HADMÉRNÖK

**A ZMNE BOLYAI JÁNOS KATONAI MŰSZAKI KAR
ÉS A KATONAI MŰSZAKI DOKTORI ISKOLA
ON-LINE TUDOMÁNYOS KIADVÁNYA**

V. Évfolyam 2. szám 2010. június

**ZMNE
BUDAPEST**

A szerkesztőbizottság elnöke:
Prof. Dr. Halász László

A szerkesztőbizottság elnökhelyettese:
Prof. Dr. Munk Sándor ezredes

A szerkesztőbizottság tagjai és egyben rovatvezetők:
Prof. Dr. Berek Lajos nyá. ezredes CSc (Biztonságtechnika)
Dr. Eleki Zoltán PhD. (Fizikai felkészítés)
Dr. habil. Haig Zsolt mk. alezredes PhD. (Védelmi elektronika, informatika és kommunikáció)
Dr. habil. Horváth László alezredes PhD. (Védelmi igazgatás)
Dr. Jászay Béla PhD. (Védelemgazdaság)
Prof. Dr. Lukács László nyá. mk. alezredes Csc. (Katonai mûszaki infrastruktúra)
Dr. Paskó József CSc. (Térképészet és geoinformatika)
Dr. Szűcs László nyá. ezredes CSc. (Katonai logisztika és közlekedés)
Prof. Dr. Turcsányi Károly nyá. mk. ezredes Csc. (Haditechnika)
Dr. Földi László mk. alezredes PhD. (Környezetbiztonság, ABV- és katasztrófavédelem)

Főszerkesztő: Dr. habil. Kovács László PhD. mk. őrnagy
Szerkesztő: Poroszlai Ákos nyá. mk. alezredes
Webmester: Dr. habil. Kovács László PhD. mk. őrnagy

A szerkesztőség elérhetősége:
Zrínyi Miklós Nemzetvédelmi Egyetem, 1101. Budapest, Hungária krt. 9-11. A. épület 8. emelet
Postacím: 1581. Budapest Pf.:15.
Telefon: +36-1-432-9048
Fax: +36-1-432-9208
HM: 29-734
e-mail: hadmernok@zmne.hu
web: http://hadmernok.hu

Kiadó: Zrínyi Miklós Nemzetvédelmi Egyetem (ZMNE)
Kiadásért felelős: Prof. Dr. Szabó János, a ZMNE rektora
ISSN 1788-1919

Jelen számban megjelent írások szerzői:

Balajti István

Bárdos Zoltán pv. alezredes – Fejér Megyei Katasztrófavédelmi Igazgatóság

Dr. med. Bedros J. Róbert – Pest Megyei Flór Ferenc Kórház

Dr. Berek Tamás mk. őrnagy – ZMNE BJKMK egyetemi docens

Bleier Attila – ZMNE KMDI doktorandusz

Bugyjás József – Óbudai Egyetem KVK

Bunyitai Ákos – ZMNE-BJKMK hallgató (MSc)

Cimer Zsolt – ZMNE KMDI doktorandusz

Deák Ferenc – NCT Ipari Elektronikai Kft.

Farkas Tibor mk. főhadnagy – ZMNE BJKMK egyetemi adjunktus

Fialka György – ZMNE KMDI doktorandusz

Fleiner Rita – Óbudai Egyetem NIK, ZMNE KMDI doktorandusz

Gerő Péter – ZMNE KMDI doktorandusz

Giczi István – ZMNE-BJKMK hallgató (MSc)

Dr. habil. Horváth László nyá. alezredes – ZMNE-BJKMK egyetemi docens

Dr. Hullám István – ZMNE

Dr. med. Huszár András – Pécsi Tudományegyetem

Inkovics Ferenc – ZMNE KMDI doktorandusz

Dr. jur. Istvanovszki László – Szervezett Bűnözés Elleni Koordinációs Központ

Dr. Kassai Károly mk. alezredes – HM Informatikai és Információvédelmi Főosztály

Körmendi Krisztina – ZMNE KMDI doktorandusz

Kuris Zoltán – ZMNE KMDI doktorandusz

Lasz György – ZMNE BJKMK hallgató (MSc)

Miskolczi Ildikó – ZMNE KMDI doktorandusz

Prof. Dr. Munk Sándor nyá. ezredes – ZMNE BJKMK egyetemi tanár

Nagy István – HM FLÜ Technológiai Igazgatóság

Dr. Négyesi Imre alezredes – ZMNE BJKMK egyetemi docens

Dr. Németh Károly nyá. orvos ezredes – HM ÁEK Verőcei Betegotthon

Neszveda József – Óbudai Egyetem KVK főiskolai docens, ZMNE KMDI doktorandusz

Őze Zoltán

Dr. habil. Pándi Erik r. ezredes – ZMNE BJKMK egyetemi docens

Papp Csaba – Hajdú-Bihar Megyei Rendőrfőkapitányság Határrendészeti Szolgálat

Dr. Pellérdi Rezső – ZMNE BJKMK egyetemi docens

Pete Dóra – ZMNE-BJKMK hallgató (MSc)

Dr. Péterfalvi Attila – Országgyűlési Biztos Hivatala, KMDI doktorandusz

Petró Tibor nyá. pv. alezredes – ZMNE BJKMK

dr. univ. Potóczki György – ZMNE KMDI doktorandusz

Prof. Dr. Rajnai Zoltán mk. ezredes – ZMNE BJKMK egyetemi tanár

Dr. med. Révai Róbert – Rendőrség Egészségügyi Központ

Serege Gábor főhadnagy – ZMNE KMDI doktorandusz

Dr. Seres György – ZMNE KMDI

Prof. Dr. Solymosi József – ZMNE BJKMK egyetemi tanár, KMDI vezetője

Solymosi Krisztina – ORFK Rendészeti és Bűnmegelőzési Intézet

Szabó Zsolt alezredes – ZMNE BJKMK Repülő és Légvédelmi Intézet

Szakál Béla – Szent István Egyetem Ybl Miklós Építéstudományi Kar

Szegediné Lengyel Piroska – Zsigmond Király Főiskola, ZMNE KMDI doktorandusz

Dr. med. Székely György – Állami Egészségügyi Központ

Tibenszkyné Dr. Fórika Krisztina sz. százados – ZMNE BJKMK egyetemi adjunktus

Tóth András főhadnagy

Vágföldi Zoltán – MH Görgei Artúr Vegyivédelmi Információs Központ

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Berek Tamás
berek.tamas@zmne.hu

