztéséhez támpontot nyújt az OECD[38] az információs rendszerek és hálózatok biztonságára vonatkozó útmutatóban [40], amelyben kilenc alapelvet határoztak meg a biztonsági kultúra megvalósítása érdekében. Ezek a következők:

- Tudatosítás elve

Az alkalmazottaknak meg kell érteniük és tudatosítani kell magukban, hogy az információs rendszerek és hálózatok hasznát csak úgy élvezhetik, veszélyeiket csak úgy kerülhetik el, ha a biztonsági kockázatok tudatában használják őket.

- Felelősség elve

Ahhoz, hogy a biztonságot fenn tudják tartani, minden alkalmazottnak tudatában kell lennie saját felelősségével, és ezt számon kell tudni rajta kérni. Minden szervezetnek rendszeresen felül kell vizsgálnia saját szabályzatait, gyakorlatait, intézkedéseit és eljárásait, valamint értékelnie kell, hogy ezek megfelelőek-e.

- Válaszintézkedések elve

A dolgozóknak kellő időben, egymással együttműködve kell a váratlan biztonsági eseményeket megelőzni, észlelni, illetve az ezekre vonatkozó megfelelő válaszintézkedéseket megtenni. Szükség szerint meg kell osztaniuk egymással a fenyegetésekkel és sebezhetőségekkel kapcsolatos információkat, ezen túl gyors és hatékony eljárásokat kell alkalmazniuk, hogy együttműködve megelőzzék, észleljék a váratlan biztonsági eseményeket, illetve megfelelő módon tudjanak reagálni azokra.

- Etika elve

Az érintetteknek tiszteletben kell tartaniuk mások jogos érdekeit. Az egyéneknek fel kell ismerniük, hogy cselekedeteik vagy azok hiánya adott esetben káros hatással is lehetnek a többi alkalmazottra. Az érintetteknek törekedniük kell arra, hogy a jó gyakorlatokat kialakítsák, és alkalmazzák, a biztonság igényét elfogadják, és mások jogos érdekeit tiszteljék.

- Demokrácia elve

Az információs rendszerek és hálózatok biztonságát megvalósító megoldásoknak a demokratikus társadalmak alapvető értékeivel összeférhetőnek kell lenniük.

A gondolatok és eszmék cseréjének szabadságát, az információ szabad áramlását, a személyes adatok megfelelő védelmét, a nyitottságot és az átláthatóságot indokolatlan mértékben nem szabad korlátozni.

[38] OECD: Organisation for Economic Co – operation and Development – Gazdasági Együttműködési és Fejlesztési Szervezet

- Kockázatfelmérés elve

A biztonság tervezése és megvalósítása során a releváns lényeges kockázatokat fel kell mérni. A kockázatfelmérés lehetővé teszi a még elfogadható szervezeti kockázati szint meghatározását. Ezen túl segítséget nyújt az információs rendszerek és hálózatok biztonságát fenntartó megfelelő szabályozások kialakításában a megvédendő információ jellegével és fontosságával arányban. Tekintettel az információs rendszerek összekapcsolására, a kockázatfelmérésnek ki kell térnie a másoktól származó vagy a mások részére okozható hatásokra.

- Biztonságtervezés és végrehajtás elve

Az érintetteknek a biztonságot az információs rendszerek és hálózatok kialakítása során lényeges szempontként kell kezelni és megvalósítani.

- Biztonságmenedzsment elve

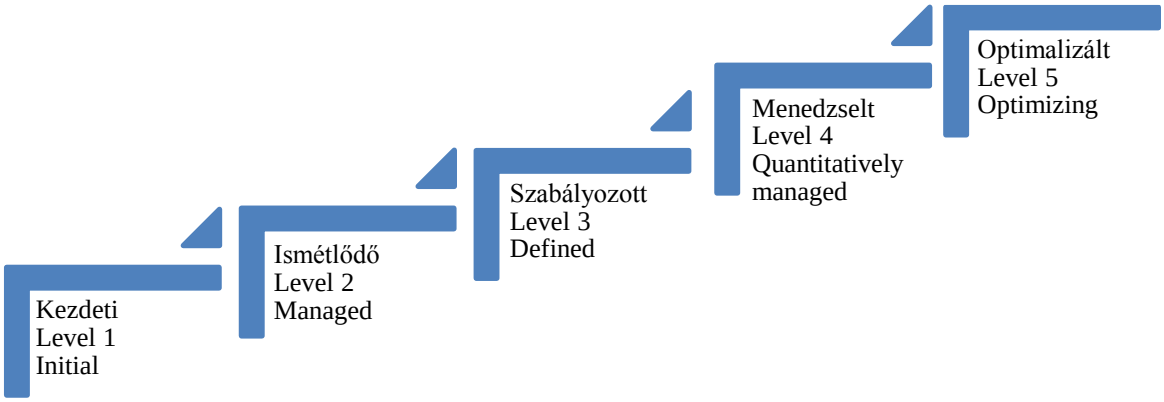
Az érintetteknek minden szempontra kiterjedő módon kell a biztonságmenedzsment feladatokat végezniük. A biztonságmenedzsmentnek kockázatfelmérésen kell alapulnia, felölelve az érintettek tevékenységének és működésének minden vonatkozását.

- Újraértékelés elve

Mivel folyamatosan jelennek meg új és változó fenyegetések és sebezhetőségek, az érintetteknek az információs rendszerek és hálózatok biztonságát folyamatosan felül kell vizsgálniuk, és újra kell értékelniük. A biztonsági irányelvekben, gyakorlatokban, intézkedésekben és eljárásokban szükséges módosításokat el kell végezniük.

A szervezeti kultúra létrehozásának sikerességét, a szervezetek biztonsági szintjét többféle modell szerint lehet értékelni. Az alábbi táblázatban a CMM[39] szerinti érettségi modellt szeretném bemutatni. A modellben öt fokozat található, amely alapján kiértékelhető egy szervezet fejlettsége a szabványos folyamatok kifejlesztése és követése tekintetében. A modell nagyon jól rávilágít arra, hogy az információbiztonsági kultúra kiépítése, fejlesztése egy fokozatos, egymásra épülő struktúrák létrehozásával végbemenő folyamat. Ebben a folyamatban fő szerepet kell kapnia az alapoknak, amelyek biztosítani tudják a tudatos és színvonalas fejlesztést.

[39] Capability Maturity Model – Képesség-érettség modell



12. sz. ábra: *Képesség - Érettség Modell – saját szerkesztés*

A Capability Maturity Model 1. szintje (kezdeti/initial) még csak kezdeti, ad-hoc érettségi szinttel rendelkezik. Ebben az esetben a szervezet már felismerte a biztonsági kultúra fontosságát, de nem tudatosan készíti fel a munkatársakat. Ezen a szinten is már igény mutatkozik a biztonsági kultúra fejlesztésére.

A Model 2. szintjén (ismétlődő/managed) a szervezet vezetése elvárja a biztonsági kultúra kialakítását, de nem törekszenek tervszerűen rá. A jogszabályoknak való megfelelésre viszont igyekeznek hangsúlyt fektetni.

A 3. szinten (szabályozott/defined) a szervezet létrehozta a biztonsági kultúra fejlesztési programot, de korlátozottak a megvalósítás eszközei. A szervezetnél a jogszabályoknak való megfelelés adott.

A 4. szinten (menedzselt/quantitatively) a szabályozottságnak köszönhetően eredményes a program megvalósítása, tudatosan részt vesznek benne a felhasználók. Ennek a szintnek az eredménye az, hogy szabályok szerint, folyamatosan, megfelelő szinten menedzselt rendszer jön létre.

Az 5. szinten (optimalizált/optimizing) megvalósul az optimalizáltság, a biztonsági kultúra fejlett, áthatja a szervezetet, a biztonsági kultúra fejlesztése beépült a szervezet folyamataiba. Ezen a szinten a biztonsági kultúra mutatószám rendszer[40] segítségével irányított és fejlesztett.

4.3 A biztonsági kultúra kialakításának és fejlesztésének időszerű kérdései

Amikor egy szervezetnél a biztonsági kultúra, a biztonságtudatosság kérdése felmerül, ideális esetben mind a vezető, mind a biztonságért felelős szakemberek minden lehetséges eszközt felhasználnak annak érdekében, hogy a kockázati tényezőket minimálisra csökkentsék. Az egyik

[40] Közérthetően nem csak az IT biztonságról Budapest, 2013. p. 106.

legjelentősebb belső kockázati tényezőt a hamis biztonságérzet jelenti. Nagyon fontosnak tartom, hogy a cégek vezetése vagy az MH szintjén a Parancsnokok minden esetben rendszeresen tájékoztassák beosztottjaikat az információbiztonság adott szintjéről, többek a hiányosságokról.
Ezt a folyamatot kívánja segíteni Magyarországon a 2013 – tól független portálként működő Isidor Kft, amely elsősorban információbiztonsággal, szoftverfejlesztéssel, webes rendszerek kialakításával és üzemeltetésével foglalkozik. Minden egyes szolgáltatás esetében szem előtt tartja a mindenkori ügyféligényeket, és a legkorszerűbb technológiák alkalmazásával biztosít számukra informatikai megoldásokat. A vállalkozás szakemberei egy olyan Biztonsági Központot[41] fejlesztettek ki, ami vállalati és egyéni felhasználók számára olyan releváns információkkal szolgál, amelyek segítségével megvédhetik a rendszereiket a sebezhetőségek, a vírusok és az egyéb fenyegetettségek ellen.
Az Isidor munkatársai folyamatosan figyelemmel kísérik az informatikai cégek illetve a nemzetközi biztonsági központok, szervezetek által jelentett sérülékenységi adatokat, és a hazai felhasználók számára releváns információkat tesznek közzé. Jelenleg több mint 2700 termék biztonsági szempontból történő figyelését valósítják meg. Az ISBK ügyfelei között bankok, állami, közigazgatási és közoktatási intézmények, valamint kis –, közepes és nagyvállalatok is megtalálhatók.
Az Isidor közlése szerint: *„A Cisco[42] 13 országban, több mint 12.000 munkavállaló megkérdezésével végzett kutatása számos olyan biztonsági megközelítést támasztott alá, amelyek jelentős mértékben meghatározzák napjaink védelmi rendszereinek hatékonyságát. Így például beigazolódott, hogy a felhasználók, munkavállalók biztonságtudatosságán van még mit csiszolni, de a biztonsági szabályzatok is igencsak elhanyagoltak.*
A felmérés eredményeiből az olvasható ki, hogy a válaszadók 69 százaléka még a jelentősebb, sokat hangoztatott biztonsági résekkel, fenyegetésekkel sincs tisztában. Nyilvánvalóan a munkavállalóknak nem is kell minden technikai részletet ismerniük, de a sérülékenységekkel kapcsolatos alapvető ismeretek hiánya már komolyan befolyásolhatja a védelem hatékonyságát." [41]
Ebből leszűrhető, hogy a szervezetek vezetői a saját eredményességük érdekében inkább megkerülik a szabályokat, mert el akarják kerülni, hogy a biztonsági intézkedések visszafogják

[41] ISBK – Isidor Biztonsági Központ
[42] Az 1984-ben alapított Cisco Systems a hálózati gazdaság előfutára volt, amely mára a világ egyik legjelentősebb nemzetközi nagyvállalatává vált. Alapítói, a kaliforniai Stanford Egyetem tudósai, úttörő szerepet vállaltak az IP protokoll fejlesztésében, amely a belső hálózatokon, illetve az Interneten keresztül folytatott kommunikáció alapvető szabványa lett. A Cisco Systems IP alapú hálózati megoldásai biztosítják mind az Internet, mind a legtöbb nagyvállalat, felsőoktatási és kormányzati intézmény számára az adatkommunikációs kapcsolatot.

a munkavégzést. Ebben az esetben egyértelműen megmutatkozik a biztonságtudatosság hiánya. Az információbiztonság tudatos szervezet kialakításának alapvető feltétele, egyben lehetősége az oktatás, képzés. Az információbiztonság tudatosság és a kapcsolódó informatikai biztonsági képzési programok egyik legfontosabb célja a szervezetek egészséges működéséhez szükséges információbiztonsági és informatikai biztonsági biztosítékok helyes kialakítása és használata. Minden szervezetnek az igényeknek és a létező – valamint a tervezett biztosítékoknak megfelelő módon ki kell alakítania a saját információbiztonság tudatosság növelő és informatikai biztonsági képzési programjait. A képzéseknek tartalmi szempontból a szervezet belső szabályozói mellett az érvényes törvényi szabályozás rendelkezéseit is figyelembe kell venniük.
A biztonsági kultúra fejlesztését a következő lépésenként célszerű megtenni:

- A szervezeti biztonsági kultúra érettségének meghatározása;
- A vezetés által - a szervezetre vonatkozó elvárások figyelembe vételével – a biztonsági kultúra kívánatos érettségi szintjének a meghatározása;
- A biztonsági kultúra fejlesztési program kialakítása ki és elindítása,
- A szükséges szabályozások, intézkedések, oktatás lépésről lépésre történő megvalósítása;
- A program eredményességének rendszeres mérése. [42]

A szervezeti biztonsági kultúra érettségének felméréséhez segítséget nyújthatnak a következő szempontok:

- Mennyi és milyen súlyú a hiányosság;
- Biztonsági mulasztás történt-e a szervezetnél;
- Melyek voltak az ellenőrzések tapasztalatai.

A biztonságtudatosság fejlesztésének igénye a társadalom különböző szintjein működő szervezetek létrehozását vonta maga után.
A *kormányzati szintű szervezetek* közül szeretném kiemelni a 2015. októberben megalakult Nemzeti Kibervédelmi Intézetet (a továbbiakban: NKI), amely többek között fontos szerepet tölt be az állami – és önkormányzati szervek biztonságtudatosságának elősegítésében. Ez a szervezet oktatási anyagokat dolgoz ki és tréningeket tart, felvilágosító, szemléletformáló kampányokat szervez. Tekintettel arra, hogy az adatvédelem minden felhasználó alapvető érdeke, ezért az NKI az állami kibervédelem támogatásán, fenntartásán és fokozottabb működtetésén túl az egyéni felhasználók tudatosítására is egyre nagyobb hangsúlyt kíván helyezni. Az NKI célja, hogy a weboldalán – különböző témakör szerinti bontásban – található anyagok és tájékoztatók

segítségével, könnyen megérthető formában, a lehető legtöbb hasznos információt jutassa el látogatói részére.

Jelentős szerepet tölt be a biztonságtudatosítás terén a Belügyminisztérium felügyelete alá tartozó Nemzeti Elektronikus Információbiztonsági Hatóság (a továbbiakban: NEIH). A NEIH részt vesz az Nemzeti Kiberbiztonsági Koordinációs Tanács munkacsoportjainak munkájában, különösen a felhasználói tudatosításban, amivel többek között a közoktatás szereplőit szeretné megszólítani, összegyűjtve a kapcsolódó, korábban kidolgozott tananyagokat.

2013. április 15-én az Országgyűlés elfogadta az állami és önkormányzati szervezetek elektronikus információbiztonságáról szóló 2013. évi L. törvényt, amely létrehozta a Kormányzati Eseménykezelő Központot (GovCERT[43] – Hungary), mint a magyar kormányzat információ – megosztó és incidens – kezelő szervezetét. A GovCERT mellett szükségesnek tartom megemlíteni a Katonai Nemzetbiztonsági Szolgálathoz tartozó MilCERT – et (katonai CERT Központ), amely jelenleg kialakítás alatt van. A két szervezet szorosan együttműködik, szakmai téren kölcsönösen segítik egymást.

A *társadalmi szervezetek* inkább társadalmi szinten és oktatási intézményekben aktívak, a *szakmai szervezetek* pedig részt vesznek a társadalmi biztonságtudatosításban, de főként a közigazgatási szervezetek és gazdasági társaságok biztonsági kultúrájának fejlesztéséhez járulnak hozzá. Ők gondoskodnak a tudatosítást végző szakemberek felkészítéséről, meghatározzák a tudatosítás módszereit, és biztosítják a szükséges segédeszközöket. Két népszerű szervezetet szeretnék kiemelni: az ISACA[44] Magyarország Egyesületet és a KIBEV[45] szervezetet.

A társadalmi szervezetek ugyancsak jelentős képviselője az Informatikai Távközlési és Elektronikai Vállalkozások Szövetsége (IVSZ), amely a „digitális tér” időszerű kérdéseivel és digitális oktatási stratégia létrehozásával is foglalkozik.

A *gazdasági társaságok* egy része a saját szervezetén belüli biztonságtudatosításon túl társadalmi szinten is végez tudatosítást. Ilyenek például a távközlési szolgáltatók, akik a szolgáltatásbiztonság növelése, és a társadalmi felelősségvállalás céljából segítik az információbiztonság tudatosítását[46].

A biztonság tudatosítása különféle módon valósulhat meg. A hagyományos iskolai oktatáson és szervezeten belüli képzéseken túl, tájékoztató brosúrák terjesztésén kívül közösségi ismertető

[43] Számítógépes Vészhelyzeti Reagáló Csoportok – Computer Emergency Response Team
[44] Információs rendszer menedzserek és ellenőrök nemzetközi szakmai szervezete (Information Systems Audit and Control Association)
[45] Önkéntes Kibervédelmi Összefogás.
[46] Pl. UPC reklámok

programok, hírlevelek szétküldése, közösségi hálózaton lévő információs csatornák igénybevételével, valamint tájékoztató honlapok létrehozásával is széleskörűvé, sokoldalúbbá tehető a tájékoztatás. A tájékoztatásnak ezek a lehetőségei gyakran sablonosak, szokványosak, túl általánosak, ezért a szakemberek folyamatosan próbálkoznak olyan lehetőségek kidolgozásával, amelyek a felhasználókat motiválják, aktivitásukat növelik. Erről Oroszi Eszter Diána beszélt a Magyar Villamos Művek által 2017–ben megrendezett konferencián. Bemutatott egy olyan – biztonságtudatosságot fejlesztő – lehetőséget, amely a felhasználók aktív bevonásával történik. A résztvevők a támadó bőrébe bújva próbálnak a felhasználó gépéhez hozzájutni, adatokat megszerezni. A „biztonságtudatossági szabaduló szoba" néven ismertté vált játék kipróbálásának tapasztalatai a következők: a résztvevők aktívak, sok esetben saját mulasztásaikat is felfedezik, szívesen megismételnék a részvételt, és elégedetten távoznak. Az utóbbi években egyre népszerűbbé váltak a szakmai konferenciák, ahol az aktuális problémák és időszerű kérdések is felvetődnek, így olyan fontos tapasztalatra is szert tehet a résztvevő, ami a saját szervezeténél nem fordult elő, de annak ismerete a biztonságtudatosság szempontjából fontos lehet.

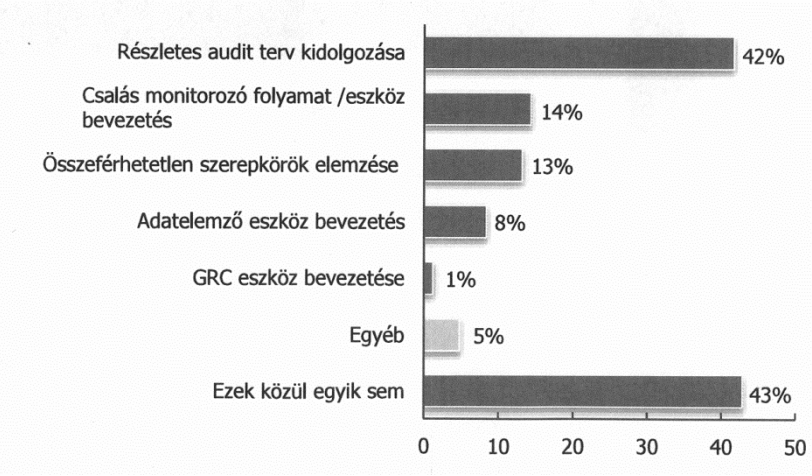
Végül, de nem utolsó sorban említést érdemel az ellenőrzés és szankcionálás, mint a biztonságtudatosítást segítő eszköz. A szankcionálás azért fontos a biztonság terén, mert ez eszköz lehet azok számára, akiket az oktatás és egyéb motivációs módszerek sem képesek rávenni arra, hogy az elvárt módon végezzék munkájukat. A szankciók alkalmazása során azonban ügyelni kell arra, hogy mindig az incidensek súlyával legyenek arányosak. Szeretném egy aktuális példával bemutatni, hogy az arányosságot és fokozatosságot hogyan lehet a gyakorlatban eredményesen megvalósítani:

Az egyik NATO haderőnemi parancsnokság direktívájában a törzsfőnök 3 lépcsős incidens kezelő szabályozást vezetett be. Az 1. incidens alkalmával a szabályok ellen vétett személy figyelmeztetést kap, felhívják az elkövető figyelmét biztonsági felelősségére. Egy éven belül történt 2. biztonsági incidens esetén egy magasabb szintű parancsnok szankcionálja az esetet.

Ugyanazon éven belüli 3. incidens esetén az illetékes parancsnok a vétkes személy biztonsági kártyájának jogosultságait visszavonja, ezáltal az incidenst elkövető nem képes bejutni a védett területre. Ennek a következménye az, hogy az adott munkakörből felmentik. Erre a gyakorlatban már sor került az elmúlt években. Ez a szabályozás egyrészt toleráns a vétkessel szemben, másrészt nem tart olyan személyt alkalmasnak biztonsági munkakörre, aki sorozatosan vét az előírások ellen.

4.4 A biztonságtudatosság és a vezetés, irányítás összefüggései

Az információbiztonság szempontjából különösen fontos a szervezeti kultúra, hiszen a szervezet általános információbiztonsága valójában annak tagjain, az egyéneken, továbbá azok aktuális viselkedésén múlik. A szervezet dolgozóinak tudatos információbiztonsági magatartását – a megfelelő képzés mellett – leginkább a felsővezetői elkötelezettség és tudatosság befolyásolja pozitív irányban, melyet a dolgozóknak meg is kell tapasztalniuk. Vezetői elfogadás, akarat, támogatás nélkül nem lehetséges rendszert kiépíteni, és biztonságosan, felelősségteljesen működtetni. Az ISACA által 2015 tavaszán elvégzett felmérés célcsoportja a releváns magyar vállalatok és intézmények voltak. A vizsgálat szerint a vezetők az információbiztonságot nagyon fontosnak tartják, de a biztonság megszilárdítására tett lépések gyakran elmaradnak, vagy csak részben valósulnak meg [43]. A felmérés alapján az év legfontosabb IT audit kezdeményezései a következők voltak:



13. sz. ábra[47]: *Információbiztonsági helyzetkép (2015 ISACA)*

Hasonló eredményt mutatott ki a PTA CERT[48] is 2012-ben. *„A magyarországi nagyvállalatok a nemzetközi átlaghoz hasonló arányban alkalmaznak átfogó stratégiát, illetve az egyes részterületekhez kapcsolódó biztonsági terveket, azonban a konkrét megvalósítás bizonyos esetekben még elmarad ettől a szinttől. Átfogó információbiztonsági stratégiája a vállalatok 61%-ának van (az ISACA tanulmánya1 szerint ez világszerte átlagosan 65%), míg például sérülékenység elemző eszközökkel csak egynegyedük rendelkezik, szemben a nemzetközi szinten átlagosan 53%-os aránnyal."* [44]

[47] A GRC (irányítás-, kockázat- és megfelelés-menedzsment) egy integrált megközelítés a vállalati kockázatok kezelésére. Bár külön entitások, de a GRC komponensei együtt alkotnak egy átfogó módszert, mely biztosítja az üzleti működés fenntarthatóságát.
[48] PTA CERT: Hungary Nemzeti Hálózatbiztonsági Központ

A jelentésekből az is kiderül, hogy a belső ellenőrzések során vizsgált informatikai biztonság fejlesztésére is nagyobb figyelmet kell fordítani

A Ponemon Institute 2015-ben készített felmérést Global Cyber Impact Report néven [45], melynek eredményeit 37 országban több mint 2200 szakember megkérdezésével szűrték le. A kutatásából kiderül, hogy a válaszadóknak mindössze negyede van teljes mértékben tisztában a kibertámadások lehetséges pénzügyi és jogi következményeivel, míg ötödük egyáltalán nem látja át ezeket, amellett, hogy a válaszadó cégek 37 százalékánál már léptek fel adatvesztéssel vagy adatkárosodással járó anomáliák.

A kutatások szerint nincs túl kicsi célpont, nincs túl kis cég, ahol ne lenne szükséges a védekezésre koncentrálni.

Ezt igazolja a Symantec [46] elemzése, mely szerint a támadások megközelítőleg felét olyan vállalatok szenvedték el, ahol 2500-nál kevesebb alkalmazott dolgozik, további 18%-uk pedig 250 alkalmazottnál is kevesebbet foglalkoztató vállalkozás volt. Folyamatos a verseny a hackerek és a biztonságot védő cégek között. A támadó sok esetben egy lépéssel előbbre jár, ugyanis neki van ideje felkészülni a támadásra, miközben a céget váratlanul éri az esemény.

A 4. fejezet 4. pontjának elején már utaltam arra, hogy egy szervezet nem válhat biztonságtudatossá anélkül, hogy a szervezet vezetője, a szervezet vezetése ne lenne biztonságtudatos. Amennyiben egy vezető nem eléggé biztonságtudatos, ez esetben az általa irányított szervezet sem lehet az. Nagyon fontosnak tartom emellett a személyes példamutatást: ha a vezető és a vezető beosztású elöljárók biztonságtudatosságot árasztanak, ennek hatására nagy valószínűséggel a beosztott állomány is hasonlóan fog viselkedni. Véleményem szerint elengedhetetlen az is, hogy egy szervezet vezetője (vezetősége) kommunikálja a dolgozók felé, hogy számára a biztonságtudatosság mit jelent, és azt is, hogy milyen elvárásai vannak ezzel kapcsolatban a beosztottakkal szemben.

A szakemberek az MSZ ISO/IEC 27001:2014 szabvány kidolgozásával olyan egységes rendszert hoztak létre, amely a korábbi szabványok hiányosságait is pótolta. A felülvizsgálatkor a szabvány kidolgozói a tartalomra vonatkozó felhasználói vélemények beillesztésére is törekedtek, valamint a különböző irányítási rendszerek integrációjának megkönnyítését is szem előtt tartották. Ezért az új szabvány a felépítés egységesítése révén a több irányítási rendszert is működtető szervezetek számára jelenti a legnagyobb előnyt.

Azoknak a vállalati vezetőknek, akiknél az MSZ ISO/IEC 27001:2014 bevezetésre került, rendelkezniük kell azokkal az alapismeretekkel, amelyek alapján biztonságtudatosabbá válhatnak.

Az Óbudai Egyetem képzési rendszerében található az információbiztonsági szakmérnöki szakirányú 2 éves levelező képzés, melyet minden olyan középvezető részére ajánlott elvégezni, aki állami szférában információbiztonság témakörrel foglalkozik. Ez a képzés segítséget nyújt felső – és középvezetőknek ahhoz, hogy szervezetükben az információbiztonsági kultúra szintjét minél magasabb színvonalúra legyenek képesek emelni.

Az ISACA készített egy nemzetközi felmérést arra vonatkozólag, vajon milyen biztonságirányítási követelmények írhatóak elő, amelyeket a szervezeteknek figyelembe kell venni az információbiztonsági irányítás során. Ez alapján az alábbi követelményeknek kell megfelelni:

A szervezeteknek olyan információbiztonsági irányítási keretrendszert, működési folyamatot kell létrehozni és szinten tartani, amely biztosítja az összhangot az információbiztonsági stratégia,[49] a szervezet céljai, feladatai, a szervezetet érintő kockázatok és a stratégia megvalósításához szükséges, rendelkezésre álló források között. A keretrendszer kialakítása során az információs rendszereket veszélyeztető kockázatokat a jogszabályok által előírt módon kell kezelni.

Figyelmet kell fordítani arra is, hogy a szervezet információbiztonsági szabványai, eljárásai, útmutatói és más dokumentumai az információbiztonsági politikának megfelelően legyenek kialakítva.

Az alábbi leírás jól szemlélteti, hogy az információbiztonsági irányítási rendszer és információbiztonsági politika milyen sokrétű és összetett.

Információbiztonsági irányítási rendszer. Információbiztonsági politika: [47]

1. Információbiztonsági stratégia.
    - Jelen állapot felmérése;
    - Célok meghatározása (kívánt állapot leírása);
    - Védelmi intézkedések és kontrollok;
    - Szükséges erőforrások;
2. Információbiztonság irányítása.
    - Irányítási szervezet;
    - Működtetés irányítása;

[49] A stratégia a célok meghatározásának és megvalósításának eszköze. Általában hosszabb távú terv a szervezeti célok elérésének megvalósításához. Fogalma alatt a szervezeti, üzleti vagy funkcionális célok, és az azok eléréséhez szükséges erőforrások (humán erőforrások, eljárások, eszközök) meghatározását, rendelkezésre állásának, illetve összehangolt működésének biztosítását is értjük.
Oroszi Eszter Diána: Információbiztonsági stratégia és vezetés NKE Budapest 2014 p.16.

- Ellenőrzés, monitorozás;
- Teljesítmény értékelés, visszamérés.

A program kidolgozása során arra is figyelmet kell fordítani. hogy egy esetleges biztonsági esemény bekövetkezése alkalmával minél kisebb kár érje az adott szervezetet. Ezért az információbiztonsági irányítási rendszer és információbiztonsági politika kialakítása során külön figyelmet kell fordítani a rendkívüli eseményekre való felkészülésre, a folyamatos reagáló képesség biztosítására. Ennek érdekében akciótervet szükséges készíteni az információbiztonsági események azonosítására, kivizsgálásukra, a problémára megoldására, valamint az eredeti rend helyreállítására. Az akcióterv elkészítése és naprakészen tartása nélkül egy szervezet nem képes hatékonyan reagálni a váratlanul bekövetkezett biztonsági eseményre. Időszakonként tesztelni kell, és felül kell vizsgálni a rendkívüli eseménykezelési tervet azért, hogy az információbiztonsági rendkívüli eseményekre eredményes választ adhassunk és javítsuk a reagálási képességet. A rendkívüli események elhárítását követően felülvizsgálatot kell tartani, mely során meg kell határozni az információbiztonsági rendkívüli események bekövetkeztének okát, a probléma megoldására megtett intézkedéseket, majd az aktuális kockázatok felmérése után értékelni kell az elhárítás eredményességét, és szükség esetén megfelelő helyesbítő intézkedéseket kell hozni. Rendkívül fontos tehát, hogy egy szervezet vezetője megértse az információbiztonsági irányítási rendszer és információbiztonsági politika alkalmazásának szükségességét, emellett felismerje azt, hogy ez egy folyamatos, állandó fejlesztéssel és tökéletesítéssel járó folyamat.

Ennek a tevékenységnek támogatója lehet a szervezet biztonsági vezetője, valamint a vezetőség többi tagja, akik számára a biztonságtudatosság igénye egyfajta „belső késztetés” kell, hogy legyen. Természetesen a biztonságtudatosság nem a vezetők veleszületett tulajdonsága, tanulni, fejleszteni kell.

4.5 Kérdőív biztonsági vezetők részére

A szervezeti vezetés és az információbiztonsági tudatosság összefüggéseinek megfigyeléséhez egy kérdőívet állítottam össze katonai alakulatok biztonsági vezetői részére. A kérdőívet azzal a céllal dolgoztam ki, hogy:

- Informálódjak a katonai szervezetek információbiztonság tudatosságának szintjéről, ezáltal képet kapjak az információbiztonsági kultúra jelenlegi szintjéről az MH – ban;

- Felmérjem, hogy milyen információbiztonsági hiányosságok fordulnak elő az alakulatoknál, és milyen mértékben játszik szerepet az emberi tényező a biztonsági vezetők tapasztalata szerint;
- Képet kapjak arról, milyen problémákkal kell szembe nézniük a biztonsági vezetőknek az információbiztonság részterületei tekintetében;
- Tájékozódjak arról, hogy a biztonsági vezetők milyen úton próbálják növelni a biztonsági kultúra szintjét szervezetükben;
- Milyen szankciókat illetve jutalmazási módszereket alkalmaznak az előírások betartatása érdekében;
- Mennyire tartják fontosnak munkatársaik oktatását, szakmai képzését, valamint saját maguk fejlődését?

A kitöltött kérdőívek eredményeit arra használtam fel, hogy kiinduló adatokat kapjak a felmerülő problémákról, a katonai alakulatok biztonságtudatosságáról. A válaszok alapján megállapítom, hogy előző feltevésemmel megegyezően szinte minden esetben emberi tényező okozza az információbiztonsági incidenseket a katonai szervezeteknél. Jellemző az, hogy a jogszabályokat és az előírásokat ismerik, de sok esetben nem tartják be. A szervezetlen munkavégzés ugyancsak gyengíti az információbiztonságot. A biztonsági vezetők ennek okait a hanyagságra, könnyelműségre, kényelemre vezetik vissza. Sokszor jelent problémát, hogy bár az előírásokat betartják, de pontatlanul és felületesen teszik azt.

A felmérés szerint az is jellemző az emberi mulasztásokra, hogy az előírt határidőket nem tartják be[50], de az is gyakran előfordul, hogy a minősített adatot felületesen kezelik.

A fizikai biztonság megvalósítása terén legtöbb nehézség az engedélyeztetések előkészítése és lebonyolítása terén adódik[51]. Az alakulatoknak – az anyagi erőforrások hiányában – korlátozottak a lehetőségeik, viszont a törvényi szabályozás olyan előírásokat támaszt, melyek megvalósítása állandó kihívást jelent.

Előfordul, hogy a nyilvántartások pontatlanok, hiányosak, ezért a válaszadók többsége fontosnak tartja az adminisztratív biztonságra történő nagyobb odafigyelést. A minősített adatkezelő rendszerek dokumentációira az eddiginél több figyelmet kell fordítani.

Az információbiztonsági munkakörökre való alkalmasság megítélésére a válaszadók a személyes elbeszélgetést, a szakmai ismeretek felmérését és a mások általi ajánlást tartották hasznosnak.

[50] Például nem váltanak jelszót az előírásoknak megfelelően
[51] Adatkezelési engedély, Rendszerengedély

A kérdőívekben leírtak alapján megállapítom: a katonai szervezetek biztonsági vezetői megfelelő figyelmet fordítanak arra, hogy hogy a szabályzókban lefektetett elvárások megvalósuljanak, betartásra kerüljenek. **A válaszok alapján a biztonsági kultúra tudatos fejlesztése és a biztonságtudatosság erősítése a jelenleginél nagyobb figyelmet kellene, hogy kapjon az MH minden alakulatánál.**

Összegzés

Ebben a fejezetben az információbiztonsági kultúra kialakításának és növelésének lehetőségeit kutattam. Megállapítottam, hogy **az információbiztonsági kultúra fejlesztése nem lehetséges szervezett irányítás, valamint tudatos, lépcsőzetes és folyamatos fejlesztés nélkül.** Megvizsgáltam az információbiztonsági irányítási rendszer működését, rendszereztem az információbiztonság tudatosság fejlesztésének társadalmi szinten működő szervezeteit. Megállapítom, hogy **megfelelő szintű képzés és oktatás nélkül az információbiztonság-tudatosság nem alakítható és fejleszthető.**

5. AZ OKTATÁS SZEREPE AZ INFORMÁCIÓBIZTONSÁGI KULTÚRA KIALAKÍTÁSÁNAK ÉS FEJLESZTÉSÉNEK FOLYAMATÁBAN

Bevezetés

A 4. fejezetben tanulmányoztam azt, hogy a biztonsági kultúra fejlesztése és a biztonságtudatosság erősítése az utóbbi években nagy hangsúlyt kapott társadalmunkban. Ebben a folyamatban kiemelt szerepet tölt be az oktatás, ezért az oktatást méltón nevezik a biztonságtudatosság alappillérének. Ebben a fejezetben az oktatás és a biztonságtudatosság kapcsolatát elemzem, emellett nagy hangsúlyt fektetek a Magyar Honvédség információbiztonsági képzésének vizsgálatára.

5.1 Az oktatás, képzés jelentősége a belső információbiztonsági szervezeti kultúra kialakításában

Sik Zoltán Nándor: Elektronikus információbiztonság és közigazgatás című előadásában [48] kihangsúlyozza, hogy a biztonsági kultúra kialakítása és fejlesztése nem szervezeti szintű feladat, hanem társadalmi ügy, vagyis fontos az egész társadalom biztonságtudatosságának megalapozása és folyamatos fejlesztése. A megalapozáshoz a családok, szülők és az oktatási intézmények is hozzájárulhatnak azáltal, hogy már a gyermekkor korai szakaszában biztonságtudatosságra szocializálják a gyermekeket. Ez az iskolákban a Nemzeti Alaptantervbe való beépítéssel még könnyebben kivitelezhető lenne.

A biztonsági kultúra társadalmi szintű szerepét kívánja hangsúlyozni számos kezdeményezés: például a Nemzeti Közszolgálati Egyetemen 2016. október 27-én– az Európai Kiberbiztonsági Hónap keretében – megrendezett workshop, melynek témája Magyarország digitális gyermekvédelmi stratégiája és az információbiztonság szerepe volt. Ennek keretében számos - a kiberbiztonságra fókuszáló - előadást, konferenciát, szakmai kerekasztal beszélgetést szerveztek az IT tudatosság, az adatvédelem, online fenyegetések megelőzésének érdekében.

Rajnai Zoltán, Magyarország kiberkoordinátora a rendezvényen arról beszélt, hogy kiemelt feladatnak tartja, hogy a kormányzat foglalkozzon a digitális eszközöket használó gyermekek védelmével is.