A JÖVŐ TISZTJEINEK ABV VÉDELMI FELKÉSZÍTÉSÉNEK IRÁNYA AZ ABV JÁRTASSÁG KÖVETELMÉNYEINEK TÜKRÉBEN

Absztrakt

A biztonságpolitikai szakértők a korábbi ABV fegyverkezési hullám hozományaként napjainkra új típusú veszélyforrásként jelölték meg az ABV fegyverek gyártásához szükséges anyagok, eszközök, szellemi termékek proliferációjából fakadó fenyegetést. Az ellenőrzés alól kikerült és kisebb felfegyverzett csoportok tárházát bővítő ABV eszközök szerepet kaphatnak kisebb helyi háborúkban. Ezzel párhuzamosan új veszélyforrásként jelent meg napjainkra a nemzetközi terrorizmus, illetve a jelenséggel összefonódó CBRN terrorizmus, valamint az aszimmetrikus hadviselés. A fegyveres erők felkészítése során számításba kell venni továbbra is a fegyveres küzdelem egyik lehetséges színtereként az ABV környezetet. A katonákat úgy kell felkészíteni, hogy a harctevékenységet folytatni tudják ABV körülmények között is. Ennek egyik feltétele egy olyan jártasság kialakítása, amely a katonát képessé teszi először is túlélni az ABV hatásokat, illetve folytatni a tevékenységet.

According to the opinions of security policy experts the new threat is the proliferation of NBC component, facilities, and brain as a result of earlier NBC arms race. It means that NBC weapons can be used by uncontrolled smaller armed groups. Connecting to the proliferation, the threats of global terrorism, NBC terrorism and asymmetric warfare are also exist. During the preparation of troops as a possible theater, NBC environment should be taken into consideration. Troops should be capable to maintain their operations in such environment also, in which, soldiers must be prepared to survive NBC effects and later maintain combat activities.

Kulcsszavak: *ABV környezet, túlélni az ABV hatásokat, kiképzés, ABV gyakorló-pálya, ~ NBC environment, survive NBC effects, Military exercises, NBC exercise field,*

A JÖVŐ HADMŰVELETEINEK VÁRHATÓ KÖRNYEZETE ÉS KÖRÜLMÉNYEI

Az ABV fegyverekkel rendelkező országok száma a II. világháború óta bővült és a jövőben tovább bővülhet. Az ABV fegyverek előállításához szükséges alapanyagok, valamint - a tömegpusztító fegyverre áhítozó küszöb-országok tevékenységének is köszönhetően - sugárzó hasadóanyagok eljuthatnak válságövezetek országaiba is, ahol egy esetlegesen kirobbanó fegyveres konfliktus során alkalmazásra kerülhetnek nem csak reguláris hadseregek, hanem alkalmilag verbuválódott felfegyverkezett csoportok részéről is.

„Az utóbbi időkben nyilvánvalóvá vált az, hogy igen jelentős ABV veszélyforrás lett a terrorizmus, különösen a nemzetközi terrorizmus. A terrorista szervezetek fegyvertára és szakmai ismerete egyre bővül. Sugárzó, mérgező, fertőző anyagok alkalmazásával szélsőséges nézeteket valló vallási szekták, nacionalista terrorszervezetek, egyéni terroristák (magányos farkasok) fenyegethetnek és szándékozhatnak elérni céljaikat.”[1]

A NATO nemzetközi szerepvállalásából és az ebből fakadó kötelezettségeinkből adódóan a Magyar Honvédség katonái a világ különböző pontjain kerülhetnek valós ABV helyzetbe. Az ABV veszélyforrások ismeretében fontos a Magyar Honvédség katonáinak felkészítése. Általános érvényességgel elmondható, hogy a legerősebb, legjobban felszerelt hadsereg is könnyen sebezhetővé válik, ha kiderül felkészítésének, felszereltségének valamely hiányossága.

A valós ABV helyzetben fellépő ABV hatásokhoz (besugárzás, sugárzó anyagok inkorporálódása, mérgezés, biológiai harcanyaggal fertőződés) társuló, nem közvetlenül az ABV fegyverek alkalmazása következményeként fellépő tényezők (pl. egyéni védőeszköz használata közben jelentkező látásélesség, mozgásképesség, komfortérzet, harcképesség, harci morál csökkenése) rontják a harcos túlélő képességét.

Az pedig belátható, hogy a katona kiképzésére, felszerelésére, fegyverzetére fordított minden egyes forint kidobott pénz az ablakon, amennyiben nem vagyunk képesek ezt a harci erőt oltalmazni a túlélés érdekében.[2]

A Magyar Honvédség új típusú feladatai a haditechnikai eszközök változásával együtt megkövetelik, hogy a harceljárások, egyéb műveleti tevékenységek átdolgozása mellett az azokra való felkészítés kiképzés korszerűsítése is megvalósuljon. Ez a folyamat jelenleg is tart, az új harcászati elvek, eljárások sorra beépítésre kerülnek kiképzési programokba, szabályzatokba. A hadviselési eljárások változásának iránya előre nem látható, arra csupán következtetni lehet a tudomány és technológia, a hadelmélet fejlődési tendenciáiból. A biztonságpolitikai szakértők elgondolása szerint a fegyveres küzdelem szinterein összecsapó felek nem egyenrangú erőt fognak képviselni, hiszen a mai csúcstechnika adaptálására még a korszerű hadseregek mindegyike sem képes. Az erőfölényt törvényszerűen ellensúlyozni kívánó aszimmetrikus hadviselés feltehetően a CBRN eszközök alkalmazása felé fog elindulni. [3]

A felkészítésnek-kiképzésnek követnie kell a katonai elméletek változásait, hiszen a jelenlegi kihívásokra már felkészült, a jövőbeni fenyegetésekre pedig jelenleg felkészülő hadsereg képvisel ütőképes erőt a háborús környezet megváltozott körülményei között.

[1] Berek Tamás: ABV felkészítés a jelenlegi veszélyforrások tükrében, 2004. Bolyai Szemle, XIII. évf. 2. szám

A PARANCSNOK[2] ELVÁRHATÓ ABV JÁRTASSÁGA

A NATO Katonai Szabványügyi Hivatal szabványosítási egyezményt (STANAG 2150) adott ki 1997-ben „Az atom-, biológiai-, vegyi fegyverek elleni védelemben szerzett jártasságról annak érdekében, hogy a műveleti területen feladatot végrehajtó és különösen nemzetközi erőket irányító parancsnokok megfelelő bizonyossággal rendelkezzenek az alárendelt erők ABV védelmi képességei felől.