Az oktatást már az óvodától el kell kezdeni, a digitális tudatosság pedig csak az élethosszig tartó tanulással érhető el. A pedagógusokat és a szülőket is egyaránt fel kell készíteni, hiszen manapság sokszor a gyerekek digitálisan sokkal előrébb járnak, mint maguk a felnőtt felhasználók, vagy az iskolában tanított tananyag. Rajnai Zoltán úgy véli, hogy a problémákat a szülők és a gyerekek egyaránt érzik, ezek megoldása össztársadalmi érdek. Az információbiztonsági tudatossági

stratégia után meg fog élénkülni a témával foglalkozó szervezetek tevékenysége, a gyermekvédelem szempontjából pedig ez az első lépés a kormányzat, a szolgáltatók és a felhasználók számára a digitális bűncselekmények elleni fellépésben. Rajnai Zoltán úgy fogalmazott*: „A stratégia egy olyan csontvázat ad, amit majd fel lehet öltöztetni."*

Az információbiztonsági kultúra kialakításának és fejlesztésének fontosságát – mint arra már korábban is utaltam – elméletben felismerték a szervezetek vezetői, de kevés gyakorlati lépést tettek a megvalósítás érdekében. Mindezt gátolja a területre fordítható pénzügyi forrás hiánya. Előzőleg szó esett arról is, hogy a humán faktornak hangsúlyos szerepe van a biztonság megteremtésében, ugyanakkor az ember potenciális veszélyforrása is lehet az információk kiszivárgásának. A felhasználók felkészületlensége vagy hiányos felkészültsége veszélybe sodorhatja az információ biztonságát, ezt azonban kellő színvonalú felkészítéssel orvosolni lehet, szerencsésebb esetben pedig meg lehet előzni.

Információbiztonsági képzéseken, konferenciákon és más számos, a témával kapcsolatos fórumon gyakran elhangzanak a következő mondatok:

„A biztonság megteremtője és fenntartója maga az ember.", „A biztonság rajtad múlik!" Ezek a mondatok felhívják figyelmünket arra, hogy az „emberi tűzfal, vagyis a munkatársak tudatos viselkedése az, amelynek kialakítása és folyamatos fejlesztése a legfontosabb, legjobban megtérülő befektetés." [49]

Ahhoz, hogy az emberek, akik az „emberi tűzfalat" alkotják, szerepüket be tudják tölteni, és biztonságtudatosan, minőségi munkát legyenek képesek végezni, ***megtervezett, színvonalas képzésben kell, hogy részesüljenek.***

Felmerül a kérdés, vajon milyen legyen az a képzés, amely támogatni tudja az információbiztonság megvalósulását, az információbiztonsági kultúra színvonalának fejlesztését?

Ez olyan szakmai képzések formájában lenne megvalósítható, melyek tartalmazzák a már használatos, és az újonnan üzembe helyezett rendszerek hatékony és biztonságos üzemeltetését célzó intézkedéseket, munkafolyamatokat, gyakorlati útmutatókat. Emellett szükség lenne információbiztonság – tudatosság képzésekre, amelyek képesek a szervezet munkatársainak figyelmét felhívni a releváns fenyegető tényezőkre. A megfelelő oktatással tudatosítani kell bennük a szükséges viselkedési formákat a megelőzés és felismerés érdekében.

Az információbiztonság-tudatosság fejlesztése céljából a Nemzeti Közszolgálati Egyetem kiadott egy segédanyagot, amely információbiztonság - tudatosság képzési programot ajánl a szakma számára. A kidolgozók olyan többszintű képzési útmutatót hoztak létre, melynek mottója: *„Tegyük a jövőt együtt biztonságosabbá."* [50]

A szerzők elgondolása szerint a program *teljes körűen*, valamint *hosszú távon* képes fejleszteni a szervezet információbiztonsági szintjét, illetve felhasználóinak információbiztonság-tudatosságát.

Az 5+1szint az alábbiakat foglalja magában:

1. szint: Általános felhasználói szint;

2. szint: Kiemelt felhasználói jogokkal rendelkező vezetők, felsővezetők tudatosítása;

3. szint: Szakértői képzés – „system hardening", sérülékenység menedzsment - üzemeltetők számára;

4. szint: Szakértői képzés – a biztonságos fejlesztés végrehajtóinak;

5. szint: Az informatikai biztonság kialakításáért felelős személyzet információbiztonság tudatosság képzése;

5+1. szint: Szervezeten belüli információbiztonsági tudatosítást végző szakértői oktató csoport kialakítása – „train the trainer" koncepció.

5.2 A Magyar Honvédség információbiztonsági oktatási, képzési rendszere

A Magyar Honvédség információbiztonsági oktatását a Honvéd Vezérkar Személyzeti Csoportfőnökség (a továbbiakban HVK SZCSF) és a HVK HIICSF felügyeli. Előbbi az oktatás, képzés szervezését[52] látja el, utóbbi pedig a képzés szakmai felügyeletéért felelős.

Az információbiztonsági oktatást a HVK HIICSF felkérésére a Nemzeti Közszolgálati Egyetem hajtja végre a saját képzési rendszerében.

Az NKE szabályozza az elektronikus információs rendszer biztonságáért felelős személyek képzési, továbbképzési tematikáját, oktatási programját, melyhez a HVK HIICSF nyújt iránymutatást azáltal, hogy kidolgozza a biztonságért felelős személy meghatározott képzettségi követelményeit. A képzési rendszerrel szemben felállított követelmények pontos meghatározása azért is szükséges, hogy naprakész, előrelátó oktatást tudjon tervezni az oktatási intézmény. A képzéssel szemben támasztott követelmények felállításakor pontosan definiálni kell azokat az ismereteket és képességeket, amelyek elsajátítását és megszerzését a megrendelő szükségesnek tart. Ez esetben a HVK HIICSF és az NKE Híradó Tanszék közötti rendszeres együttműködés elengedhetetlen.

Az NKE által kidolgozott tematikák alapján az információbiztonsági képzések az NKE Hadtudományi és Honvédtisztképző Kar Híradó Tanszék akkreditált (adatkezelési engedéllyel rendelkező) tantermeiben kerülnek lebonyolításra.

[52] Beiskolázás megtervezése, megvalósítása, képzettségek nyomon követése, képzettségi hiányosságok számon tartása.

A Híradó Tanszéken folyó képzési formák a következők:

Elsőként a Híradó Tanszék **Katonai üzemeltetés alapképzési szakán** (BSc képzés) választható **katonai információbiztonsági modult** ismertetem. Az alapszakon tanuló hallgatók a 6., 7., 8. szemeszterben tanulják az információbiztonsággal kapcsolatos ismereteket.

A katonai információbiztonsági specializáció követelményeit az alábbi leírás tartalmazza:

„A végzett hallgató legyen képes: [51]

- *a Magyar Honvédség adatkezelő rendszereit érintő kérdésekben az információbiztonság teljes körű képviseletére;*
- *kezelni az állandó telepítésű adatkezelő nemzeti és külföldi nyílt, nem nyilvános, minősített elektronikus adatokat feldolgozó rendszerek tervezésével, létrehozásával, üzemeltetésével, fenntartásával, megszüntetésével kapcsolatos szakmai kérdéseket;*
- *a gyakorlatok, konferenciák és egyéb rendezvények rendszereinek tervezésére, fejlesztésére, beszerzésére, tesztelésére, üzembe helyezésére, üzemeltetésére, illetve megszüntetésére;*
- *az elektronikus adatkezelő rendszer személyi, fizikai, adminisztratív biztonsági követelményeinek megvalósítására;*
- *az adatkezelő rendszerek biztonsági követelményeinek és az ezek megvalósítására irányuló rendszabályok meghatározására;*
- *a szervezet, illetve rendszer specifikus biztonsági szabályzatok kidolgozására, kidolgoztatására;*
- *a rendszerek hatósági akkreditálásával, auditálásával és egyéb hivatalos ügyintézéssel kapcsolatos feladatok végzésére;*
- *szervezetek közötti együttműködés szervezésére, szabályozására, a külső ügyfelekkel, harmadik fél hozzáférésével kapcsolatos biztonsági kérdések megoldására, valamint információvédelmi feladatok összehangolására;*
- *a nemzeti és a külföldi nyílt, nem nyilvános, minősített elektronikus adatkezelő rendszerek biztonságát javító intézkedésekre, azok végrehajtására, kockázatarányos biztonsági eljárások kidolgozására javaslatot tenni;*
- *elektronikus adatokat feldolgozó rendszerek kockázatelemzésének végzésére, dokumentálására;*
- *a minősített elektronikus adatkezelő rendszer, TEMPEST felelős feladatainak végzésére; rendszer biztonsági ellenőrzésére, a tapasztalatok kiértékelésére; a biztonsági incidensek kezelésére; szervezetek szakmai tevékenységének irányítására, támogatására;*

- *az elektronikus biztonsági feladatokat ellátó személyek részére a szakmai képzés tervezésére, szervezésére, valamint szakmai továbbképzések, felkészítések megtartására;*
- *a rejtjelző rendszerek tervezése folyamatának átlátására, a különböző rendszerelemekből hálózati struktúra kialakítására;*
- *a rejtjelző eszközök üzemben tartásának koordinálására, az időszakos tervek és jelentések kidolgozására;*
- *az elsajátított rejtjelzéssel összefüggő szabályzók értelmezésére, a felmerült problémák esetén a szabályozók alkalmazására;*
- *a rejtjeltevékenységgel összefüggő dokumentum elkészítésére, naprakészen tartására;*
- *javaslatot tenni a NATO, az EU, a nemzeti nem nyilvános, minősített rendszerek védelmét biztosító rejtjelző eszközök biztonságát javító intézkedésekre és jóváhagyás után azok végrehajtására;*
- *megfelelő szakmai gyakorlat megszerzését követően a nemzetközi szervezetekben feladatok végrehajtására;"*

2006-tól mesterképzésben is lehetőség nyílt az információbiztonsági ismeretek magasabb szintű elsajátítására MSc *Védelmi, vezetéstechnikai rendszertervező szakon*. Ez a szak jelenleg szünetel, helyette MSc *Katonai üzemeltetés mesterképzési szak* elvégzésére nyílt lehetőség, amely 2 félév időtartamú. [52]

Összességében az információbiztonsági felsőoktatási képzés egy új, innovatív képzési eljárás, amely lehetőséget ad arra, hogy olyan magasan képzett szakemberek kerüljenek a szakterületre, akik képesek arra, hogy bonyolult biztonságtechnikai védelmi rendszereket működtetni tudjanak, fel tudják venni a versenyt a rendszerek ellen felmerülő kihívásokkal.

Információbiztonsági tanfolyamok

A biztonságtudománynak alkalmazkodnia kell korunk számítástechnikai, technológiai fejlődéséhez, ezért elengedhetetlenül szükség van a korábban beosztásba helyezett állomány szakmai képzésére, továbbképzésére. Ezt a lehetőséget is az NKE Híradó Tanszék biztosítja.

Az elektronikus információbiztonsági tanfolyamokat félévenként – általában egy alkalommal – rendezi meg a Híradó Tanszék. A felelősségi körök és eszközök figyelembevételével az alábbi tanfolyamok nyújtanak új ismereteket a beiskolázottak számára:

- Információbiztonság menedzselése tanfolyam
  Tanfolyami tematika: [53]

- Rendszeradminisztrátor tanfolyam
  Tanfolyami tematika: [54]
- Rendszerbiztonsági felügyelő tanfolyam
  Tanfolyami tematika: [55]
- Kockázatelemzés tanfolyam
  Tanfolyami tematika: [56]
- TEMPEST[53] tanfolyam
  Tanfolyami tematika: [57]
- Rejtjelző alaptanfolyam
  Tanfolyami tematika: [58]
- Rejtjelző ismeret kiegészítő tanfolyam
  Tanfolyami tematika: [59]
- Információvédelmi eszközkezelő tanfolyam (EKMS, TCE, stb.)
  Tanfolyami tematika: [60]

A tanfolyamok egy része alaptanfolyam, amelyek elvégzése ma már kötelező ahhoz, hogy egy személyt beosztásba helyezzenek. Ilyen a rejtjelző alaptanfolyam.
Vannak olyan képzések is, amelyek elvégzése és a sikeres vizsga letétele nem feltétele annak, hogy a beosztásába kerülő személy megkezdhesse munkatevékenységét. Ezek a munkavállalók később kerülnek tanfolyami beiskolázásra. Ide tartozik a rendszeradminisztrátori vagy a rendszerbiztonsági felügyelő képzés.
A 36 órás rejtjelző, a kockázatelemzés, valamint a TEMPEST tanfolyamok lehetőséget nyújtanak a parancsnokok számára, hogy az információbiztonság területén bekövetkezett, vagy a közeljövőben bekövetkezendő jogszabályi változások, szakmai újítások elsajátítására iskolázzanak be tapasztalt, a szakmában már jártas szakembereket. Az ilyen jellegű tanfolyamok jó lehetőséget nyújtanak – többek között – a 2009. évi CLV. tv hatályba lépésével, az elektronikus adatkezelő rendszerek üzemeltetésével kapcsolatos változások, ÜBSZ változás, NATO elektronikus adatkezelő rendszerek ellenőrzésével kapcsolatos újdonságok, módosítások megismerésére.
Amint a tematikai leírás mutatja, a Híradó Tanszéknek arra is van módja, hogy egy akkreditált oktatási egységben[54] információvédelmi eszközkezelő tanfolyamokat bonyolítson le. Ezek a

[53] Elektronikai adatfeldolgozó egységek kisugárzásának elemzése
[54] NKE 41. épület 2,5. emelet, amely minősített adatkezelési engedéllyel rendelkezik.

tanfolyamok elméleti és gyakorlati ismeretek elsajátítására is alkalmat nyújtanak. Az intézmény csak részben rendelkezik a képzések megtartásához szükséges eszközökkel, ezért a képzések idejére a Magyar Honvédség vitéz Szurmay Sándor Budapest Helyőrségi Dandár biztosítja a hiányzó technikai eszközöket.

A 2017/18. tanévben két új információbiztonsághoz kapcsolódó tanfolyam elindítását tervezte be az Informatikai Tanszék. Az *Informatikai biztonságtudatosság tanfolyam* mellett az *Informatikai incidenskezelés alapjai* tanfolyamok új lehetőséget nyújtanak a biztonsági kultúra szintjének növelésére az MH – ban.

5.3 Pszichológiai és didaktikai áttekintés a képzési követelmények felállításához és a tematikák kialakításához

Az előző pontban felsoroltam azokat az elektronikus információbiztonsági tanfolyamokat, amelyek tanfolyami tematikáit a mellékletek tartalmazzák. A tematikák bemutatják a feldolgozandó és az elsajátításra váró anyag tartalmi felépítését, a tananyag összetételét, valamint az elsajátításra rendelkezésre álló idő mennyiségét is.

Az oktatásban eltöltött 3 évtized tapasztalata, valamint pedagógiai, pszichológiai és didaktikai tanulmányaimra alapozva megállapítom, hogy az információbiztonsági képzés során a tanfolyamok nagy részénél, valamint a Katonai üzemeltetés alapképzési szakán esetében is a tanfolyamok anyagának mennyisége, és az elsajátításra szánt idő aránya nem megfelelő, ugyanakkor fontosnak tartom hangsúlyozni, hogy átfogó, sokrétű ismeretet próbálnak nyújtani ezek a tanfolyamok. Következtetésképpen levonható, hogy a tananyag mennyisége és nehézségi foka nincs megfelelő arányosságban a tanfolyamokra betervezett óraszámokkal és a lebonyolítási idővel.

Ezen túl további nehézséget okoz a tanfolyamok protokollja. Ez a gyakorlatban az alábbi módon valósul meg: a tanfolyami kurzusok egy vagy két hétig tartanak, a tanfolyamon részt vevő személyek napi 6 – 8 órában új ismereteket sajátítanak el, majd közvetlenül az utolsó tanítási nap utáni napon kerül sor a vizsgára. Felmerül annak a kockázata, hogy az amúgy is túlméretezett elsajátítandó anyagot a vizsgázó nem képes ilyen időkorlátok között a megfelelő szinten elmélyíteni. Ennek a feltevésemnek a tudományos alátámasztására szeretnék néhány egyszerű példát hozni a megismerő folyamatok pszichológiájából.

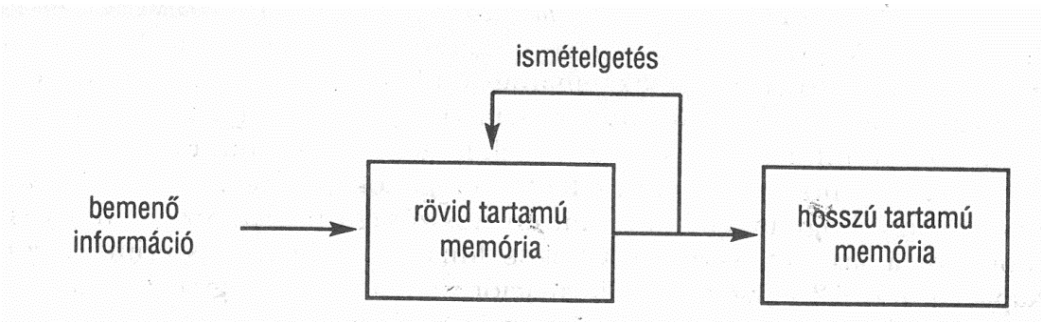
<u>Az emlékezet tároló modellje:</u> [61]

Az információfeldolgozás pszichológiai jellegű problémáinak kérdéseivel a II. Világháború után kezdtek el foglalkozni a szakemberek. Számos megfigyelést és kísérletet végeztek katonákkal a

munkavégzésük során, ugyanis igen sok probléma adódott azzal kapcsolatban, hogy a katonák a kapott információkat nem voltak képesek a megfelelő szinten feldolgozni. Az angol hadsereg vezetői a sorozatos hibákat nem fenyítéssel és büntetéssel torolták meg, hanem egy meglehetősen előremutató megoldást találtak: szakemberek bevonásával végeztek kísérleteket, hogy vajon mi megy végbe az emberben, amikor hatalmas mennyiségű információ áradat éri, vagyis az embert, mint *információ feldolgozó rendszert* kezdték vizsgálni. Az emberi információfeldolgozás kapacitásának határait kijelölni elsődleges problémává vált. Létrejött az *ergonómia*, amely az ember és gép kölcsönhatásait elemző alkalmazott pszichológia.

Az a képességünk, hogy hihetetlen mennyiségű információt tudunk elraktározni agyunkban annyira természetes, hogy az emlékezetünkkel csak akkor foglalkozunk, amikor nem jut eszünkbe egy szó, vagy nem tudunk felidézni valamit. Ilyenkor a memóriánkat tesszük felelőssé. De hogy is van ez valójában? Korai elméletek szerint a memória két részből áll: rövidtartalmú memóriából (a továbbiakban: RTM) és hosszútartalmú memóriából (a továbbiakban HTM). Az érzékszervekből bejövő információ először az RTM-be kerül.