Ahhoz, hogy a parancsnok ABV jártasságát viszonyrendszerbe helyezve a főbb követelmények kiemelésével bemutassam, feltétlenül ki kell térnem a katonával szemben megkövetelt ABV jártasság szintjére.

A katonával szemben elvárható követelmény, hogy felismerje az ABV fegyverek alkalmazására utaló jeleket és ezen információk birtokában tenni tudjon valamit, legalább saját túlélése érdekében.

Ismernie kell az ABV veszélyre figyelmeztető jelzéseket, fel kell ismernie a riasztást. Készség szintjén kell tudnia alkalmazni az egyéni védőeszközét.[4] Véleményem szerint az egyéni védőeszközét becsukott szemmel is alkalmazásba kell tudni venni mindenkinek.
Ezzel összefüggésben a katonának tudnia kell védőruhájának, gázálarcának biztonsági korlátait. A megalapozatlan túlzó tévhit a védőeszköz védelmi képességéről ugyanis éppolyan veszélyes, mint a külső veszély önmagában. Nem csupán azt kell tudnia a harcosnak, hogy mi ellen véd a védőeszköz és hol lehet alkalmazni azt, hanem azt is, hogy mi ellen nem véd és mely esetekben használhatatlan.

A védőruha, gázálarc fel- és levételével, illetve alkalmazásával kapcsolatos fent említett problémák világossá teszik azt, hogy a készség szintű alkalmazás nem egyenértékű azzal, hogy „fel tudom-e venni a védőruhát”. A le- és felvételt, a védelmi szinteket folyamatosan kell gyakorolni addig, ameddig a katona nem csupán becsukott szemmel, hanem egyéb külső fizikai és pszichikai behatások alatt is gondolkodás nélkül végre tudja hajtani azokat. Vajon ugyanolyan gyorsan alkalmazásba lehet venni a védőeszközt az ellenség által tűz alá vett területen tűzharc közben a harci stressz hatása alatt? A pánikreakciók kialakulásának elkerülésére természetesen a gyakorlás sem nyújt 100%-os bizonyosságot, de csökkenti azok kialakulásának lehetőségét. A katona túlélési esélyénél maradva nem vitatható az sem, hogy ha a harcos a fent taglalt készséggel rendelkezik is, ez még mindig kevés, hiszen neki úgy kell túlélni, hogy mellette a feladatát is el tudja végezni. Ennek okán szituációs lőgyakorlatokon és számtalan harcászati gyakorlaton kell begyakoroltatni a katonával Ezeket a fogásokat gyakorolni kell éjjel–nappal, esőben–hóban, hidegben–melegben, nyílt terepen–erdős hegyes területen, stb. A katonának, minden körülmények között végre kell tudni hajtania feladatát. Gázálarcban, védőruhában is. Erre jártasságot kell szerezni, rendszeresen kell alapfeladatának megfelelő gyakorlatokat végrehajtani ABV védőeszközben is. A lövészkatonának például közel azonos hatásfokkal kell kezelni saját egyéni tűzfegyverét éppúgy, mint alegysége kollektív fegyvereit akár gázálarcban is. Ezt a jártasságot rendszeres gyakorlással lehet csak megszerezni. A saját alegysége érdekében, annak szükségességéből, hogy megtudjuk, hogy mi ellen és mennyi ideig kell védekezni vegyi, sugárfelderítést kell végrehajtani az alegység állományából kiállított nem szervezetszerű vegyi, sugárfelderítő rajnak a rendszeresített felderítő eszközökkel.

Ezt a feladatot a katona csak úgy tudja végrehajtani, ha nem csupán ismeri, kezelni is tudja a mérőeszközt valós körülmények között. Mindezekre a feladatokra elég egyszer egy alapos felkészítést tartani, de a megszerzett ismeretekből a napi gyakorlások, harcászati gyakorlatok során kell rutint kovácsolni.

---

[2] A műben a parancsnok kifejezést általános értelemben használom harcoló, harctámogató, harcbiztosító alegység minden szintű parancsnokaira értelmezve egyaránt kiterjesztve a technikai beosztású különböző szintű parancsnokokra

Az ABV jártasság a NATO STANAG 2150 szerinti követelményei a parancsnokok vonatkozásában előírja, hogy a parancsnoknak a beosztottait meghaladó ABV védelmi ismeretekkel kell rendelkeznie. Ahhoz, hogy a parancsnok a veszélyes objektumok környezetében vagy csapásból származó ABV környezetben is tervezni és végre is tudja hajtani a műveletet, ismerni kell az ABV csapásokból és a nem csapásból származó vegyi-, biológiai-és sugárszennyeződés eseményekből eredő veszélyeket.[4] Riasztás és értesítés (Warning & Reporting) hatékonyságának tekintetében kiemelten lényeges a CBRN jelentések tartalmának értelmezése és a riasztás és értesítési rendszer rendszabályainak ismerete.

A műveleti területen folytatott tevékenység hatásfokát, illetve sikerességét jelentősen befolyásolja sok egyéb tényező mellett az ABV fenyegetettségi szint. A harci kötelék védelme érdekében a parancsnoknak meg kell határoznia a személyi állományra vonatkozó védelmi szintet és be kell vezetnie a védelmi rendszabályokat, valamint a beépített kollektív védelmi berendezések (Collective Protection - COLPRO) készenlétét és használatuk rendjét.
A védelmi intézkedések egész sora viszont a rendeltetésszerű feladat-végrehajtást nehezítik. Az adott tevékenység időigénye megnövekszik, ezen kívül a személyi állományra is jelentős pszichikai terhet ró. Az ABV esemény előtt bevezethető passzív rendszabályok közül a profilaktikus készítmények kiosztása és az esetleges alkalmazása okán egyáltalán nem elhanyagolható felelőssége van a parancsnoknak. A parancsnok döntési képessége itt is fontos. A fentiekben felvázolt probléma kezelésének egyik pillére az ABV helyzetfelmérés és helyzetértékelés.