Ezt a folyamatot szemlélteti az alábbi ábra: [62]



14. sz. ábra: *Az emlékezet társas modellje*

A kutatások azt bizonyítják, hogy az RTM időkapacitása korlátozott. Az RTM a befogadott információt csupán néhányszor tíz másodpercig tudja tárolni. Az RTM-ből való felejtés oka egyrészt az, hogy *az információ befogadásának kapacitása korlátozott*, másrészt, *az információ emléknyomai elhalványodnak, majd eltűnnek*. Az információ RTM-ben tartását elősegíti az ismétlés. Amikor az RTM információbefogadó képessége megtelik, az új információ csak úgy fér el, ha *korábbi információt töröl ki*. Arra a kérdésre, hogy mekkora az RTM kapacitása, George

Miller[55] [63] adott választ, miszerint az RTM kapacitása 7+/- 2 egység. Ez azt jelenti, hogy átlagosan 7 betűt, 7 szót vagy 7 számot tudunk egyszerre megjegyezni.

Az RTM-ben elegendő ideig tartott információ átíródik, beépül, bevéső dik a korlátlan kapacitású HTM-be. Itt az információ nagyon hosszú ideig képes tartózkodni, ezért lehetséges, hogy idős emberek nagyon jól vissza tudnak emlékezni gyermekkori élményeikre.

Az információ stabil beépülése a HTM-be azonban konszolidációs időszakot igényel. Ennek a konszolidációs periódusnak a hossza függ a megtanulandó anyag terjedelmétől és jellegétől. A konszolidációs folyamatot a túl korán érkezett újabb és újabb információk megjelenése megzavarhatja. Az is előfordulhat, hogy egy új tananyag megtanulása után újabbat tanulva a két anyag interferál [56]egymással, vagyis segítheti és gátolhatja is egymás felidézhetőségét. Ez alapján megfigyelhetjük a negatív interferencia jelenségét, amely során a később tanult tananyag gátolja a korábban megszerzett ismeretek konszolidációját. Ezt a jelenséget a pszichológia retroaktív gátlásnak hívja. Ennek fordítottja a proaktív gátlás, amely akkor következik be, amikor a korábban tanultak szorítják ki az emlékezetből a később tanultakat. *Annak érdekében, hogy ezt megelőzzük, érdemes a nagyon intenzív tanulás után szünetet és pihenést beiktatni, hogy az ismeret szilárdan be tudjon épülni a HTM-be.* **Amennyiben az információk nem rögzülnek kellőképpen, az ismétlés elmaradt, a kódolás nem volt megfelelő, valamint a jelentések között nem alakultak ki asszociatív[57] kapcsolatok, a megtanult anyag felejtése következik be.**

Didaktikai, vagyis az oktatás, tanítás oldaláról szeretném kiemelni, hogy az oktatás – képzés szempontjából nem csak a tananyag mennyiségére, és az elsajátításra szánt időre szükséges odafigyelni a tervezés során, hanem arra is, hogy milyen mennyiségű tananyagot, milyen összetételű résztvevőknek szeretnénk megtanítani Mindezek mellett hangsúlyt kell fektetni a ***cél – tartalom – módszerek*** hármas egységére is. Tervezéskor ki kell tűzni azokat a célokat, amelyeket a képzés során meg szeretnénk valósítani, majd a célokhoz kell igazítani a megfelelő tartalmat. Végül, de nem utolsó sorban meghatározzuk a legmegfelelőbb oktatási módszereket, amelyek egy kitűzött cél elérésének gyakorlati módjait határozzák meg. Mindezt annak érdekében szükséges megtenni, hogy az elsajátítás a lehető legsikeresebb legyen, a képzést a tervszerűség és hatékonyság jellemezze.

[55] George Armitage Miller pszichológus, legtöbbet idézett munkája a rövidtávú memóriához kapcsolódó "The Magical Number Seven, Plus or Minus Two", vagyis A bűvös hetes szám, plusz/mÍnusz kettő, ami a Psychological Review-ban jelent meg 1956-ban.

[56] kölcsönhatásba lép, kölcsönösen hat egymásra

[57] összekapcsoló, társító, egyesítő

Az oktatási folyamatban számos didaktikai feladatot kell megvalósítani, amelyek ciklikusan visszatérő tudatos tanári-tanulói tevékenységet jelentenek.

Ezek a következők: [64]

1. a figyelem felkeltése, tanulói motiváció;
2. informálás a célokról;
3. előzetes ismeretek felidézése;
4. az új ismeretekhez szükséges prezentációk elkészítése;
5. tények, jelenségek, folyamatok elemzése;
6. fogalomalkotás, következtetések levonása;
7. rendszerezés és rögzítés;
8. a tanultak alkalmazása;
9. a teljesítmények mérése, értékelése;

Az oktatás tudománya a tanítás-tanulás hatékonyságának és eredményességének megvalósítása érdekében alapelveket dolgozott ki. A didaktikai alapelvek olyan általános követelmények, irányelvek, amelyek a tanítási-tanulási folyamat legfontosabb törvényszerűségeit tükrözik, ezért nagyon fontosnak tartom, hogy figyelmet fordítsunk rájuk a tervezés és megvalósítás során.

A didaktikai alapelvek a következők: [65]

- Az elmélet és a gyakorlat összekapcsolásának elve;
- Tudományosság és szakszerűség elve;
- A tudatos és aktív elsajátítás elve;
- Ismeretek tartósságának elve;
- Szemléletesség elve;
- A rendszeresség és fokozatosság elve,
- Tanítási, oktatási módszerek (Az oktatási módszerek bemutatása a 1. számú mellékletben található meg.);

5.4 A képzések átalakításának lehetőségei a didaktikai és pszichológiai szempontok figyelembe vételével

A **Katonai üzemeltetés alapképzési szakon választható katonai információbiztonsági modul** összesen 3 félévet foglal magába. Ez alatt kell a honvéd tisztjelölteknek a tantervben leírtakat elsajátítani. A specializáció követelményrendszere azonban olyan magas szintű kimeneti tudást vár el a hallgatóktól, ami nem arányos az ismeretek elsajátításához rendelkezésre álló idővel.

Szakmai tapasztalataim alapján megállapítható, hogy az információbiztonsági specializációt végzett tiszteknek az egyetemről kikerülve olyan elméleti és gyakorlati tudással kellene

rendelkezniük, amellyel képesek lennének a szakmai munka elvégzésére. Ez a következőt jelenti: az egyetemen megtanult elmélet segítségével tudjanak eligazodni az információbiztonsági kihívások területén, ismerjék a hatályos jogszabályozási rendszert, legyenek képesek az elméleti tudás gyakorlatban történő alkalmazására. A valódi gyakorlati tudás és a szakmai hozzáértés, profizmus az évek során fog kialakulni azáltal, hogy szakmai tapasztalatot szereznek, folyamatosan képzik magukat.

A katonai információbiztonsági specializáció követelményeit a rendelkezésre álló képzési idő, az elsajátítandó tananyag mennyisége, valamint az emberi elme információ befogadó képességéhez viszonyítva átdolgoztam. A szakmai elvárások és a biztosabb alaptudás igényének figyelembe vételével az alábbi **követelményrendszer alkalmazását javasolom a Katonai üzemeltetés alapképzési szak katonai információbiztonsági modulon:**

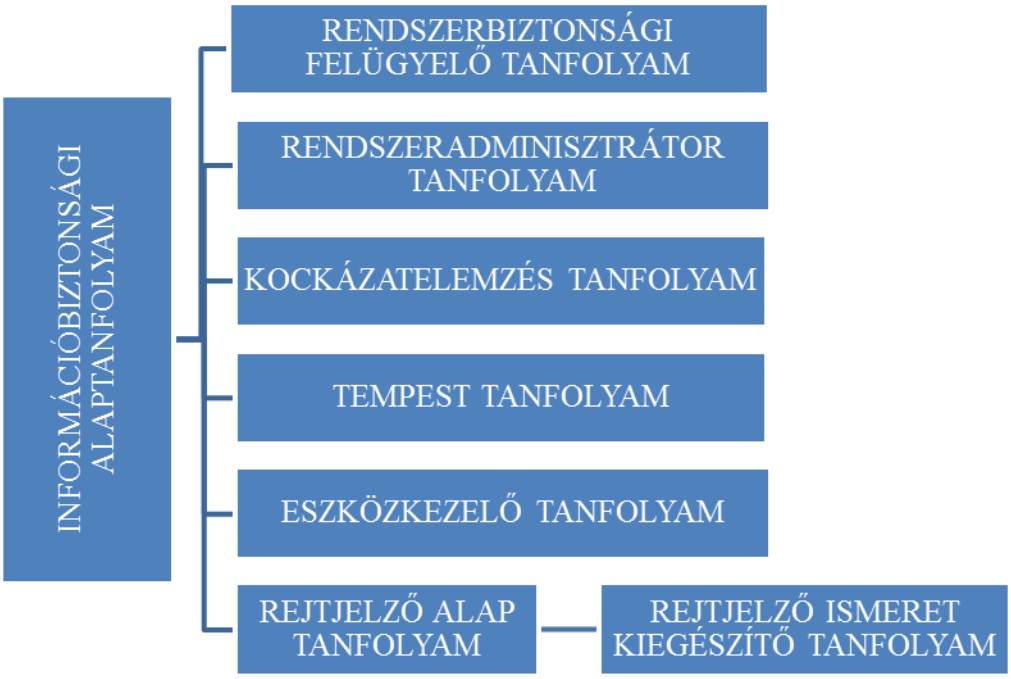
A honvéd tisztjelölt:

- ismerje és alkalmazza az információbiztonsággal kapcsolatos jogszabályokat: törvényeket, rendeleteket, utasításokat, intézkedéseket;
- sajátítsa el az alapnyilvántartás vezetésének szabályait, és rendelkezzen rejtjelző szakirat kezelési alaptudással;
- ismerje a minősített adatkezelő rendszerek működtetéséhez tartozó dokumentációkat, legyen képes ezeket elkészíteni, és pontosan vezetni;
- legyen alkalmas tapasztalt vezető iránymutatása mellett az elektronikus adatkezelő rendszer személyi, fizikai, adminisztratív biztonsági követelményeinek megvalósítására;
- birtokolja a minősített adatkezelő rendszer üzemeltetéséhez szükséges alapismereteket, legyen képes az üzemeltetéssel kapcsolatos feladatok ellátására;
- birtokolja az állandó telepítésű adatkezelő nemzeti és külföldi nyílt, nem nyilvános, minősített elektronikus adatokat feldolgozó rendszerek teljes életciklusával kapcsolatos szakmai ismereteket;
- sajátítsa el a kockázatelemzéssel és kockázatkezeléssel kapcsolatos ismereteket, legyen képes a kockázatelemzés és kockázatkezelés gyakorlati feladatait végrehajtani;
- ismerje meg a kompromittáló kisugárzás elleni védelemre (TEMPEST) vonatkozó általános követelményeket, a TEMPEST felelős feladatait;
- rendelkezzen a rejtjelzéssel kapcsolatos elméleti ismeretekkel, alkalmazza a rejtjelző eszközök üzemben tartásának szabályait,
- legyen képes tapasztalt vezető iránymutatása mellett a rendszerek hatósági akkreditálásával, auditálásával és egyéb hivatalos ügyintézéssel kapcsolatos feladatok végzésére;

- legyen képes tapasztalt vezető iránymutatása mellett a gyakorlatok, konferenciák és egyéb rendezvények rendszereinek tervezésében, üzembe helyezésében, üzemeltetése alatt, illetve megszüntetése során aktívan közreműködni.

Az **információbiztonsági tanfolyamok** megújítása érdekében egy ***információbiztonsági alaptanfolyami rendszert*** dolgoztam ki, amely jó alapot szolgál a többi tanfolyam elvégzéséhez. A tanfolyami rendszer átalakításával elérhető lenne egy hatékonyabb képzés kialakítása úgy, hogy a képzésben résztvevő személy elsőként egy általános információbiztonsági alapot kap, ezt nevezzük „információbiztonsági alaptanfolyamnak”. A többi tanfolyam erre az alaptanfolyamra épül, és az információbiztonsági alaptanfolyam sikeres elvégzése feltétele a többi speciális tanfolyamnak.

Az új tanfolyami rendszer felépítése:



15. sz. ábra: *Elektronikus információbiztonsági tanfolyami rendszer – saját szerkesztés*

Az általános információbiztonsági tanfolyam képzési anyaga tartalmazna minden olyan ismeretet, melyek a szakterületen munkát végző munkatársak szakmai alapkompetenciájához nélkülözhetetlenek, tehát a többi szakmai tanfolyamra már minden egyes beiskolázott személy egy biztos alaptudással érkezne. Az alaptanfolyam tematikáját az alábbi témakörök beépítésével képzelem el:

- Információbiztonsági alapismeretek (alapfogalmak, történeti áttekintés, az információbiztonság helyzete a civil szférában és a Magyar Honvédségben, Az MH információbiztonsági szervezeti felépítése);
- Az információbiztonság részterületei, főbb előírásai;
- Jogalap: nemzeti, NATO, EU szabályzók, a MH saját készítésű szabályzói;
- Az információbiztonság megteremtésében részt vevő személyek, munkakörök, feladatkörök;
- Engedélyeztetések, akkreditálások, ellenőrzések, vészhelyzeti tevékenység;
- Információbiztonsági kultúra kialakítása, fejlesztése;
- Megvalósításra váró feladatok, új kihívások a szakma területén.

Ily módon az információbiztonsági alaptanfolyam bevezetése alkalmas arra, hogy például a Rendszerbiztonsági felügyelő tanfolyam átfogó elméleti részét kiváltsa, ezáltal ezen a tanfolyamon nagyobb figyelmet kaphatnának olyan fontos tananyagok, gyakorlati feladatok, amelyek közvetlenül a feladatkör elvégzéséhez feltétlenül szükségesek. Ezek a következők: felkészülés az akkreditációs folyamatra, lebonyolítás, rendszerengedélyek kérelmezése, meghosszabbítása, Rendszerbiztonsági követelmények (a továbbiakban RBK), Üzemeltetés-biztonsági Szabályzat (a továbbiakban ÜBSZ) elkészítése.

Az eddigi gyakorlat szerint a Rendszerbiztonsági felügyelő tanfolyam utolsó napjaiban a hallgatók vagy egy teljes ÜBSZ-t, vagy annak egy fejezetét készítették el egy megadott rendszerre. Ehelyett célszerűbb és hasznosabb volna az a megoldás, hogy a tanfolyami résztvevők az oktató irányításával közösen töltsék ki az ÜBSZ típusainak egyes pontjait, kapjanak részletes magyarázatot kérdéseikre, hogy később ezeket a tapasztalatokat fel tudják használni saját munkájuk során. A Rendszerengedélyek űrlapjának kitöltéséhez ugyanezt a módszert javaslom. A tanfolyamon résztvevő beiskolázottak az ÜBSZ és az RBK kitöltésével kapcsolatos tudásukról a vizsga alkalmával adnának számot.

Az átalakítással és az alaptanfolyam bevezetésével kiküszöbölhető az a probléma is, hogy az egyes tanfolyamokon átfedések fordulnak elő a tananyag tartalmában.

Hatékonynak és célravezetőnek hiszem azt, hogy egy 4-5 napos elméleti oktatás után kapjon a tanfolyamon résztvevő személy időt arra, hogy az elméleti tananyag leülepedjen, valamint az illető az alkalmazás szintjén is kipróbálhassa új elméleti ismereteit. Ezt a módszert azért tartom előnyösnek, mert a felnőttek a tapasztalatból szerzett tudást könnyebben megszerzik, és

tartósabban megtartják. Az sem elhanyagolandó, hogy ebben az esetben minden személy a saját szervezete szintjén, a saját szervezete problémáira tud fókuszálni.
A rejtjelző alaptanfolyamon rövid idő alatt túl sok elméleti és gyakorlati tananyagot kell a résztvevőknek elsajátítani, ezért a hallgatók az elmélyítés szakaszához képtelenek elérni. Az információbiztonsági alaptanfolyam nagy segítséget adhatna ahhoz, hogy a két hetes tanfolyamon már csak a rejtjelzéssel kapcsolatos konkrét ismereteket kelljen megtanulni. Így a tanfolyam tananyaga a következőképpen változhatna meg:
1. Rejtjeltevékenység végzésével kapcsolatos elméleti ismeretek.
2. Rejtjelző szakügyviteli ismeretek (elmélet, gyakorlat).

A képzés rendszerének kialakítása során fontosnak tartom figyelembe venni azokat a pedagógiai és módszertani útmutatásokat, amelyek a szakmai ismeretek könnyebb elsajátítását segítik elő. Alapvető követelmény számomra, hogy a képzés, oktatás rendszerének kialakítása során pedagógus végzettséggel rendelkező szakembert is bevonjanak a tervezői munkába. Egy didaktikai ismeretek nélkül tervezett és végrehajtott tanfolyam több kárt okozhat a képzésben, mint amennyi hasznot nyújthat. Ez inkább hátráltatja az információbiztonság tudatosításának fejlesztését azáltal, hogy a képzés résztvevői érdektelenek lesznek, így teljesen motiválatlanokká válhatnak.
Az információbiztonsági képzés hasznosságának és eredményességének fő tényezője, hogy a résztvevők számára az elhangzott információk hitelesek, érdekesek legyenek, valamint megfelelő legyen a motiváció a képzésen való részvételre és az ismeretanyag elsajátítására.
A tervezés során arra is ügyelni kell, hogy az elsajátítandó információ mennyiségét a hallgatók be tudják fogadni. Figyelmet kell tehát fordítani a szükséges és arányos tananyag megalkotására és oktatására.
A tanfolyamok, képzések zárásaként hasznosnak tartom egy vizsga beiktatását. A vizsgára való felkészülés ösztönzést jelenthet azok számára, akik egyébként nem eléggé elkötelezettek a tanulás, fejlődés iránt. A vizsga megtervezésekor azonban ügyelni kell arra, hogy csak olyan tananyag kerüljön visszakérdezésre, ami a tanfolyamon feldolgozásra került. Amikor egy vizsgázó sikertelen vizsgát tesz, keressük meg, vajon mi volt az oka a sikertelenségnek. Az illető nem készült fel rendesen a vizsgára? Nem rendelkezett a tanfolyam elvégzéséhez szükséges előképzettséggel? Amennyiben több vizsgázó nyújt gyenge eredményt, érdemes megvizsgálni az oktatási módszereket, a tananyag mennyiségét. A vizsga értékelése az oktatóknak tükröt tart, a tapasztalatok elősegítik az oktatói munka színvonalának emelkedését.