Az ABV helyzet felmérésén alapuló helyzetértékelés elvitathatatlanul a parancsnoki munkafolyamat része. Az ABV értékelést támogathatják az ABV-RIÉR-ből származó jelentések és a műveleti területen elöljáró ABV Központ előrejelzései, mégis adódhat olyan körülmény, amelyben a parancsnok döntésének előkészítésekor csak az alárendelt alegységek nem szervezetszerű vegyivédelmi részlegéből (másodlagos ABV védelmi feladatokra felkészített) vegyi,-sugárfigyelő alegységtől (VSBF) jelentett adatokra támaszkodhat. A pontos számítógépes adatfeldolgozás és értékelés hiányában is intézkedni kell az ABV védelmi rendszabályokra. Ekkor az ismert adatok mellett a bekövetkezett ABV, és/vagy nem csapásból származó vegyi, radiológiai, vagy biológiai eseményről beérkezett kezdeti – VSBF által jelentett – műszeres mérési és a megfigyelési eredményeket kell alapul vennie a döntés-előkészítéshez. A már meglévő, azaz ismert információk körét képezi például az érintett állomány elhelyezkedése, az időjárási viszonyok, a terep jellege, illetve egyéb értékelhető adatok.

A parancsnoknak képesnek kell lennie műveleteket ABV környezetben tervezni a vegyi-, biológiai és radiológiai expozíció lehető legalacsonyabb szinten tartása és az ALARA elv mellett figyelembe véve a fenyegetettséget és az alárendelt alegységek eltérő műveleti képességeit. . A hadszíntér felderítő előkészítése során a parancsnoknak meg kell tudni fogalmaznia a törzs irányába az elsődleges felderítési igényét, amelynek egyebek mellett a fenyegetettség értékelésére, a hadműveleti terület értékelésére, a terep elemzésére és a meteorológiai helyzet elemzésére kell irányulnia A kiképzés, a rendeltetés és az ABV védőeszközökkel való ellátottság komoly mértékben meghatározza az alegységek harci képességeit. A parancsnoknak ugyanakkor fel kell tudnia mérni az alárendeltségébe tartozó, vagy alárendeltségébe utalt vegyivédelmi szakalegység képességeit is, annak érdekében, hogy alkalmazni tudja azokat a művelet biztosítása során. Ismernie kell az anyagi technikai felszereltségüket és lehetőségeiket. [5]

A parancsnoknak meg kell állapítania az ABV és vagy nem csapásból eredő vegyi, biológiai és radiológiai eseményeknek a műveletek végrehajtására és az alegységekre gyakorolt hatásait. Nyilvánvalóan ehhez tisztában kell lennie az ABV fegyverek személyi állományra, harci-technikai eszközökre, műszaki létesítményekre, harcterületre ható

elsődleges és másodlagos pusztító tényezőivel, illetve hogy azok milyen mértékben befolyásolják az általa vezetett katonai műveletet.

A parancsnoknak a fentieken fel kell tudni becsülni saját kötelékének harci képességeit és a lehetőségeit esetleges ABV körülmények közötti végrehajtáshoz. A parancsnoknak ismernie kell az ABV fegyverek hatásait, különösen a végrehajtandó művelet vonatkozásában. Figyelembe kell vennie az ABV események fő erőkifejtésre gyakorolt hatását, és fel kell készülnie a megfelelő ABV védelmi eljárások bevezetésére.

A parancsnoknak az ABV helyzettől függően kényszerű módon olyan intézkedéseket kell meghoznia, melyek csökkentik személyi állományának harcképességét, harci moráljét, ezen keresztül veszélyeztethetik az általa kitűzött cél elérését. Éppen ezért a parancsnoknak folyamatosan mérlegelnie kell az ABV környezetbe került alegysége tekintetében a védőeszközökre vonatkozóan elrendelt védelmi szintek alkalmazásának könnyítésekor több tényező mellett a várható egészségkárosodás és az életben maradás között akkor is, ha előre nem lehet tudni, hogy a többletkockázat valódi sikerrel járt volna-e. A parancsnoknak kell rendelkeznie azzal a jártassággal, hogy adott időben fel tudja mérni a szennyezett terepszakaszon végzett tevékenység kockázatát. A kockázat elemzését követően annak megfelelően kell terveznie a műveletet.

A harctevékenység körletében található szennyezett terepszakaszok, illetve veszélyes anyagokat rejtő ipari objektumok nagymértékben korlátozzák a hadműveletek manőverszabadságát. A parancsnoknak a harctevékenység tervezésekor a már megszerzett vegyi-, sugár-felderítési adatok alapján figyelembe kell ezeket venni.

A szennyezett terepszakaszról történő levonulást követően a parancsnoknak meg kell tudni határozni azt, hogy szükség van-e mentesítésre vagy sem, a mentesítés terjedelmét. Amennyiben mentesítésre kerül a sor, természetesen meg kell tudni szervezni annak végrehajtását.

Fel kell tudni becsülni a védőeszköz huzamosabb időn keresztül tartó viselésének kellemetlen hatásait, és ha kell, könnyítéseket (alacsonyabb védelmi szintet) kell elrendelnie, azaz fel kell tudni ismernie azt a határt, amely elérése után katonáira (és a feladat sikerére) nagyobb veszély leselkedik az ABV védőeszköz legmagasabb szinten való viseléséből fakadó másodlagos hatások által, mint maga a külső ABV veszély. A parancsnoknak minden helyzetben meg kell találnia azt a védelmi szintet, amely megfelelő az adott ABV fenyegetettségnek, de nem jár akkora harcképesség–csökkenéssel, ami az alegység elsődleges küldetésének végrehajtását veszélyeztetné. Az ABV helyzettől függően lehet, hogy ezt a kockázat–haszon mérleget újra kell gondolnia óráról órára, és ennek megfelelően kell változtatnia a védelmi szinten.

A parancsnoknak fel kell tudnia mérni azt a gátló tényezőt, hogy az egyéni ABV védőeszközökben és a szennyezett terepszakaszon csökken a harci kötelék manőverszabadsága. Ezzel összefüggésben parancsnokkal szemben támasztott követelmény, hogy fel tudja becsülni az egyéni ABV védőeszköz hosszabb ideig történő viselésének hatásait. Kell tudnia alkalmazni azokat az intézkedéseket, melyek csökkenthetik a védőeszköz harcképességre, komfortérzetre gyakorolt hatásait. A szennyezett terepszakaszon végzett tevékenység során a parancsnoknak rengeteg információt kell feldolgoznia többek között a személyi állomány harci moráljáról, valamint a műveleti környezet aktuális állapotáról. Adott esetben rövid időn belül lehetővé kell tennie néhány alegység számára a könnyítést a védőruha viselésének terén. Ezzel számos további feladat jelenik meg. Meg kell oldani az adott kötelék kivonását, vagy leváltását a közvetlen műveleti feladatok alól és ezzel párhuzamosan találni kell, vagy alkalmassá kell tenni egy, vagy több, a tevékenységi körletben felelhető objektumot a szükségszerű pihentetés érdekében. Már az is nehéz munka felmérni, hogy az adott ABV hatások alatt végre tudják –e hajtani a szabott feladatot, vagy sem.