A képzés lezárásaként a beiskolázottaknak lehetőségük van kérdőív kitöltésére is, melyben elégedettségüket, vagy elégedetlenségüket fejezhetik ki, de a tapasztalat szerint hasznos, jól alkalmazható ötletekkel is segíthetik az oktatók munkáját.

Összegzés

Ebben a fejezetben kihangsúlyoztam az oktatás információbiztonsági kultúra alakításában betöltött szerepét. Megvizsgáltam továbbá a Magyar Honvédség információbiztonsági oktatási rendszerét, **rávilágítottam azokra a tényezőkre, amelyek átalakításával egy rendszerezett, logikusabb képzés valósulhatna meg.**

Az 5. 3. pontban összefoglalt pszichológiai ismeretek alátámasztják annak jelentőségét, **hogy az oktatás, képzés tervezése során, a tananyag kiválasztásakor fontos odafigyelni a tanítandó anyag mennyiségének meghatározására tekintettel az emberi agy befogadó képességére, és azokra a tényezőkre, amelyek az információk elsajátítását megkönnyíthetik.** (megfelelő gyakorlási idő, konzultáció lehetősége, gyakorlati alkalmazás, stb.). Az oktatáselméleti ismeretek pedig hozzájárulnak az oktatás – képzés színvonalasabb tervezéséhez, eredményesebb lebonyolításához.

A képzési tematikák áttanulmányozása, és pszichológiai, valamint didaktikai elméletek figyelembevételével kidolgoztam egy új, többlépcsős információbiztonsági tanfolyami rendszert.

A Katonai üzemeltetés alapképzési szak katonai információbiztonsági modul képzésben egy **új kimeneti követelményrendszert állítottam össze,** amely a képzési idővel és a tananyag mennyiségével arányosságot mutat.

6. A SZAKMA - SPECIFIKUS KIVÁLASZTÁS

Bevezetés

Értekezésem bevezető részében már leírtam, hogy öt évig a katonai felsőoktatásban dolgoztam, ahol többek között szakmai tanfolyamokat szerveztem és órákat tartottam. Azt tapasztaltam, hogy eltérő személyiségbeli tulajdonságokkal rendelkező emberek eltérő attitűddel viszonyulnak a biztonság kérdéséhez, ezért a képzések alkalmával szerzett tapasztalatok, konzultációk és a személyes interjúk megerősítettek abban, hogy a szakmai kiválasztás kérdésével érdemes foglalkozni.

6.1 A szakmai kiválasztásról

A „valamire" való alkalmasság megállapítása, az alkalmas egyedek kiválasztása – általános értelmezésben az alkalmassági vizsgálatok – egyidősek az emberiséggel. A történelem során az ember és munka szinkronizálása, mint probléma és követelmény folyamatosan jelen volt. Már a mitológiák, naiv eposzok, ősi népmesék is említik az alkalmasságot, a kiválasztás kezdeti formáit. A természeti népeknél ma is megfigyelhető beavatási szertartások célja, hogy a fiatalt olyan próba elé állítsák, ami a későbbi élete során felmerülő élethelyzetekben való helytállását is előre vetítheti. [66]

Platón[58] Az Állam (Politeia) [67] című művében szintén megjelenik az alkalmasság elvének korai, tudományos igényű megfogalmazása: *„…nincs két ember, akik születésüknél fogva tökéletesen azonosak lennének, hanem mindegyik különbözik a többitől képességei szerint és az egyik erre, a másik arra a tevékenységre alkalmas"*.

A civilizáció fejlődésével, a szakmai specifikációk kialakulásával, majd az ipari termelés elterjedésével az adott feladatkörre való alkalmasság megállapításának szükségszerűsége egyre inkább előtérbe került. A munkaerő kiválasztásával kapcsolatban az első lényeges kihívás az ipari forradalom korában volt, amikor is tömeges igény merült fel munkásokra, sőt ezt a folyamatot fokozta a munkamegosztás megjelenése is. Ebből az időből származik Lyard angol alsóházi képviselő azóta elhíresült mondása: *„Megfelelő embert a megfelelő helyre"* [68].

A XIX. század végén egy erőteljes gazdasági fellendülés hatására hangsúlyosan előtérbe került a munkaerővel való hatékonyabb gazdálkodás, emiatt fontossá vált a kiválasztási technikák tökéletesítése. A technika és a tudomány fejlődése újabb és újabb módszereket hívott életre. Ezek a módszerek az élet valamennyi területén éreztetik hatásukat. Nem véletlen, hogy az

[58] Platón (görögül: Πλάτων), (Kr. e. 347, Athén), ókori görög filozófus, iskolaalapító. Hatása jelentős volt az ókori és a középkori filozófiára, művei manapság is viták és filozófiai vizsgálódások tárgyát képezik.

integrált stratégiai emberi erőforrás gazdálkodásban az „emberi erőforrások áramlása” az egyik legfajsúlyosabb terület.

Napjainkban a menedzseri munka alapvető feltétele mások helyes megítélésének és megértésének képessége. Ez a képesség az emberi erőforrás menedzsment számos tevékenységében kulcsfontosságú, ezek közül kiemelkedik a kiválasztási, felvételi folyamat, de további fontos területei között szerepel a beosztottak munkájának értékelése is.

A munkára való alkalmasság egzakt, tudományos eredmények alapján történő megállapításának professzionális módja a munka alkalmassági vizsgálat. Célja, hogy egy adott munkakörre, szakterületre a legalkalmasabb dolgozók kerülhessenek. Az alkalmassági vizsgálat arra törekszik, hogy a dolgozók későbbi munkahelyi magatartását (teljesítményüket, munkájuk minőségét) a belépéskor elvégzett vizsgálatokkal előre jelezze. **Az alkalmassági vizsgálat legfőbb értéke egyrészt az, hogy segítségével kiszűrhetők azok az egyének, akik az adott munkavégzéshez alapvetően szükséges kompetenciákkal, emberi tulajdonságokkal nem rendelkeznek, másrészt növelhető azok aránya, akik – a kiválasztást követően – kiválóan megfelelnek, beválnak az új munkahelyükön.**

A munkára való alkalmasság alapja a megfelelés elve, melyet Csirszka János könyvében így fogalmaz meg:

„A megfelelés elve lényegében azt a kívánatos viszonyt fejezi ki, mely szerint minél tökéletesebb a személyiség és a munka jellegzetességeinek kölcsönös alkalmassága, annál megalapozottabb az értékes, eredményes és egyben tartósan harmonikus munkavégzés valószínűsége.” [69]

„Az alkalmasság a beválást, mint célt anticipálja, és annak valószínűségét magában rejti. Első megközelítésben az úgynevezett funkcionális meghatározás szerint a munkaalkalmasság a munka jellegzetességeinek olyan szükséges összhangja, amely megadja a beválás lehetőségét és valószínűségét.” [70]

Bár a vizsgálatokkal sem lehetséges teljes bizonyossággal meghatározni egy-egy jelölt jövőbeni magatartását, beválását, de mindenképpen csökkenteni tudják a hibás kiválasztás és a be nem vált munkaerő arányát. Csirszka János szerint: *„Az egyéni adottságok szempontjából az előnytelenebb helyzetben lévő, kevésbé alkalmas embernek sokkal több fáradságot kell személyiségvonásainak fejlesztésére, pótlására fordítania, mint a tárgyi adottságoknak és feltételeknek megfelelő személyiségű egyénnek.”* [71]

A hatékony munka, a megfelelő teljesítmény előfeltétele a magas szintű ismeretek, képességek, készségek, tulajdonságok birtoklása. A professzionális kiválasztási politika a későbbiek során kellő megtérülést jelenthet egy adott szervezetnek.

Világi Rudolf címzetes egyetemi docens a kiválasztás folyamatát általánosan így fogalmazta meg:

„A kiválasztás során a munkakör követelményprofilját összehasonlítjuk a munkakörre jelentkezők "hozott" tudásával, képességeivel, illetve személyiségjegyeivel, és akinél a legkisebb az eltérés, azt alkalmazzuk az adott munkakörben." [72]

6.2 Az alkalmasság kérdésköre

Az alkalmasság fogalma

Bármilyen szervezetről beszélünk is, a betöltendő munkakörhöz az alkalmazónak tisztában kell lennie a munkához szükséges képesség – és készség szintekkel és ezeket fel kell tudnia mérni a kiválasztott esetében.

A munkaköri alkalmasság annak megállapítására is kiterjed, hogy egy meghatározott munkakörben, beosztásban és munkahelyen végzett tevékenység által okozott megterhelés a vizsgált személy számára milyen igénybevételt jelent, és annak leküzdésére alkalmas-e a jelölt.

A „Kiválasztás és interjútechnikák" című kiadványban [73] olvashatunk arról, hogy milyen alkalmassági munkaköri kritériumoknak kell megfelelni egy alkalmassági vizsgálat során. Az előírások összetettek, jelen van bennük személyi –, egészségügyi, képesség – és készségbeli megfeleltség, a munkakörrel kapcsolatos motivációs elvárás. **Lényeges összetevő a személyiség megfelelősége a személyiségvonások és az értékrendszer alapján. Fontos kritérium, hogy a személyiség érettsége és jellemzői illeszkednek-e az adott munkakörben elvárt optimumhoz.**

Az alkalmasság szintjei

Csirszka János: *„A személyiség munkatevékenységének pszichológiája"* című könyvében határozza meg az alkalmasság szintjeit, melyet a következő saját készítésű táblázatban foglaltam össze:

Az alkalmasság szintje	Tartalmi meghatározás	Előfordulás gyakorisága
Abszolút alkalmasság	Az egyén minden munkafeltételnek abszolút megfelel.	nagyon ritka
Kiváló, ill jó alkalmasság	A szükséges kritériumok közötti megfelelés kiegészül a jelölt egyéb pozitív adottságaival.	ritka

Átlagos alkalmasság	Csupán a szükséges kritériumoknak felel meg.	átlagos
Gyenge alkalmasság	Megfelel az alapvető kritériumoknak, de szükségből alkalmazzák, mert nincs nála jobb.	leggyakoribb

6.3 A kiválasztási folyamat

Bármilyen szervezetről legyen szó, az alábbi kiválasztási szakaszokat mindenképpen be kell tartani. A kiválasztás tervezésének folyamata a következő:

„1. A munkakör elemzése: adott munkafolyamatnak és munkafeladatoknak az alapos megismerése, elemzése abból a célból, hogy meghatározzuk, az egyes tevékenységek ellátásához milyen ismeretek, képességek, készségek, tapasztalatok, személyiség-jellemzők, stb. szükségesek.

2. A munkaköri profil (specifikáció) elkészítése: ez a dokumentum tartalmazza az alkalmassági követelmények meghatározását, azokat a belső elő követelményeket, kritériumokat, amelyek a megfelelő szakmai tevékenységhez szükségesek azért, hogy pozitív kapcsolat jöhessen létre az egyén és a munkája között.

3. A munkaköri specifikáció: a munkaköri jellemzők, követelmények és kötelességek ismeretében meghatározhatjuk, hogy milyen képzettséggel, tudással, képességekkel, személyiségjegyekkel rendelkező egyént keresünk.

4. A kiválasztás módszereinek meghatározása: a kritériumoknak megfelelő módszer-együttes kiválasztása, mely biztosítja a sikeres kiválasztást, s előre jelzi a munkavégzésben a valószínű sikert. Az eljárások összefüggenek a munkakörök jellemzőivel, és általában több módszer szükséges az összes kritérium méréséhez.

5. A mérések elvégzése: a munkára jelentkezők vizsgálata a meghatározott eszközökkel.

6. A kiválasztással kapcsolatos döntés előkészítés és döntés: az eredmények értelmezése és az azok alapján való kiválasztás. Az előrejelzés viszonyítása a teljesítményhez: fél- vagy egy év múlva a felvett dolgozóknál meg lehet nézni, hogy a kritériumok mentén hogyan teljesítenek, s az előrejelzés szerint beváltak-e a munkakörükben." [74]

6.4 Az alkalmasság és kiválasztás protokollja az MH–ban

Katonajelöltek kiválasztására már az I. Világháborúban is sor került az MH – ban, és ez az eljárás napjainkban is igen fontos része a szervezetbe való bekerülésnek. A katonai vezetők rákényszerülnek beosztottjaik alapos megismerésére annak érdekében, hogy az adott katona magas szinten legyen képes elvégezni munkáját, folyamatosan motivált és megbízható legyen.

A fejezet elején említettem, hogy már Platón is foglalkozott az emberek képességbeli különbségével. Ezen túl érdemes megemlíteni az ókori Spártát is, ahol a katonai életre való kiválasztás már csecsemőkorban megtörtént, hogy aztán a katonai nevelést már gyermekkorban elkezdjék.

Az alkalmasság kérdésköre és a pszichológia tudomány között szoros kapcsolat áll fenn. A pszichológia születése a 19. század végére tehető, amikor Wilhelm Wundt[59] 1879-ben megalapította első kísérleti pszichológiai laboratóriumát. Az általa elért eredményeket már a hadseregben is alkalmazták. A katonapszichológia fellendülése, külön pszichológiai ágként való megjelenése az első világháború idején következett be. Amikor az USA belépett a háborúba, hatalmas létszámú és nagy ütőerejű hadseregre volt szüksége. Ennek érdekében munkapszichológusokat kértek fel, hogy segítsék az újoncok kiválasztását, beosztásba helyezését, kiképzését.

A két világháború között Németországban 22 kutatóállomáson mintegy 250 pszichológus dolgozott. Csakúgy, mint az USA esetében, a katonapszichológusok foglalkoztak a kiválasztással, beosztásba helyezéssel, a vezetés, a készenlét problémáival. A második világháború után létrejött bipoláris világrend kettőssége megfigyelhető a katonapszichológia fejlődésében is. A nyugati demokráciákban a pszichológiának ez a résztudománya gyorsan fejlődött, az alakulatoknál pszichológusok tevékenykedtek, képezték az állományt, tudományos vizsgálatokat folytattak. Ezzel szemben a szocialista országokban nem végeztek kiválasztást annak ellenére, hogy Magyarországon a katonapszichológia kezdete már az I. Világháború idejére visszanyúlik: 1918-ban az Osztrák – Magyar Monarchiában első ízben végeztek katonai alkalmasság vizsgálatot. Lassú, de folyamatos fejlődésen ment keresztül a magyar katonai alkalmasság vizsgálat, melynek eredményeként az 1970-es években alakult meg a Kecskeméti Repülőorvosi, Egészségvizsgáló és Kutató Intézet, ahol a légierő számára folytattak kiválasztást. 1978-ban megalakult a Központi Sorozóbizottság. A pszichológiai osztály feladata volt a beosztásprofilok megalkotása, munkaköri leírások elkészítése és a vizsgálati eszközök bemérése. Az osztály meghatározta a katonai beosztások sajátosságait és az ehhez szükséges követelményrendszert. A katonapszichológia következő jelentős állomása a csapatpszichológusi hálózat újjáéledése volt. A 2010-ben kiadott 89/2010. (X. 22.) HM utasítás rendelkezik a Csapatpszichológiai Szolgálat kialakításáról és működési rendjével összefüggő egyes feladatokról.

[59] Wilhelm Maximiliam Wundt (1832. – 1920) német pszichológus és fiziológus.

„A kiválasztás célja annak a munkatársnak a megtalálása, aki a legnagyobb valószínűség szerint beválik." [75] Ez alapján elmondható, hogy a hangsúly a beváláson van. Egy alaposan átgondolt kiválasztási rendszer mind a szervezet, mind a munkavállaló számára hasznos, hiszen a beosztottak ott érzik jól magukat, ahol képességeiket, készségeiket a lehető legteljesebb mértékben kamatoztathatják, emellett anyagi és erkölcsi megbecsülésben részesülnek.

6.5 A Magyar Honvédség alkalmasság vizsgáló rendszere

Az MH–ban az alkalmasság vizsgálatokat a 10/2015. (VII. 30.) HM rendelet szabályozza. A dokumentum részletesen kitér arra, hogy milyen esetekben van szükség alkalmasság vizsgálatokra, ezen belül is pszichológiai vizsgálatokra. A katonai alkalmasság vizsgálatok célja kiszűrni azokat a vizsgálati személyeket, akik az MH különböző katonai szervezeteiben, békekörülmények között a várható beosztásukkal szemben támasztott pszichológiai követelményeknek aktuálisan és várhatóan hosszabb távon nem felelnek meg. Tóth Eszter százados cikkében leírja, hogy milyen beosztásba kerülőknél szükséges speciális vizsgálat. Ilyen vizsgálatra kerül sor például búvár, ejtőernyős vagy tűzszerész munkakörök esetében.

„Amennyiben abból a feltételezésből indulunk ki, miszerint fontos, hogy a megfelelő ember a megfelelő feladatot végezze el, akkor szükséges megvizsgálni a személy képességeit, készségeit, az adott munkafolyamat elvárásainak megfelelően. Ennek kapcsán olyan kérdések merülnek fel, hogy mit, milyen eszközzel, módszerrel vizsgáljunk, melyek a legfontosabb vizsgálandó tulajdonságok, milyen számú képesség vizsgálata lesz elegendő az adott munkakörhöz, érdemes-e több vizsgálatot elvégezni a minél pontosabb eredmény érdekében." [76]

NATO csatlakozásunk óta az alkalmasság és kiválasztás még fontosabb kérdéssé vált, mint korábban. A tagországok egymás segítségére lehetnek abban, hogy milyen új és hasznos módszereket célszerű alkalmazni az alkalmasság vizsgálatokban. A német, lengyel és holland haderőben használják a kompetenciaprofil fogalmát. Tóth Eszter cikkében rávilágít, hogy ezt a profilt az egyes munkakörök alapos ismeretével, és a korábban bevált katonák segítségével hozták létre. Ahhoz, hogy a fogalmat megértsük, tisztázni kell jelentését. A kompetencia sokrétű fogalom, többféle meghatározása létezik, de mindegyik megemlíti a személyiséget, a tudást, a képességet és a készségeket.

A kompetenciáknak három fajtájával találkozhatunk. Az általános kompetenciákat a képzés alakítja ki, ezekre épülnek a funkcionális kompetenciák, amelyek a kiváló teljesítményt szolgáló szakmai tudást jelentik. A harmadik kompetenciatípust a kulcskompetenciák alkotják, amelyek egy szervezet vagy intézmény stratégiai célját szolgálják. [77]

A kompetencia alapú kiválasztás célja a következő: azt az egyént kell keresni és megtalálni, aki a legnagyobb valószínűség szerint a legjobb minőségben beválik egy adott munkakörre. Egy alaposan átgondolt kiválasztási rendszer mind a szervezet, mind a munkavállaló számára rendkívül előnyös.