Minden feladat esetén a parancsnok határozza meg, hogy mik az elérendő célok. Abban az esetben, ha az ABV események veszélye számottevő, akkor a parancsnoknak kell iránymutatást nyújtania a hadműveleti prioritások kitűzésével. [6]

Ha a szennyezett terepszakaszon, huzamosabb ideig tartó tevékenység elkerülhetetlen, akkor a parancsnoknak mérlegelnie kell az esetleges könnyítő rendszabályok bevezetését, aminek lehetősége igen gyakran korlátozott. Tisztában kell lennie az ABV kockázatvállalás következményeivel, és csupán egy hajszálon múlhat döntésének eredménye. Fel kell ismernie azt a nem egyértelmű helyzetet, amelyben a védőeszköz személyi állományra gyakorolt hatása eléri azt a mértéket, amely harcképességet rontó következménye a katona túlélését fenyegeti. Abban a helyzetben kell döntenie a szükségszerű könnyítések alkalmazásáról, melyben ha nem megfelelően ítéli meg a helyzetet, nagyobb veszélynek teszi ki a személyi állományt a külső ABV hatások által. Az egyéni ABV védelem indokolatlan fenntartása, vagy túlzottan magas védelmi szint alkalmazása (4. védelmi szint) is veszélyeztetheti a katona túlélését és ezzel a művelet sikerét.

Természetesen parancsnokság vegyivédelmi tisztjeinek, tiszthelyetteseinek a törzs többi funkcionális elemeivel, csoportjaival együttműködve segíteni kell a parancsnokot minden olyan célkitűzés és tájékoztatás kiadásában az alárendelt szervezetek részére, ami növeli az ABV védelmi képességeket. [6]

A parancsnokokkal együtt minden tiszt-, és tiszthelyettesnek ismernie kell:

- a vegyi-, sugárfigyelő őrs (VSFŐ) valamint rendszeresített vegyi és sugárfigyelő eszközök telepítését.
- Az ABV felderítés eljárásait.
- Meg kell tudni határoznia mindenkinek a felderítés szükségességét, illetve a felderítés módját. Meg kell határoznia a parancsnoknak a helyzettől, valamint a felderítési céltól függően, hogy a vegyi-, sugárfelderítő járőr melyik felderítési technikát alkalmazza, természetesen a tevékenység és a jelentések rendjét is.
- Minden szintű parancsnoknak ismernie kell az ABV rendszabályokat.

Az ABV esemény előtt bevezetendő passzív rendszabályok, mint például az egyéni sugáradag-mérés megszervezése, az esetleges profilaxis előkészítése, a szükséges műszaki munkák elvégzése és az alapvető harcászati – hadműveleti rendszabályok alkalmazása összetett feladat, amit begyakorlás nélkül igen nehéz pontosan és megbízhatóan végrehajtani a harctevékenységgel összehangolva. Minden szintű parancsnok felelős az ABV védő felszereléssel történő ellátás, karbantartás és az utánpótlás megszervezéséért.

A műveleti területen való tevékenység, illetve az ABV esemény hatása alá került kötelék személyi állományának túlélési esélyit meghatározó tényező az esemény (ABV) alatti rendszabályok bevezetésének gyorsasága és hatékonysága.

A riasztás és értesítés, a közvetlen védelmi intézkedések foganatosítása, a nem szervezetszerű erőkkel végzett vegyi-, sugárfelderítés, valamint az esetleges kivonás – áttelepülés megszervezése gyakorlatot igényel, nem beszélve az esemény után bevezetendő rendszabályokról. Ezek eredményes végrehajtása javíthatja az állomány pszichikai-harci morálját, túlélését, de ha a parancsnok hibázik, vagy késlekedik, esetleg rosszul dönt, a harcképesség gyors csökkenése a művelet sikertelenségét okozhatja. A jövő tisztjeinek tehát igen alapos ABV felkészítésben kell részesülnie.

A KATONAI SZAKOK ALAPKÉPZÉSÉN RÉSZTVEVŐ HALLGATÓI ÁLLOMÁNY ABV FELKÉSZÍTÉSÉNEK JAVASOLT IRÁNYA

A 90/2008. (HK 8.) HM HVKF intézkedése a katonai felsőoktatási intézményben, az alapképzésben ösztöndíjszerződés alapján, a mesterképzésben központi támogatás alapján tanulmányokat folytató hallgatókkal, valamint a Magyar Honvédséggel szolgálati jogviszonyt létesítő tiszti beosztásba tervezett személyekkel szemben támasztandó általános katonai és katonai szakmai követelményekről világosan megfogalmazza a leendő tisztek katonai, szakmai kompetenciáit. Az intézkedés 1. számú melléklete a ZMNE alapképzését befejező, kibocsátandó tisztekkel szemben támasztandó általános katonai és katonai szakmai követelmények között kiemeli: „a tiszt rendelkezzen ismeretekkel a tömegpusztító és gyújtófegyverek pusztító hatásairól, az ellenük való védelem lehetőségeiről…”[7]

A katonai műveletekben feladatot végrehajtó tisztnek tisztában kell lenni az alárendeltségébe tartozó kötelékek ABV védelmi képességeivel, azaz teljes bizonyossággal tudnia kell azt, hogy a felelősségi körébe tartozó erők képesek-e ABV támadást túlélni, illetve ABV környezetben feladatot végrehajtani vagy megkezdett műveletet befejezni.
Amennyiben a parancsnok nincs birtokában a fent említett információnak, nem képes reálisan felmérni és értékelni a saját csapatok harci képességeit és ez végzetes lehet a művelet sikere szempontjából.