„Visszatérve a kompetenciaalapú kiválasztás lehetőségéhez: a jelentkezőt először felmérnénk, és ezután tennénk javaslatot a jövendőbeli munkakörére. A vizsgálat során kiderítenénk a jelölt érdeklődését, motivációját, tesztekkel, interjú(k) segítségével felmérnénk a képességeit, személyiségét, tudását. Ezek után kerülhetne sor javaslattételre, hogy milyen beosztásokra, melyik szervezethez, milyen munkakörre lenne alkalmas a jelentkező. Így az ideális jelölt nagy valószínűséggel a képességeinek megfelelő munkakört töltené be, sikeres lenne a beosztásában, jobban végezné munkáját, ezáltal növelnénk a dolgozói elégedettséget." [78]

Ennek megvalósítását az információbiztonság területén hosszú távú és eredményes befektetésnek gondolom.

A fenti eljárást a honvéd tisztjelöltek és a tiszthelyettes jelöltek pályaorientációja során is javaslom alkalmazni, így elkerülhető lenne az a több esetben előforduló jelenség, hogy a hallgatók szakmai terület iránti érdektelensége, alkalmatlansága miatt tanulmányaik iránti motivációjuk hiányzik, majd később munkavégzésük színvonala is alacsony szintű lesz, vagy esetleg pályaelhagyóvá válnak.

6.6 Az információbiztonság szintjének növelése szakma–specifikus kiválasztási rendszer alkalmazásával

„A közszolgálati kiválasztás fő funkciója, hogy minden szakterületen a legalkalmasabbak kerüljenek be a közigazgatási szervezetekbe. Ehhez professzionális kiválasztási politika szükséges. Ezért a közszolgálat számára nagy megtérülést jelent, ha folyamatosan fejleszti személyzet-kiválasztási stratégiáját." [79]

A fenti megállapítással teljes mértékben egyetértek, a professzionális kiválasztás során a magam részéről is kulcsszónak tartom a megtérülést, beválást. A hatékonyság érdekében a honvédelmi szervezeteknek is a munkakör tartalmához leginkább illeszkedő kiválasztási módszereket és eszközöket kell alkalmazniuk. Ennek természetes előfeltétele, hogy a kiválasztási eszközök és módszerek beválási indexén[60] túl figyelmet fordítsanak a módszerek esetleges kombinációjának lehetőségére is. A kiválasztási módszerek közül a tesztek használata népszerű pontossága, objektivitása és nyomon követhetősége miatt. Önálló alkalmazása azonban nem célszerű, mert

[60] Valószínűségi index

csak azokat a tulajdonságokat tudja szűrni, amelyek a vizsgálódás körébe belekerültek. Dr. Gyökér Irén oktatási segédanyagában felhívja a figyelmet a tesztelés és az interjú együttes alkalmazására. A személyes interjú lebonyolításakor figyelmet kell fordítani arra, hogy jól előkészített legyen, mivel ez a módszer az interjút folytató személy személyes érzékelésére épít. A két módszer nem helyettesítheti egymást, együttes alkalmazása viszont komplex vizsgálatot eredményez.

Fontos kérdés számomra, vajon azok a munkakörök, amelyek az információbiztonság számára kockázatot jelenthetnek, miért nem igényelnek speciális szűrést? Különösen nagy veszélyt jelent egy olyan munkatárs, aki minősített adatokat kezel, minősített adatkezelő rendszereket üzemeltet. A minősített adattal, informatikai rendszerekkel dolgozó katona nem fizikai erejét kell, hogy kifejezze, munkavégzésének eredménye nem elsősorban attól függ, hogy milyen jól teljesít a lőgyakorlaton. **Sikeres és színvonalas munkájának feltétele az információbiztonsággal kapcsolatos elméleti és gyakorlati tudásán túl, hogy rendelkezzen olyan emberi vonásokkal, tulajdonságokkal, amelyek információbiztonsági munkakörben és minősített adatkezelés esetén elengedhetetlenek. Alapvető elvárásnak tekintem, hogy ilyen munkát végezve a munkatárs megbízható, magabiztos, elkötelezett és tudatos legyen, emellett legyen számára fontos a pontosság, a tökéletességre törekvés is. Kiemelem, hogy rendelkezzen az illető szabálytudattal, felelősségtudattal, legyen befolyásolhatatlan és legyen képes önkontrollra.** Ezek hiányában meglehetősen nagy a kockázata, hogy az illető felületesen fog kezelni olyan minősített adatokat, adatkezelő rendszereket, amelyek talán Magyarország katonai védelmét is veszélybe sodorhatják. Gondoljunk Magyarország katonai reptereire, légiirányító központjaira, radar helyszíneire. Ezen túl fontos kiemelni hazánk Ország Védelmi Tervét, a minősített informatikai rendszereket, rejtjelző berendezéseket, minősített adathordozókat, és nem utolsósorban a minősített dokumentumokat.

A kockázatok csökkentése érdekében érdemes volna felülvizsgálni az információbiztonság megteremtésével összefüggő munkakörök esetében – különös tekintettel minősített adatkezeléssel kapcsolatos beosztásoknál – egy specifikus szűrési lehetőséget.

Egy alaposan átgondolt szűrő rendszer mind a szervezet, mind a munkavállaló számára hasznos, hiszen egy olyan munkatárs, aki alapvetően pontos és megbízható, semmilyen áron nem kompromittálható, egy információbiztonsági munkakört nagy valószínűséggel színvonalasabban tud ellátni, a szervezet pedig nagyobb biztonságban, kevesebb kockázattal tud működni. Egy kompetencia alapú szakmai kiválasztás nem csupán a munkakörben való beválás miatt fontos, hanem szükséges hangsúlyozni, hogy információvédelmi beosztásokban dolgozó katonák ritka esetben kerülnek át más szakmai területre, tehát egy katona esetében egy biztonsági munkakör a

legtöbb esetben hosszú távra, akár egy pályafutásra is szólhat. Ez alátámasztja azt a feltételezésemet, hogy érdemes időt és energiát fektetni a *minőségi kiválasztásra*, hiszen a megtérülés hosszú távra szól.

A kompetencia alapú kiválasztáshoz szeretném hozzáfűzni azt is, hogy szükségesnek tartom vizsgálni a jelölt erkölcsi magatartását is. Vajon mennyire alkalmas az egyén a normák, előírások elfogadására és betartására? Vizsgálni kell azt is, hogy a jelölt ösztönösség helyett képes legyen tudatos viselkedésre. Többször tapasztaltam katonák olyan megnyilvánulását, amikor egy alacsonyabb minősítési szintű adat esetében úgy gondolták, hogy a szabályokat nem kell olyan komolyan betartani, mint egy magasabban minősített adat esetében. Egy alkalmas jelölt számára természetes kell, hogy legyen: a minősített adat minden szinten minősített. Egy információbiztonsági munkakör ellátására alkalmas személy nem döntheti el, hogy mi a fontosabb: egy „Korlátozott terjesztésű" minősítési szintű számítógép, az MH 59. Szentgyörgyi Dezső Repülőbázis repülési terve, nyilvántartása, az MH Nemzeti Légi Vezetési Központ, vagy az Ország Védelmi Terv. **Minden információbiztonsággal kapcsolatos munkát végző személynek azonosulnia kell azzal, hogy a szabályok megkerülése és felülbírálása helyett azok maradéktalan betartása az ő legfőbb feladata.**

Egy információbiztonsági munkakör betöltéséhez nélkülözhetetlenek bizonyos személyes kompetenciák, adottságok, jellemvonások, értelmi-és érzelmi viszonyulások, amelyek lehetővé teszik a hatékony és eredményes munkavégzést. Mivel ezek feltárása nehéz és összetett, ezért egy valóban hasznos szakma specifikus szűrés kidolgozása alapos, bonyolult munkafolyamatot jelent.

Az információbiztonsági munkakörökre tervezett szűrést kétféle módon tartom lehetségesnek:

1. Általánosan alkalmazott kiválasztás minősített adatkezelés esetén – központi vizsgálat (teszt és személyes beszélgetés).
2. Fakultatív lehetőség a vezetők részére (kérdőív és személyes beszélgetés).

Ennek a két alkalmassági vizsgálatnak a kidolgozása és bevezetése összetett munka lenne, de alkalmazását – a kockázatok csökkentése érdekében – mindenféleképpen hasznos módszernek tartom.

Összegzés

A 6. fejezetben megvizsgáltam az MH általános alkalmasságvizsgáló rendszerét, és arra jutottam, hogy az információbiztonsági munkakör betöltéséhez – különösen minősített adatokkal, adatkezelő rendszerek működtetésével összefüggő beosztások ellátásához –, szükség lenne egy szakma – specifikus szűrő rendszer kidolgozására és alkalmazására. Egy alkalmassági vizsgálat

segítségével valószínűsíthető a minél jobb beválás, így az információbiztonsági munkakörök betöltéséhez szükséges személyiségbeli tulajdonságokkal rendelkező személyek alkalmazása növelheti az információbiztonság szintjét.

A kiválasztásnak hozzá kell járulnia, hogy a nem megbízható munkatársak ne kerülhessenek felvételre, és fel kell tudni ismerni azt, ha valamelyik munkatársunk megbízhatatlanná vált.

Az a szervezet, ahol kellő figyelmet fordítanak a beosztottak alkalmasságára, sokkal magasabb információbiztonsági kultúrával rendelkezik mint az, ahol spontán szerveződés történik.

A KUTATÓMUNKA ÖSSZEGZÉSE

Értekezésemben olyan témakör tudományos igényű vizsgálatát kíséreltem meg, amely az információbiztonsági szint növelésének szükségességét, fejlődését, humán vonatkozásait komplexen vizsgálja a jelenkori követelmények tükrében.

Történelmi áttekintésben mutattam be az információbiztonság kezdeti szerepét, jelentőségének folyamatos növekedését. A nemzetközi és hazai helyzetleírás segítségével rávilágítottam arra, hogy az információbiztonság napjainkban az egyik legdinamikusabban fejlődő tudományág.

Disszertációm 1. fejezetében ismertettem az információbiztonság részterületeit, az azt szabályozó jogi hátteret, valamint azokat a munkaköröket, amelyek összefüggenek az információbiztonság megteremtésével.

Mivel dolgozatomban az információbiztonság megvalósulásának humán vonatkozásait komplexen vizsgáltam, ezért a 2. fejezetben kifejezett hangsúlyt fektettem az MH ellenőrzési rendszerének bemutatására. Ezt azért tartottam kiemelten fontosnak, mivel az információbiztonság szintje legegyszerűbben az ellenőrzések során mérhető.

A 3. fejezetben az információbiztonság megvalósulásának humán vonatkozásait dolgoztam fel. Szükségesnek tartottam rávilágítani, hogy a minősített adathoz való hozzáférés előfeltételét biztosító nemzetbiztonsági ellenőrzés nem vizsgálja komplexen azt a személyt, aki magasan minősített adatokhoz is hozzájuthat munkája során. A pszichológiában alkalmazott személyiségelméletekkel támasztottam alá, hogy az emberi tulajdonságok hangsúlyos szerepet játszanak a humán alkalmasság terén.

Kutattam az információbiztonsági stratégia, az információbiztonsági kultúra kérdéskörét.

A biztonságtudatos szervezet jellemzőinek meghatározásával, a biztonsági kultúra kialakításának és fejlesztésének tanulmányozásával bizonyítottam, hogy egy szervezet biztonsági kultúrája és a vezetés, irányítás között szoros összefüggés létezik. Az MH – ban az információbiztonság megfelelő szintjének a megvalósításával és megtartásával kapcsolatos nehézségek feltárása érdekében kérdőívet készítettem az alakulatok biztonsági vezetői részére. A kérdőívek kiindulási alapot adtak kutatómunkámhoz.

Az MH információbiztonsági képzési rendszerének elemzése is ebben a fejezetben található. Pedagógiai és oktatási tapasztalataim tükrében vizsgáltam meg az információbiztonsági képzés jelenlegi helyzetét, szakmai, pedagógiai és logikai szempontok szerinti megújításának lehetőségeit. Feltevéseim igazolásához pszichológiai elméleti és gyakorlati ismereteket használtam fel.

A dolgozat 5. fejezetében egy olyan témában kutattam, amelyik eddig elkerülte a szakma figyelmét. Bemutattam az MH alkalmassági vizsgálatának rendszerét azzal a szándékkal, hogy

felhívjam a figyelmet egy szakma specifikus kiválasztás előnyös alkalmazására az információbiztonsággal összefüggő munkakörök vonatkozásában. A kiválasztást abban az esetben is szükségesnek tartom, amikor a tisztjelöltek az egyetemi képzés során katonai üzemeltetés alapképzési szak katonai információbiztonsági modult választanak. Annak megvalósulásához, hogy az egyetemi oktatásban minél magasabb szinten képzett hallgatók végezzenek, olyan emberi tulajdonságok nyújthatnak segítséget, mint a szorgalom, tudás megszerzésére irányuló akarat, fejlődésre való igény, nyitottság, lelkiismeretesség, szabálytudat. Ezért fontos már a hallgatók körében is a kiválasztás, hogy a képzés minőségbiztosításának alanya – a tanuló – az alapelvárásoknak megfelelő legyen.

SUMMARY OF THE RESEARCH

In my dissertation, I analysed a topic from an academic point of view which examine the necessity, development and human aspects of the level of the information security in a complex way along the contemporary requirements.

Through a historical overview, I presented the initial role of the information security and the persistent growth of its significance. Using the international and national descriptions of the current situation I pointed out that nowadays information security is one of the most dinamically developing discipline.

In the first chapter of my dissertation, I delineated the subdivisions of the information security, the legal regulations and the scope of activities which are related to the establishment of the information security.

As in my dissertation I examined the human aspects of the fulfilment of the information security in a complex way, in the second chapter I put a pronounced emphasis on the presentation of the control system of the Hungarian Defence Forces. I considered this extremely important because in the simpliest way, the level of the information security can be measured through the control activities.

In the third chapter, I elaborated the human aspects of the relization of the information security. I found necessary to highlight that the national security control which is meant to secure the access to classified informations doesn't scan the person who is able to access to strictly qualified datas in a complex way. Using the personality theories ?? applied in the field of Psychology, I confirmed that the human characteristics play a prominent role in human competence.

I studied the issues of the Information security strategy and the information security culture. By defining the charasteristics of a security-conscious organistaion and by investigating the creation and development of the security culture, I proved that there is a close connection between an organistaion's security culture and its leadership, management. In order to identify the difficulties within the Hungarian Defense Forces in connection with the realisation and maintaining of appropriate level of the information security, I prepared a questionnaire for the security leaders of the military corps. Based on the answers had been given for the questionnaires, I clarified the discrepancies and correspondences between certain organisations.

Through my research, I treated specially the role of education, training in the development of the information security culture within the organisations and in the rise of the security consciousness. The analysis of the training system of the informations security within the Hungarian Defense Forces may also be found in this chapter.

I examined the current situation of the training system of the information security, the potentials how to reform it according to professional, pedagogical and logical aspects in the context of my pedagogical and educational experiences. To justify my hypothesis, I applied psychological theoretical and practical knowledge.

In the fifth chapter of my dissertation, I looked into a topic that slipped the competents' notice so far. I introduced the system of aptitude tests within the Hungarian Defense Forces with the intent to draw attention on a preferred application of profession-specific selection with regard to the scope of activities related to the information security. I find the selection necessery even if during their university studies, the officer-candidates choose an information security module. To achieve that the students finishing the university get the best education possible, human caracteristics like diligence, willingness to acquire knowledge, the need for development, open-mindedness, conscientiousness can help. That is the reason why it would be important to have a selection among the students so that he or her would be a good subjective of a quality education.

TUDOMÁNYOS EREDMÉNYEK

1. **Kidolgoztam, és bevezetésre javaslom az elektronikus információbiztonsági tanfolyami alapképzést**, amelyben a képzéssel összefüggő kutatásaim eredményeképpen hipotéziseimet igazoltam. A feltárt nehézségek megelőzése, semlegesítése érdekében logikus, célravezető tanfolyami képzési rendszert dolgoztam ki. Ez a módszer alkalmas arra, hogy a szakma területén dolgozó személyek beosztásba kerülésük előtt megkapják azt az alapképzést, aminek birtokában felelősséggel kezdhetik meg munkájukat. Ennek a képzési rendszernek az alkalmazása kiküszöböli az elaprózott tanfolyami beiskolázást, valamint többlépcsős rendszere miatt széleskörű, rendszerezett ismereteket nyújt a képzésekben résztvevők számára.
Az információbiztonsági alaptanfolyam követelményrendszerének felállításához és tematikájának kidolgozásához a dolgozat 4. fejezetének 9. pontjában tettem javaslatot.
Az új képzési rendszer megvalósításának munkálataiban szükségesnek tartom információbiztonsági munkát végző szakemberek, és pedagógus részvételét egyaránt.

2. **Kidolgoztam a** Katonai üzemeltetés alapképzési szakán (BSc képzés) választható **katonai információbiztonsági modul információbiztonsági új képzési követelményeit.** Ezt a rendszert úgy alakítottam át, hogy a hallgatók ismeretei a diploma megszerzésével széleskörűek, a gyakorlatban jól hasznosíthatók legyenek. Figyelembe vettem azt is, hogy a végzett tisztek tudása az információbiztonság minden területére kiterjedjen, ugyanakkor figyelmet fordítottam arra is, hogy a tananyag mennyisége megfelelően befogadható, és feldolgozható legyen a 3 félév alatt.

3. Elemzéseimet és értékeléseimet követően **kidolgoztam a Magyar Honvédség információbiztonsági alkalmasság vizsgáló rendszerének kialakítására szóló javaslatokat.** Az eredmények alapján javaslatot teszek egy olyan szakma specifikus kiválasztási rendszer létrehozására, amely elősegíti az információbiztonság szintjének emelését azzal, hogy egy „szűrőrendszer” segítségével a munkakörre alkalmatlan személyeket felderíti, ezzel csökkenti a biztonsági kockázatot. A részletes kidolgozáshoz szükségesnek tartom pszichológusok, információbiztonság területén jártas szakemberek és személyiségfejlesztéssel foglalkozó trénerek bevonását is.

4. Értekezésemben **bebizonyítottam,** hogy az ember kiemelten felelős az információbiztonsági incidensek előfordulásáért. A **humán biztonság összetevőit** kutatva megállapítom, hogy ezt a témát komplexen kell vizsgálni, mert a felmerülő kockázatokat csak így lehet a megfelelő szintre csökkenteni. A humán biztonság szemléltetése céljából olyan ábrát készítettem, amely

tartalmazza azokat az alapvető elvárásokat, amelyek feltétlenül szükségesek ahhoz, hogy információbiztonsági munkakört betölthessen egy személy, vagy ezen belül minősített adatokkal, minősített adatkezelő rendszerekkel egy adott személy munkát végezhessen. Hipotéziseim igazolására kutatásaim alapján igazoltam és megállapítom, hogy **a humán biztonság nem valósulhat meg a 3. fejezet 3. pont 1. alpontban bemutatott összetevők nélkül.**

AJÁNLÁSOK

1. Az általam kidolgozott képzési rendszer a jelenleg alkalmazott tematikánál hatékonyabban tudná az információbiztonsági oktatást szolgálni, ezért javaslom az általam kidolgozott többlépcsős képzési modell bevezetését megfontolni a döntéshozóknak.

2. Az oktatási követelmények felállításakor kiemelt figyelmet fordítsanak az elsajátítandó tananyag mennyiségének, nehézségi fokának és az elsajátításra szánt idő mennyiségének az arányára.

3. A katonai üzemeltetés alapképzési szak, katonai információbiztonsági modulra szánt tanulmányi idő összesen 3 félév. Ez alatt kell a honvéd tisztjelölteknek a tantervben leírtakat elsajátítani. A követelmény azonban olyan magas szintű kimeneti tudást vár el a hallgatóktól, ami nem arányos a rendelkezésre álló idővel. Ennek orvoslására olyan – általam kidolgozott – követelményrendszert ajánlok alkalmazásra, amely biztosabb alaptudás elsajátítását eredményezheti.

4. A rejtjelző ismeret kiegészítő tanfolyam olyan biztos alapokra épülő kiegészítő képzés, amely olyan személyek beiskolázását követeli meg, akik megfelelő szakmai alapokkal rendelkeznek. Nekik legfőképp olyan új információkra van szükségük, amelyek a rejtjelzés területén a közelmúltban kerültek bevezetésre, és fontos szerepet töltenek be a szakmában. Például az új rejtjelszabályzat bemutatása, fejlesztések, új rejtjelző berendezések alkalmazása, gyakorlati munkában és nyilvántartásban bekövetkezett változások, stb…, Ezért véleményem szerint az Információvédelem helye, szerepe a Magyar Honvédségben című fejezet nem releváns a rejtjelző ismeret kiegészítő tanfolyam tartalmával.

5. A nemzetbiztonsági ellenőrzés önmagában csak a vizsgált személy kockázatmentességét biztosítja. A komplex, megbízható eljárás érdekében javaslatot teszek – az általam ajánlott – szakma specifikus kiválasztási módszer kidolgozására. Ennek a módszernek a létrehozásával lehetőség nyílna egyrészt egy egységes eljárásra az MH – ban, másrészt a módszer a parancsnokok számára is segítséget nyújthat a beosztottak alkalmasságának megítélése során.

HIVATKOZOTT IRODALOM

[1] Simon László: Az információ, mint fegyver - KNBSZ Szakmai Szemle 2016/1. szám

[2] Óbudai Egyetem Biztonságtudományi Doktori Iskola honlapja - A Doktori iskola szakmai programja - Biztonság és biztonságtudomány p. 3.

[3] www.kiberhaboru.hu (letöltés ideje: 2017.01.10.)

[4] http://www.reuters.com/article/us-cyber-nato-idUSKCN0Z12NE (letöltés ideje: 2017.01.10.)

[5] http://www.nato.int/cps/en/natolive/topics_56626.htm (letöltés ideje: 2017. 01. 13.)

[6] www.origo.hu/.../20170119-hatvan-szazalekkal-nott-a-nato-elleni-informatikai-tamad... (letöltés ideje: 2017. 01. 24.)

[7] Bernáth László – Révész György: A pszichológia alapjai Tertia, 1998 p. 215.

[8] Magyar Értelmező Kéziszótár I. kötet Akadémia Kiadó Budapest 1985 p. 139.

[9] Weisz János előadása MVM Zrt. Biztonsági Igazgatósága 2017. május 24.

[10] http://infoter.eu/video/informaciobiztonsag_inteju_sik_zoltan_nandor (Letöltés ideje:2016. 11. 07.)

[11] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, 2008 Bolyai Szemle XVII. évfolyam 4. szám p. 137 – 156. Budapest, ZMNE BJKMK, ISSN 1416 1443

[12] Közérthetően nem csak az IT biztonságról Budapest, 2013. p. 16.

[13] Dr. Kő Andrea: Informatikai irányítás és menedzsment NKE Vezető és Továbbképző Intézet Budapest 2014. p. 17.

[14] 90/2010. (III. 26.) Kormányrendelet V. fejezet

[15] Tansegédlet a minősített adat védelméről szóló törvény alkalmazásához, KIM, NKI 2010. p.13.

[16] 2009. évi CLV törvény 24§

[17] A büntető törvénykönyvről szóló 2012. évi C törvény 265§

[18] Honvédelmi Közlöny CXL évfolyam 12. szám p. 1271.

[19] A híradó katonák és híradó alegységek kiképzésének szakmódszertana ZMNE BJKMK Budapest, 2008. p. 66-67.

[20] 90/2010. (III. 26.) Kormányrendelet III. fejezet

[21] nbf.hu/dokumentumok

[22] Dr. Horváth Zsolt László: Az információbiztonsági irányítási rendszer alapjai, p. 11

[23] Gordon W. Allport: A személyiség alakulása Kairpsz, 1998

[24] Carl Gustav Jung: Lélektani típusok Budapest 1989 ISBN: 9630749521

[25] Mirnics Zsuzsanna: A személyiség építőkövei Bölcsész konzorcium 2006, ISBN 963 9704 17 2 p. 45.
[26] http://www.internetlivestats.com/internet-users (letöltés ideje: 2017. 08. 08.)
[27] http://www.internetlivestats.com/one-second/#google-band (letöltés ideje: 2017. 08. 08.)
[28] http://www.youtube.com/yt/press/statistics.html (letöltés ideje: 2017. 08. 08.)
[29] http://szifon.com/tag/statisztika (letöltés ideje: 2017. 08. 08.)
[30] http://blog.kissmetrics.com/facebook-statistics (letöltés ideje: 2017. 08. 08.)
[31] http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf (letöltés ideje: 2017. 02. 02.)
[32] http://expandedramblings.com/index.php/amazon-statistics (letöltés ideje: 2017. 02. 02.)
[33] www.virushirado.hu/hirek (letöltés ideje: 2017. 08. 08.)
[34] Dr. Horváth Zsolt László: Az információbiztonsági irányítási rendszer alapjai, p. 11
[35] Kevin D. Mitnick: A megtévesztés művészete Perfact 2003 ISBN: 9789632065557
[36] Dr. Magyar Sándor: Az informatikai biztonságtudatosság jelentősége az adatvédelem területén KNBSZ Szakmai Szemle 2015/2. szám
[37] 41/2015 (VII.15.) BM rendelet 4. melléklet 3.1.7.3. pont
[38] 60/2013 (IX. 30.) HM Utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról
[39] Molnár Imre: Változásmenedzsment a hazai gyakorlatban PhD értekezés, Sopron 2015 p. 24.
[40] Az információs rendszerek és hálózatok biztonságára vonatkozó OECD irányelvek: Útban a biztonságkultúra felé; Gazdasági Együttműködési és Fejlesztési Szervezet, OECD 2003
[41] http://isidor.hu (letöltés ideje: 2017. 02. 02.)
[42] Oroszi Eszter Diána: Információbiztonsági stratégia és vezetés NKE Budapest 2014 p. 33.
[43] Információbiztonsági helyzetkép 2015 ISACA https://www.isaca.hu/index.../mailid-71-isaca-informaciobiztonsagi-helyzetkep-2015 (letöltés ideje: 2017. 04. 06.)
[44] PTA – CERT – Hungary nemzetközi hálózatbiztonsági központ, 2012 www.cert-hungary.hu/node/184 (letöltés ideje: 2017. 02. 02.)
[45] www.aon.com/risk (letöltés ideje: 2017. 04. 06.)
[46] https://hu.wikipedia.org/wiki/Symantec (letöltés ideje: 2017. 04. 06.)
[47] Oroszi Eszter Diána: Információbiztonsági stratégia és vezetés NKE Budapest 2014 p.16.
[48] Sik Zoltán Nándor: Elektronikus információbiztonság és közigazgatás előadás

www.budaib.hu/eloadas.html (Letöltés ideje: 2017. 04. 06.)
[49] Közérthetően nem csak az IT biztonságról Budapest, 2013. p. 108.
[50] Mádi-Nátor Anett – Kardos Zoltán: Információbiztonság-tudatosság gyakorlat NKE 2014. p. 8. ISBN: 978-615-5491 NKE 2014. p. 8 – 13.
[51] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Oktatási Portfoliója p.19 – 20. (hhk. uni-nke.hu/oktatas)
[52] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Oktatási Portfoliója p. 37. (hhk. uni-nke.hu/oktatas)
[53] HHK/156-15/2015
[54] HHK/156-17/2015
[55] HHK/156-18/2015
[56] HHK/156-12/2015
[57] HHK/156-20/2015
[58] HHK/156-19/2015
[59] HHK/156-16/2015
[60] HHK/156-11/2015
[61] Bernáth László-Révész György: A pszichológia alapjai Tertia 2002 p. 121-122.
[62] Bernáth László-Révész György: A pszichológia alapjai Tertia 2002, p. 121.
[63] George Armitage Miller https://hu.wikipedia.org/wiki/George_Armitage_Miller (letöltés ideje: 2017. 02. 02.)
[64] Nagy Sándor: Az oktatás folyamata és módszerei Volos Kiadó 1997 ISBN: 963-85767-0-7
[65] Prohászka Lajos: Az oktatás elmélete Budapest 1937 Országos Középiskolai Tanáregyesület
[66] Nagyné Bereczki Szilvia: A szakma specifikus pszichológiai alkalmassági vizsgálat helye és szerepe a haderőreform tükrében PhD értekezés 2008
[67] Platón: Állam (Politeia) Gondolat, Budapest, 1988 ISBN: 9632827201
[68] Dr. Bokodi Márta: Kiválasztási és interjútechnikák Budapest 2014 ISBN: 978-615-5491-19-1 p. 5.
[69] Csirszka János: A személyiség munkatevékenységének pszichológiája Akadémiai Kiadó 1985
[70] Csirszka János: A személyiség munkatevékenységének pszichológiája Akadémiai Kiadó 1985
[71] Csirszka János: A személyiség munkatevékenységének pszichológiája Akadémiai Kiadó

1985

[72] Világi Rudolf: A szervezeti kultúra érvényesülése a szervezet létszámgazdálkodásában 19. oldal www.uni-zsigmond.hu/images_uploaded/4eedeaca51624.pdf (Letöltés ideje: 2007. 02. 02.)

[73] Dr. Bokodi Márta: Kiválasztási és interjútechnikák Budapest 2014 ISBN: 978-615-5491-19-1

[74] Hegyi Hella: Személyiség a kompetenciák mögött Pécsi Tudományegyetem Alkalmazott Pszichológiai doktori dolgozat 2012. p. 16-17.

[75] Tóth Eszter: A katonai alkalmasság vizsgálatok múltja, jelene és jövője. Honvédségi Szemle, 2015/6. szám, p. 78.

[76] Tóth Eszter: A katonai alkalmasság vizsgálatok múltja, jelene és jövője. Honvédségi Szemle, 2015/6. szám, p. 83.

[77] Tóth Eszter: A katonai alkalmasság vizsgálatok múltja, jelene és jövője. Honvédségi Szemle, 2015/6. szám, p. 79.

[78] Tóth Eszter: A katonai alkalmasság vizsgálatok múltja, jelene és jövője. Honvédségi Szemle, 2015/6. szám, p. 82.

[79] Dr. Bokodi Márta: Kiválasztási és interjútechnikák, NKE Budapest 2014, p. 4. ISBN: 978-615-5491-19-1

[80] Dr. Gyökér Irén: Emberi erőforrás menedzsment Oktatási segédanyag műszaki menedzser hallgatók számára BMGE 2005 p. 35.

ÁBRÁK JEGYZÉKE

IRODALOMJEGYZÉK

Könyvek:

Bernáth László – Révész György: A pszichológia alapjai Tertia, 1998

Csirszka János: A személyiség munkatevékenységének pszichológiája Akadémiai Kiadó 1985.

Gordon W. Allport: A személyiség alakulása, Kairosz Kiadó Budapest, 1998

Carl Gustav Jung: A lélektani típusok Európa Kiadó Budapest, 1994

Platón: Állam (Politeia) Gondolat Budapest, 1988

Falus István: Didaktika. Elméleti alapok a tanítás tanulásához. Nemzeti Tankönyvkiadó Budapest, 1998

Nagy Sándor: Az oktatás folyamata és módszerei 1997

Hans Berner: Az oktatás kompetenciái 2004

Prohászka Lajos: Az oktatás elmélete OPKM, Budapest, 1995

Prohászka Lajos: A pedagógia, mint kultúrfilozófia Királyi Magyar Egyetemi nyomda Budapest p. 28. 1929

Csányi Vilmos: Az emberi viselkedés Sanoma Budapest 2007

Dr. Czuprák Ottó – Dr. Kovács Gábor: Vezetés és szervezéselmélet NKE 2013

Jegyzetek:

Az információbiztonsági irányítási rendszer alapjai, jegyzet Óbudai Egyetem (2016. 01. 31.)

Tansegédlet a minősített adat védelméről szóló 2009. évi CLV. törvény alkalmazásához KIM, NKI 2010.

A híradó katonák és híradó alegységek kiképzésének szakmódszertana ZMNE BJKMK Budapest, 2008

Közérthetően nem csak az IT biztonságról Budapest, 2013

Oroszi Eszter Diána: Információbiztonsági stratégia és vezetés NKE, Budapest, 2014

Dr. Kollár Csaba: Az információbiztonság tudatosság fejlesztése a (felső) vezetők körében coaching és tanácsadás módszerével, Magyar Coachszemle, 2016/3.

Mádi-Nátor Anett, Kardos Zoltán: Információbiztonság-tudatosság gyakorlat NKE 2014

Világi Rudolf: A szervezeti kultúra érvényesülése a szervezet létszámgazdálkodásában

Dr. Bokodi Márta: Kiválasztási és interjútechnikák, NKE Budapest 2014

Janovics László – Szászvári Karina: A képességek alapján történő munkaerő kiválasztás módszertana Pécs 2000 p. 132-154.

Juhász Márta: A kiválasztás pszichológiai alapjai Oktatási segédlet Budapest 2002 BMGE Gazdasági és Társadalomtudományi Kar Ergonómia tanszék
Nemeskéri Gyula · Pataki Csilla: A HR gyakorlata 2007, ISBN: 9789630630382
Dr. Gyökér Irén: Emberi erőforrás menedzsment Oktatási segédanyag műszaki menedzser hallgatók számára BMGE 2005

Cikkek:

Simon László: Az információ, mint fegyver Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle 2016/1. szám
Virányi Gergely: A biztonság - fogalomról másként
A 2013. évi L. törvény végrehajtása érdekében a Magyar Honvédségnél szükséges elektronikus információvédelmi szakfeladatok Hírvillám VIII. évfolyam, 4. szám 2013 december
Dr. Magyar Sándor: Az informatikai biztonságtudatosság jelentősége az adatvédelem területén Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle 2015/2. szám
Tóth Eszter: A katonai alkalmasság vizsgálatok múltja, jelene és jövője. Honvédségi Szemle, 2015/6. szám
Csernyánszky Miklós: Élethosszig tartó tanulás a jövő egyik útja Országos Humánpolitikai Konferencia 2002
Nemeskéry Gyula: A képzés, mint az emberi erőforrás fejlesztésének kiemelt eleme Humánpolitikai Szemle, 2002/1-2. szám
Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, 2008 Bolyai Szemle XVII. évfolyam 4. szám p. 137 – 156. Budapest, ZMNE BJKMK, ISSN 1416 1443
Falus István: Van-e az oktatásnak elmélete? Iskolakultúra 2001 9. szám p. 42 – 45.

Értekezések:

Krasznay Csaba: A magyar elektronikus közigazgatási alkalmazások információbiztonsági megoldásai; PhD értekezés, ZMNE 2011.
Nagyné Bereczki Szilvia: A szakma specifikus pszichológiai alkalmassági vizsgálat helye és szerepe a haderőreform tükrében PhD értekezés 2008
Hegyi Hella: Személyiség a kompetenciák mögött Pécsi Tudományegyetem Alkalmazott Pszichológiai doktori dolgozat 2012
Ollé János: Tanítási – tanulási stratégiák az oktatási folyamatban PhD disszertáció Budapest, 2007

Jogszabályok:

2009. évi CLV törvény a CLV törvény a minősített adat védelméről

90/2010. (III.26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének valamint a minősített adat kezelésének rendjéről

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

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről

335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről

484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről

185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenység vizsgálat lefolytatásának szabályairól

186/2015. (VII. 13.) Korm. rendelet a központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről

187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről

ISO/IEC 17799:2005

60/2013 (IX. 30.) HM Utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról

Guidelines for the Security of Information Systems and Networks, OECD, 2002

MSZ ISO 27001 Szabvány

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

NIS irányelv

COM(2013) 48 final Az Európai Parlament és a Tanács Irányelve a hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről

Honlapok:

Óbudai Egyetem Biztonságtudományi Doktori Iskola honlapja, https://bdi.uni-obuda.hu/ Letöltés ideje (2017. 02. 02) .A Doktori iskola szakmai programja, Biztonság és biztonságtudomány 3. oldal

Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Oktatási Portfoliója http://hhk.uni-nke.hu/ (Letöltés ideje: 2017. 02. 02)

ISIDOR honlapja (főoldal) https://www.isidor.hu (Letöltés ideje: 2017. 02. 02.)

Információbiztonsági helyzetkép 2015 ISACA https://www.isaca.hu/ (Letöltés ideje: 2017. 02. 02.)

http://www.doktori.nyme.hu/512/1/Molnar_Imre_disszertacio.pdf (letöltés ideje: 2016. 11. 20.)

George Armitage Miller https://hu.wikipedia.org/wiki/George_Armitage_Miller (letöltés ideje: 2017. 02. 02.)