Éppen ezért kiemelten súlyt kell fektetni a személyi állomány ABV felkészítésére, különös tekintettel a jövő tiszti állományára.
Hiába rendelkeznek a harci kötelékek a legkorszerűbb rendszeresített ABV védelmi felszereléssel, ha felkészítés rendszeréből hiányoznak azok az elemek, amelyek alkalmassá teszik a parancsnokot azok alkalmazására a feladat végrehajtás érdekében ABV környezetben.

Véleményem szerint a katonai szakokon a jelenleginél nagyobb hangsúlyt kell fektetni a leendő katonai vezetők – a harcoló, a harctámogató és a harcbiztosító alegységek jövőbeli parancsnokainak ABV felkészítésére a szükséges és elvárt ABV jártasság kialakítása érdekében. A katonai alapozó felkészítés keretében illetve később a differenciált szakmai felkészítés során kell a hallgatóknak azokat az ismereteket átadni, melyek birtokában és azok ismétlődő rendszerű gyakorlásával képessé válnak a fentiekben felvázolt problémák felmérésére, értékelésére és alárendeltjeik vezetésére ABV körülmények között is.

Ennek fényében a felkészítést következő tematikában javaslom felépíteni.

A már említett NATO STANAG 2150-ben kifejezett elvárás az, hogy a parancsnok jártassága nem kell, hogy elérje az ABV szaktiszti (tiszthelyettesi) állomány szintjét, de meg kell haladnia a minden katonától elvárható ABV jártasság képességét.[4]
A képességek kifejlesztésének útján az első kilométerkő az általános katonai felkészítés keretében megvalósuló alapkiképzés.

1. A Magyar Honvédség alapkiképzési programja célul tűzi ki azt, hogy a katona a kiképzés végére rendelkezzen alapvető ABV jártassággal.

Az MH alapkiképzési programja biztosítja azt, hogy a katona a kiképzés végére megismerje:

- a ABV- és gyújtófegyver alkalmazásából származó veszélyeket és az ellenük való védelem lehetőségeit, rendszabályait;
- az egyéni és kollektív védelem eszközeit, használatuk rendjét;
- a vegyi-, sugárfelderítő eszközöket, mentesítő eszközöket és anyagokat;



1. ábra. Egyéni védőeszköz fel-, és levételének oktatása alapkiképzésen (a szerző felvétele)

2. Ezt követően a tiszti alapképzés során ezeket az ismereteket folyamatosan frissen kell tartani, azokat gyakoroltatni kell a képzés első éveiben az egyes harcos szintjén. Erre lehetőséget biztosít a katona harckiképzése. (2.-4. szemeszter)

Az időközben bekövetkezett változásokat (pl. új eszközök rendszerbe kerülése során) be kell építeni a képzésbe. A tisztnek a túlélés és a feladat sikeres elvégzésének érdekében képesnek kell arra lennie, hogy a meghatározott feladatot, bármely okból kialakuló vegyi-, biológiai-, sugárszennyezés, valamint harctéri tüzek körülményei között is végre tudja hajtatni alárendeltjeivel. Ezt a célt szolgálva szükségesnek találom a képzés időszakában terepen végrehajtott összes harcászati, szakharcászati, műszaki, lőkiképzési foglalkozás keretében biztosítani a gyakorlás lehetőségét. A foglalkozásokon öt oktatási kérdés közül egyet ABV védőeszköz hatása alatt kellene végrehajtani. Ezen kívül a szennyezett terepszakasz leküzdését is külön ABV foglalkozáson kell elsajátítatni és gyakoroltatni az általános harcászati felkészítés keretében.



2. ábra: Vegyivédelmi hallgatók felkészítése (a szerző felvétele)

3. A tisztképzésben résztvevők az általánost meghaladó ABV jártasságát abban az időszakban kell kialakítani, amikor a hallgató már rendelkezik vezetői ismeretekkel, illetve a csapatgyakorlatokon megszerzett rajparancsnoki jártassággal. A harcászat, szakharcászat, tehát a harckiképzés keretében alkalmassá válik legalább raj – tűzcsoport kötelék harc tevékenységének vagy harctámogató tevékenységének irányítására.

Ekkor (5.-6.-7. szemeszter) a harcászati foglalkozásokon beállított, a fegyveres küzdelem különböző külső körülményeit szimuláló harcászati helyzetbe kell beépíteni a vélt vagy - az imitációs lehetőségek kihasználásával kialakított - valós ABV hatásokat.



3. ábra: **VSF járőr tevékenységének gyakorlása (a szerző felvétele)**

A jól felépített ABV kiképzés a hallgatók felkészítését jól szolgálja, azáltal, hogy olyan helyzetet ismernek meg, amire nehéz felkészülni, de az átélt gyakorlat, a leküzdés tudata segítséget nyújt a későbbi erőpróbákban, és a félelmet, valamint a szorongást kezelve újabb ismerettel gazdagodnak. Megismerhetik félelmeiket, képességeiket, korlátaikat. Veszély esetén tapasztalataikból merítve képesek lesznek később is megküzdeni a helyzettel.[8]. Veszélyhelyzetben fellépő pánikreakció kialakulásának lehetőségét a legalaposabb kiképzés sem zárja ki, azonban valószínűségét csökkenti. A túlélés érdekét szolgáló ABV rendszabályok feladatainak végrehajtása nem szabad, hogy mérlegelés tárgyát képezze a kritikus pillanatokban.

AZ ELKÖVETKEZŐ IDŐSZAK FELADATAI

A tanintézeti felkészítés során azt kell elérni, hogy a természetestől eltérő környezet,- amit elsősorban az egyéni védőeszköz jelent az ABV veszély tudatával – megszokottá váljon. Másrészt azt, hogy a legfontosabb tevékenységek végrehajtása automatikussá váljon. Ez a módszeres gyakoroltatással és sulykolással érhető el.
E módszerek alkalmazásának teret biztosítanak a következők:

- Gyakorlatok
- Normagyakorlatok ismétlése
- ABV rendszabályok végrehajtásának gyakorlása
- Egyes harctevékenység gyakorlása imitált ABV körülmények között
- Váratlan helyzetek generálása:
- ABV riadó elrendelése váratlanul (szokatlan helyzetekben)
- Egyéni védőeszköz váratlan alkalmazása (pl. tanteremben, terepfoglalkozásokon stb.)
- Egyéni védőeszköz alkalmazás hosszútávon (több órás időtartamra)
- Gázkamra-gyakorlatok (jelenleg erre nincs lehetőség)
- Tűzakadály-pálya

Szimulálhatók azok a pszichikumot megterhelő helyzetek, amelyek a felkészítés során való alkalmazásra a valós ABV helyzetet imitáló körülményekkel együtt a személyi állomány pszichikai trenírozására lehetnek alkalmasak.
Jelenleg hasonló hatású a tűzakadály-pálya, de az elmúlt évtizedekben a kiképzés során felhasználták a gázkamra-gyakorlat és az „éles-gyakorlatok" rejtette lehetőségeket is.
A gázkamra gyakorlat az alapkiképzés része volt 1997-ig, akkor kikerült abból. Az addig erre a célra felhasznált klór-pikrin felkerült a vegyi-fegyver tilalmi listára és a készleteket meg kellett semmisíteni. Miért ne lehetne ugyanilyen céllal alkalmazni olyan ingerlő vegyületeket, melyek könnyen beszerezhetők, tárolásuk és felhasználásuk nem igényel különös védőintézkedéseket. Az erre a célra számba vehetők közül megemlíthető a „CN" és a „CS", melyek a legálisan beszerezhető könnygázspray-k töltőanyagaként polgári kereskedelmi forgalomban is kaphatók. A NATO számos tagállamának haderejében a felkészítés részét képezi az ingerlő anyagokkal végrehajtott „gázkamra gyakorlat", valamint a szakalegységek kiképzése során végrehajtott „éles" gyakorlat mérgező harcanyagokkal .
A jövőben meg kell vizsgálni, hogy a leendő tisztek – majdani parancsnokok ABV jártasságának a STANAG 2150 irányelveinek megfelelő kialakítása érdekében, milyen feltételeket tudunk saját erőforrásokból hazai körülmények között biztosítani

A hallgatók felkészítése a gyújtófegyverek elleni védelem terén is számos körülmény újragondolását kívánja meg a közeljövőben

A tűzakadály-pálya kiképzési foglalkozások rendszerben tartása továbbra is szükséges. A katonák gyújtófegyverek elleni védelemre történő kiképzése lényeges a katonák pszichikai felkészítése szempontjából. A gyújtófegyverek továbbra is az alacsony előállítási költségű fegyverek közé tartoznak, melyek hatékonyan alkalmazhatók mind az élőerő, mind pedig objektumok ellen. Ezek a tulajdonságok bármely alkalmazó fél számára csábítóvá teszik a gyújtófegyvereket. Szükséganyagokból is gyorsan, könnyen lehet kialakítani hatékony szükség gyújtóeszközöket. Katonai műveletek végrehajtása alkalmával a műveleti területen nem csupán szándékoltan keletkezhetnek tüzek, hanem hagyományos fegyverek alkalmazása következtében akár véletlenül is. A tűzakadály-pálya foglalkozás másik célja a harctéri tüzek leküzdésére történő felkészítés, és ennek keretében a tűzoltás módszereinek megismerése, elsajátítása valamint gyakorlása szükségeszközökkel, kézi tűzoltó eszközökkel és rendszeresített tűzoltó készülékekkel. A gyakorlás kiterjed a harcjárműben, a harcárokban keletkezett tüzek, valamint az égő személy oltására is. Ezek az ismeretek lényeges elemei a katona kiképzési kompetenciáinak. Ezen foglalkozás alkalmával sajátítják el a katonák a rendszeresített ködösítő és füstjelző eszközök használatát, alkalmazásuk elveit is. Ez a foglalkozás tehát alapozó előkészítése a későbbi komplex harcászati foglalkozásoknak is.
Szükséges- a feladat újraszabályozása, számos körülmény megváltozása miatt. A jelenlegi 93M gázálarc kialakításában eltérő a 70M gázálarctól. Ezen kívül az alegységek alkalmazási környezetének megváltozása, maga után vonta a harceljárások megváltozását is, ezt követnie kell a felkészítés fejlesztésének is. Megfontolásra javaslom a foglalkozás kibővítését olyan módon, hogy a két kiképzési napra tagolt foglalkozás első napján a jelenlegihez hasonlóan történjen a harcos felkészítése a jelenlegi szabályozó alapján (Kézikönyv a terrorizmus és az emberkereskedelem elleni harc katonai feladatainak oktatásához, NYt.szám:4/266, HM HKF, 2009.) ami a Vv/17-es (Utasítás a csapatok gyújtóeszközök elleni védelmére) szabályzatra épül. A második kiképzési napra pedig olyan harcászati helyzetet célszerű beállítani, amely lehetővé teszi a gyakorlat komplexitásának érvényesülését. A komplex foglalkozásba mindenképpen szükséges a tűzakadály-pálya leküzdését, a harcárokban keletkezett tüzek oltását, a páncélozott szállító harcjárművön keletkezett tüzek oltását és ködösítési feladat végrehajtását beépíteni. A kiképzendő állomány a megindulási terepszakaszról, a harcászati helyzet és a feladat ismertetését követően tűzcsoportonként, ill. tűzpáronként, a kijelölt

csoportparancsnokok irányításával kezdi meg a végrehajtást. Az egész gyújtófegyverek elleni védelem kiképzést egyetlen harcászati helyzetbe kell beleágyazni úgy, hogy annak végrehajtása feladatorientált legyen. Ezzel a módszerrel már sikerült sikeres gyakorlati bemutató foglalkozást levezetni a Zrínyi Miklós Nemzetvédelmi Egyetem ócsai kiképző bázisán.

Katonai tanintézeteink rendelkeznek harcászati kiképző bázissal, annak területén tűzakadály-pályával, így rendelkezünk az ABV felkészítési rendszer egy fontos bázisával, a gyakorlótérrel. Nem túl jelentős ráfordítással, jó tervezéssel ki lehetne alakítani a jövőben ezen az alapzaton egy olyan ABV védelmi komplex gyakorló-pályát, amely alkalmas lenne az ABV védelmi jártasság szinte minden elemének kialakítására.

A tiszti hallgatók ABV védelmi felkészítése és gyakoroltatása alapvető fontosságú mind a szakfeladatokra történő felkészítés, mind a szak és nem szakfeladatok ABV környezetben való végrehajtásra történő felkészítés, mind pedig a megfelelő pszichikai felkészítés érdekében.