Világi Rudolf: A szervezeti kultúra érvényesülése a szervezet létszámgazdálkodásában 19. oldal www.uni-zsigmond.hu/images_uploaded/4eedeaca51624.pdf

(Letöltés ideje: 2017. 02. 02.)

http://www.reuters.com/article/us-cyber-nato-idUSKCN0Z12NE

(letöltés ideje: 2017.01.10.)

http://www.nato.int/cps/en/natolive/topics_56626.htm (letöltés ideje: 2017. 01. 13.)

www.origo.hu/.../20170119-hatvan-szazalekkal-nott-a-nato-elleni-informatikai-tamad (letöltés ideje: 2017. 01. 24.)

http://www.internetlivestats.com/internet-users/ (letöltés ideje: 2016. 11. 07.)

http://www.internetlivestats.com/one-second/#google-band (letöltés ideje: 2017. 02. 02.)

https://www.youtube.com/yt/press/statistics.html (letöltés ideje: 2017. 02. 02.)

https://szifon.com/tag/statisztika/ (letöltés ideje: 2017. 02. 02.)

http://blog.kissmetrics.com/facebook-statistics/ (letöltés ideje: 2017. 02. 02.)

http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf (letöltés ideje: 2017. 02. 02.)
http://expandedramblings.com/index.php/amazon-statistics/ (letöltés ideje: 2017. 02. 02.)
http://expandedramblings.com/index.php/amazon-statistics/ (letöltés ideje: 2017. 02. 02.)
https://securelist.com/analysis/kaspersky-security-bulletin/58265/kaspersky-security-bulletin-2013-overall-statistics-for-2013/ (letöltés ideje: 2017. 02. 02.)
http://www.budaib.hu/eloadas.html (letöltés ideje: 2017. 03. 13.)
http://slideplayer.hu/slide/1942955/ (letöltés ideje: 2017. 03. 13.) Sík Zoltán
www.semmelweis.hu/pszichiatria/files/2013/02/szemelyisegelmeletek.pdf
www.aon.com/risk (letöltés ideje: 2017. 04. 06.
https://hu.wikipedia.org/wiki/Symantec (letöltés ideje: 2017. 04. 06.)
Információbiztonsági helyzetkép 2015 ISACA
https://www.isaca.hu/index.../mailid-71-isaca-informaciobiztonsagi-helyzetkep-2015
(letöltés ideje. 2017. 03. 09.)
PTACERT-Hungary nemzetközi hálózatbiztonsági központ, 2012
www.cert-hungary.hu/node/184 (letöltés ideje: 2017. 02. 02.)
Világi Rudolf: A szervezeti kultúra érvényesülése a szervezet létszámgazdálkodásában
www.uni-zsigmond.hu/images_uploaded/4eedeaca51624.pdf (Letöltés ideje: 2017. 02. 02.)
www.budaib.hu/IW_Sik.ppt (Letöltés ideje: 2017. 01. 09.)

MELLÉKLETEK

1. számú melléklet:

Az oktatás módszereinek felosztása Nagy Sándor és Falus Iván didaktikai elméleteiben

Nagy Sándor (1993)

Új ismeretek tanítása – tanulása:

- motiváció permanens biztosítása
- cél tudatosítása
- tanári kommunikáció (közlés, elbeszélés, magyarázat)
- beszélgetés/megbeszélés
- szeminárium és vita
- felfedezés, tanulás
- szemléltetés
- differenciált szervezés
- tanulók munkáltatása

A képességek tanítása – tanulása:

- aktív fogalomalkotás
- gondolkodás formáinak tanítása
- problémafelvető oktatás
- publikáció vezérvonalának a kiemelése
- struktúrák felfedezése a tananyagban
- tananyag elemzése

Falus István (2003)

- előadás
- magyarázat
- elbeszélés
- tanulók kiselőadása
- megbeszélés/beszélgetés
- vita
- szemléltetés
- munkáltató módszer
- projektmódszer
- tanulási szerződés
- kooperatív módszerek

- szimuláció és játék
- tanulmányi kirándulás
- házi feladat

2. számú melléklet:

Információbiztonság menedzselése tanfolyam

részvételi létszám 16 fő

tanfolyam óraszáma 36

Tanfolyami tematika:

I. A honvédelmi tárca elektronikus információbiztonsági szabályozása

NATO, EU biztonságpolitika, és az azt támogató szabályozók rendje;

nemzeti jogszabályok és a nemzeti hatóságok által alkalmazott módszertanok áttekintése;

a honvédelmi szervezeteknél alkalmazott belső rendelkezések – szabályozás – jellemző; a honvédelmi szervezetek elektronikus adatkezelő rendszereinek szabályozásával kapcsolatos integrálási feladatok;

II. A szabvány alapú keretrendszer kialakítása

Szervezési feladatok

Adatok és adatkezelő rendszerek azonosítása, felelősségek, az adatok osztályba sorolása;

Az elektronikus adatkezelő rendszerek fizikai, személyi, adminisztratív biztonsági dokumentumai.

Üzemeltetési feladatok, védelmi rendszabályok.

A hozzáférés, ellenőrzés feladatai.

A beszerzés, fejlesztés, karbantartás biztonsági kérdései.

Incidenskezelés, működésfolytonosság, megfelelőség.

III. Életciklus menedzsment feladatok: a szabályozottság figyelemmel kísérése, megfelelőségi táblázatok, felülvizsgálat

3. számú melléklet:

Rendszeradminisztrátor tanfolyam

részvételi létszám 16 fő

tanfolyam óraszáma 72

Tanfolyami tematika:

1. Modul: Információ biztonsági alapismeretek, szabályozási környezet

   Információ biztonsági ismeretek: alapvető fogalmak (definíciók, alapelvek)

   Információvédelmi szakterületet szabályzó struktúra

   az elektronikus adatkezelő rendszerekkel kapcsolatos nemzeti-, NATO-, EU policy, direktíva szintű követelmények,

   a nemzeti jogszabályok és a nemzeti hatóságok által alkalmazott módszertanok,

   a szakterület tevékenységét meghatározó HM belső rendelkezések (HM utasítások, szakutasítások, intézkedések, szabályzatok).

2. Modul: Szabványalapú keretrendszer kialakítása (elektronikus adatkezelő rendszerek információbiztonsági követelményei)

   Az adatok és adatkezelő rendszerek azonosítása az adatok osztályba sorolása (felügyeleti szervezeti elemek, szakirányítás általános feladatai, biztonsági menedzsment),

   Személyi biztonsági alapelvek és követelmények,

   Fizikai biztonsági alapelvek és követelmények,

   Adminisztratív biztonsági alapelvek és követelmények,

   Kompromittáló kisugárzás elleni védelem.

3. Modul: Életciklus menedzsment feladatok

   a minősített elektronikus adatkezelő rendszerek biztonsági dokumentációja (RBK),

   kockázatmenedzsment követelmények azonosítása és a kezdeti

   számítógépek (hálózatok) biztonsága (biztonsági beállítás, frissítés, karbantartás, teszt, biztonsági funkciók, biztonsági üzemmódok),

   a rendszerek biztonságáért felelős személyek feladatai ellenőrzés, változások követése, biztonsági esemény, külső meghajtó feloldása, biztonsági naplófájlok ellenőrzése, mentésekben való részvétel, felhasználó felvétele, módosítása, törlése, képzése, rendszerből történő kivonás. Biztonsági incidensekkel kapcsolatos eljárásrend.

4. Modul: Rendszerüzemeltetési alapismeretek

   Hálózati alapismeretek (fizikai, adatkapcsolati és hálózati szint), protokollok

   működése:

   hálózati eszközök funkciójuk működési elvük (router, switch, stb.),

optikai hálózat jellemzői, kialakítása,
router, switch programozás (hozzáférés, IOS csere, beállítások),
hálózati biztonsági megoldások.
Informatikai biztonság:
informatikai biztonság elméleti alapjai,
hálózatbiztonság: tűzfalak, IPS/IDS, SPAM-szűrés, honeypotok, hálózati vírusvédelem, végponti védelem, kártékony kódok elleni védekezés.
Szerverek:
operációs rendszerek biztonságos üzemeletetése: Windows XP, Windows Server 2003,
Active Directory üzemeltetése és a biztonsági házirendek: AD fogalma, AD létrehozása, elemei, működése, csoportházirendek,
MS Exchange 2003 Server: Levelezés protokollok, Exchange 2003 beállításai, elemei, működése, csoportházirendek.

4. számú melléklet:

Rendszerbiztonsági felügyelő tanfolyam

részvételi létszám 16 fő

tanfolyam óraszáma 72

Tanfolyami tematika:

I. Információ biztonsági ismeretek, szabályozási környezet

Alapvető fogalmak (definíciók, alapelvek)

Információvédelmi szakterületet szabályzó struktúra

Az elektronikus adatkezelő rendszerekkel kapcsolatos nemzeti-, NATO-, EU policy, direktíva szintű követelmények.

A nemzeti jogszabályok és a nemzeti hatóságok által alkalmazott módszertanok

A szakterület tevékenységét meghatározó HM belső rendelkezések (HM utasítások, szakutasítások, intézkedések, szabályzatok)

II. Szabványalapú keretrendszer kialakítása (elektronikus adatkezelő rendszerek információbiztonsági követelményei

Az adatok és adatkezelő rendszerek azonosítása az adatok osztályba sorolása (felügyeleti szervezeti elemek, szakirányítás általános feladatai, biztonsági menedzsment)

Személyi biztonsági alapelvek és követelmények

Fizikai biztonsági alapelvek és követelmények

Adminisztratív biztonsági alapelvek és követelmények

Kompromittáló kisugárzás elleni védelem

III. Életciklus menedzsment feladatok

A szabályozói környezet figyelemmel kísérése, megfelelőségi táblázatok, a felülvizsgálattal kapcsolatos teendők

Kockázatmenedzsment követelmények azonosítása és a kezdeti kockázatelemzés elvégzése

Számítógépek (hálózatok) biztonsága (biztonsági beállítás, frissítés, karbantartás, teszt, biztonsági funkciók, biztonsági üzemmódok)

A minősített elektronikus adatkezelő rendszerek biztonsági dokumentációja (RBK)

A minősített elektronikus adatkezelő rendszerek biztonsági dokumentációja (ÜBSZ)

Üzemeltetéshez szükséges okmányrendszer felépítése, alkalmazása

IV. Minősített elektronikus adatkezelésre feljogosított adatkezelő rendszer működtetése során követendő eljárások a teljes életciklus alatt

A rendszerek biztonságáért felelős személyek feladatai

Konfiguráció ellenőrzés, változások követése, biztonsági esemény, külső meghajtó feloldása, biztonsági naplófájlok ellenőrzése, mentésekben való részvétel, felhasználó felvétele, módosítása, törlése, képzése, rendszerből történő kivonás

Biztonsági incidensekkel kapcsolatos eljárásrend

V. Gyakorlati feladat

Minősített elektronikus adatkezelésre tervezett munkaállomás biztonsági szabályzatának (ÜBSZ felhasználók részére) kidolgozása

5. számú melléklet:

Kockázatelemzés tanfolyam

részvételi létszám 16 fő

tanfolyam óraszáma 36

Tanfolyami tematika:

I. A kockázatelemzésre és felmérésre vonatkozó általános követelmények

A nemzeti/NATO/EU Biztonságpolitikák a támogató direktívák kockázatelemzésre és felmérésre vonatkozó követelményei, irányelvei

A kockázatelemzésre vonatkozó nemzetközi és nemzeti szabványok, jogszabályok és ajánlások

A kockázatelemzés célja, modellezése, elvi felépítése, szabályozó rendszere, kapcsolódó dokumentumok

II. Rendszer-szintű, kezdeti kockázatkezelés

A kockázatfelmérés folyamata (a kockázatelemzésre vonatkozó terv, felmérés, jelentés)

Akkreditálási stratégia

A kockázatelemzési terv

A kockázat felmérése

A kockázatelemzés jelentés

III. A kockázatfelmérés és elemzés, gyakorlati feldolgozás

A kockázatelemzésre vonatkozó feladatok tipizálása a szaktanteremben lévő számítógépes hálózat esetében (védendő obj. meghat. (rendszerleírás), vagyontárgyak értékelése, fenyegetéslista, sebezhetőség lista, kockázat mátrix, maradványkockázat, kockázati jelentés, az SSRS kockázatokra vonatkozó összefoglalása).

6. számú melléklet:

TEMPEST tanfolyam

részvételi létszám 16 fő

tanfolyam óraszáma 36

Tanfolyami tematika: [53]

I. A kompromittáló kisugárzás elleni védelemre (TEMPEST) vonatkozó általános követelmények

II. Infosec technikai és alkalmazási direktíva a kisugárzás biztonságáról

III. NATO zónázási eljárásrend

IV. NATO TEMPEST követelmények és kiértékelési eljárásrend

V. NATO létesítmények tervezésére és minősített információt feldolgozó eszközök telepítésére vonatkozó követelmények

VI. Minősített információt feldolgozó elektronikai eszközök telepítésére vonatkozó követelmények

VII. A TEMPEST felelős feladatai

VIII. A kompromittáló kisugárzás elleni védelem

Gyakorlati feldolgozás: TEMPEST ellenőrzési lista, valamint a feljegyzés kitöltése a szaktanteremben lévő számítógépes hálózatra vonatkozóan.

7. számú melléklet:

Rejtjelző alaptanfolyam

részvételi létszám 16 fő

tanfolyam óraszáma 80

Tanfolyami tematika:

I. Az információvédelem helye, szerepe a Magyar Honvédségben.

II. Informatikai és hálózatbiztonsági alapismeretek.

III. Rejtjeltevékenység végzésével kapcsolatos ismeretek.

IV. Rejtjelző szakügyviteli ismeretek.

8. számú melléklet:

Rejtjelző ismeret kiegészítő tanfolyam

részvételi létszám 16 fő

tanfolyam óraszáma 36

Tanfolyami tematika:

I. Általános rejtjelzési ismeretek.

II. Szabályzói környezet.

III. Rejtjeltevékenység szervezeti felépítése.

IV. Fizikai, személyi biztonsággal kapcsolatos ismeretek.

V. Rejtjelző hálózati ismeretek.

VI. Általános ügyviteli ismeretek.

VII. Missziós rejtjelzéssel, logisztikai feladatokkal kapcsolatos ismeretek.

VIII. Rejtjelző vonatkozású szakanyag kezelés. Rejtjelügyvitel gyakorlati ismeretek.

9. számú melléklet:

Információvédelmi eszközkezelő tanfolyam (EKMS, TCE….)

részvételi létszám 16 fő

tanfolyam óraszáma 36

Tanfolyami tematika: [56]

I. Információbiztonsági ismeretek.

II. Szabványalapú keretrendszer kialakítása.

III. Eszközök szolgáltatásai, üzemeltetése és üzemben tartása.

IV. Minősített elektronikus adatkezelő rendszerek működése során követendő eljárások a teljes életciklus alatt.

V. Gyakorlati feladat (eszközök működtetése).

10. számú melléklet:

Informatikai Biztonságtudatosság Tanfolyam

I. Tk. Informatikai biztonság alapvető fogalmai

A biztonság értelmezése

Miért fontos az IT és az információbiztonság

Információbiztonság

A biztonságtudatos szervezet

Megelőzés módszerei (ismeretszerzés, tudatosítás, adatmentés, IT eszközök védelme

A felhasználók felelőssége (biztonsági események bejelentése, elhárítása

II. Biztonsági kultúra megvalósításának alapelvei

Tudatosítás elve

Felelősség

Válaszintézkedések elve

Etika elve

III. Számítógépes visszaélések típusai 2

Jogosulatlan adathozzáférés, módosítás

Jelszavak feltörése

Kéretlen-, illetve hamis lánclevelek

Kártékony alkalmazások (vírus, féreg, trójai, rootkit)

Zombihálózat, reklámprogramok,kémprogramok, hamis szoftverek

Adathalászat, fertőző honlapok, adatforgalom eltérítés

IV. Fizikai visszaélések típusai

Megtévesztésen alapuló csalások

IT személyiséglopás

IT eszközök és adathordozók eltávolítása

Személyes-, illetve hivatali adatok megosztása közösségi hálózatokon

V. Az informatikai eszközök biztonságos használata

Microsoft alapú operációs rendszerek biztonságos használata

A személyes adatok törlése a dokumentumokból

A dokumentumok jelszavas védelme

A dokumentumok titkosítása

Levelezőrendszerek biztonságos használata

Eszközök közötti adatszinkronizálás kockázatai

Vezeték nélküli internet (WiFi) használat kockázatai

Okostelefonok biztonságos használata

Jelszómenedzselő alkalmazások használata

11. számú melléklet:

Informatikai incidenskezelés alapjai tanfolyam

1. Modul: Információ biztonsági alapismeretek, szabályozási környezet

1.1. Információ biztonsági ismeretek (elsősorban informatikai biztonság)

- alapvető fogalmak (definíciók, elvek)

1.2. Információvédelmi szakterületet szabályzó struktúra

- az elektronikus adatkezelő rendszerekkel kapcsolatos nemzeti-, NATO-, követelmények,
- a nemzeti jogszabályok és a nemzeti hatóságok által alkalmazott módszertanok,

- a szakterület tevékenységét meghatározó HM belső rendelkezések (HM utasítások, szakutasítások, intézkedések, szabályzatok).

1.3. Incidenskezelési módszerek és stratégiák. Az incidenskezelés megszervezése, vezetői feladatok

1.4. Aktuális biztonsági incidensek bemutatása (a publikusan ismert események értékelése)

2. Modul: Hálózati-, és végponti nyomforrások

2.1. Nyomrögzítés, -elemzés:

- Windows rendszereken, Linux rendszereken, hálózati eszközökön.

2.2. Adathordozók kezelése: HDD, SSD, USB, DVD.

2.3. Törölt, sérült adatok visszaállításának lehetőségei

2.4 Nyomok elemzése: kulcsszavas keresés, fájltípus alapú keresések, idővonal készítése (timeline).

3. Modul: Kártékony kódok

3.1. Lehetséges elemzési módszerek bemutatása.

3.2. Lehetséges ellenintézkedések bemutatása.

4. Modul: Incidensek forgatókönyve

4.1. Gyakori incidens példák, valamint az incidenskezelés lépései

- Kártékony kód,
- Hálózati lehallgatás,
- Közbeékelődéses támadás (MitM),
- Túlterheléses támadás (DoS / DdoS),
- Webes támadások,

4.2 Technikai kontrollok hatékonysága (tűzfal, AV, IDS/IPS, honeypot)

MELLÉKLETEK JEGYZÉKE

PUBLIKÁCIÓK JEGYZÉKE

1. Mógor Tamásné, Rajnai Zoltán:
Az információbiztonsági kultúra jelenlegi helyzete és fejlesztésének időszerű kérdései Magyarországon.
Felderítő szemle 2017:(2) pp. 1-5. (2017)

2. Mógor Tamásné, Rajnai Zoltán:
Risk analysis of electronic data handling systems
acta technica corviniensis – bulletin of engineering 2017:(3) pp. 1-4. (2017)

3. Mógor Tamásné, Rajnai Zoltán:
Crimes against computer systems and their punishment in Hungary
HÍRVILLÁM = SIGNAL BADGE 2017:(3) pp. 1-5. (2017)

4. Mógor Tamásné, Rajnai Zoltán:
Elektronikus adatkezelő rendszerek kockázatelemzése, kockázati módszerek bemutatása
BOLYAI SZEMLE XXIII:(2) pp. 43-59. (2014)

5. Mógor Tamásné, Rajnai Zoltán:
Elektronikus adatkezelő rendszerek kockázatelemzése, kockázati módszerek bemutatása, összevetése
HÍRVILLÁM = SIGNAL BADGE 4:(2) pp. 29-51. (2013)

6. Mógor Tamásné:
Elektronikus adatkezelő rendszerek kockázatelemzése, kockázati módszerek bemutatása, összevetése
In: Fregan Beatrix (szerk.)
Kockázatelemzés, kockázatértékelés: tanulmányok az Óbudai Egyetem Biztonságtudományi Doktori Iskola kutatásaiból. 207 p.
Budapest: Óbudai Egyetem, 2013. pp. 44-69.
(ISBN:978-615-5018-98-5)