A kiképzés során kitűzött célok csak úgy valósulnak meg, hogyha következetesen ragaszkodunk ahhoz, hogy valamely ismeretnek készség szintjét alakítjuk ki a felkészítés során. Ezt csak úgy lehet megvalósítani, ha a kiképzés lehetőséget biztosít a „megismeréstől" a „tanulás" és „megerősítés" folyamatán keresztül az „alkalmazni tudás", azaz a jártasság kialakítására. Ez úgy érhető el, ha a felkészítés során a megtanult ismereteket módszeresen és mindig más szituációban gyakoroltatjuk. A fenti követelmények csak akkor teljesülnek, ha lehetősége van a leendő katonatisztnek szokni a megváltozott, gyakran elviselhetetlenül kényelmetlen körülményeket, illetve a fenyegető veszélyeztető hatásokat úgy, mint például az ABV hatásokat ellenőrzött körülmények között, biztonságosan tudják megtapasztalni. Számos eddig is alkalmazott kiképzési módszer ezen alapszik, azaz a félelem tárgyát kontrollált környezetben és szabályozott módon kézzelfogható közelségbe kell hozni a katonához. [9]
A jelen dolgozatomban is említett gyújtófegyverek elleni védelem kiképzését is ezen elvek mentén végezzük az általános katonai felkészítés során a katonává válás folyamatában.
Egyértelműen levezethető és bizonyítható, hogy az ABV védelmi feladatok a harctevékenység fajtáinak mindegyikében jelentkeznek, tehát a harcra történő felkészítésben sem képviselhetnek kisebb arányokat, hiszen ezzel gyenge láncszemmé válna a katona/alegység harci képességeinek rendszerében

IRODALOMJEGYZÉK

1. Conditions of the NBC exercise fieeld creation, 2007. Hadmérnök, www.hadmérnök.hu/archivum/2007/3
2. Berek Tamás: ABV felkészítés a jelenlegi veszélyforrások tükrében, 2004. Bolyai Szemle, XIII. évf. 2. szám, ISSN: 1416-1443
3. Berek Tamás: Fight capabality in NBCcircumtances and the military training: Vth International Symposium on Defence Technology 21-22 Apr 2008 Budapest,Hungary
4. ABV védelmi jártasság NATO szabvány szerinti követelményei, 2004., MH Szárazföldi Parancsnokság
5. Berek Tamás: A parancsnokok felkészítésének kihívásai az ABV jártasság tükrében,in: Tavaszi Szél Konferenciakiadvány, Budapest, 2007.ISBN 978-963-87569-0-9, 441.p.
6. Atom, biológiai, vegyi védelmi doktrína, MH DOFT kód: 12018, MH ÖHP kiadványa, 2010.

7. 90/2008. (HK 8.) HM HVKF intézkedése a katonai felsőoktatási intézményben, az alapképzésben ösztöndíjszerződés alapján, a mesterképzésben központi támogatás alapján tanulmányokat folytató hallgatókkal, valamint a Magyar Honvédséggel szolgálati jogviszonyt létesítő tiszti beosztásba tervezett személyekkel szemben támasztandó általános katonai és katonai szakmai követelményekről
8. Bereczki Sz.-Berek T.: Szorongás-, düh-, kíváncsiság szint változása a tűzakadály-pályán konferencia előadás, 2004. Kard és toll, 2004. 2. szám 64. p.
9. Berek Tamás: Felkészítés a ABV veszély elkerülésére – a felkészítés bázisa, 2008. Bolyai Szemle, XVIII. évf. 1. szám, ISSN: 1416-1443

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Nagy István
istvan.nagy@hmth.hu

MÉRGEZŐ HARCANYAG FELHŐ DETEKTÁLÁSÁNAK VIZSGÁLATA DIGITÁLIS KÉPFELDOLGOZÁS SEGÍTSÉGÉVEL

Absztrakt

Az utóbbi évtizedekben az információs technológia területén tapasztalható drasztikus teljesítménynövekedésnek köszönhetően, számtalan feladat megoldását tudjuk számítógépekkel végezni pl.: folyadékok viselkedését szimulálhatjuk, arcfelismerő rendszert készíthetünk. Napjainkra a vegyivédelmi alkalmazásokat is behálózza az informatika. Kutatásom célja olyan nehezen definiálható anyagok kimutatásának támogatása digitális képfeldolgozással, mint pl.: mérgező harcanyag felhő. A Magyar Honvédségben erre a célra létezik eszköz (RAPID), azonban alkalmazhatóságának javítása napjaink aktuális feladata.

Dramatic performance improvement in the field of information technology in last decades resulted in solving several kinds of tasks using computers, such as simulation of behavior of fluids, producing face recognition system etc. Nowadays not Chemical, Biological, Radiological and Nuclear (CBRN) Defence applications even can be imagined without informatics. My research is aimed at supporting indication of difficult –to-define materials, e.g. toxic agent clouds, by the use of digital image processing. For these purpose the Hungarian Defence Forces has special system (RAPID), however its applicability has to be improved nowadays.

***Kulcsszavak**: digitális képfeldolgozás, távérzékelés, vegyivédelem, mérgező harcanyag felhő ~ digital image processing, remote sensing, CBRAN Defence, Chemical Warfare Agent*

Bevezetés

„A vegyi felderítés általános értelemben a vegyi szennyezettség észlelését, kimutatását, meghatározását jelenti. A vegyi felderítés eszközrendszerében a távfelderítő eszközök különleges helyet foglalnak el. Az ilyen eszközök képesek a szennyezett térrészen kívülről érzékelni és meghatározni a szennyezettség típusát és mértékét. Alkalmasak a mérgező anyagfelhők gyors felderítésére, mozgásuk követésére.”[2]
Napjainkban - kihasználva az érzékelők adta lehetőségeket, mint például a jobb felbontó képesség és dinamika tartomány, versenyképes ár, stb. - olyan távérzékelő rendszereket lehet építeni, melyek hatékonyan tudják támogatni a vegyi távfelderítést is. A távfelderítésben alkalmazható mérési módszerek passzív, illetve aktív eljárásokra oszthatók annak megfelelően, hogy alkalmazunk-e megvilágító fényforrást vagy sem. A passzív eljárásoknál a vizsgált térrészből érkező spontán elektromágneses sugárzást - pl.: szórt napfényt – vizsgáljuk. A Magyar Honvédség rendelkezik egy RAPID típusú, passzív üzemmódú távérzékelő eszközzel, mely az 1. ábrán látható.



1. ábra. RAPID alapműszer

A műszer detektálási határa, 30°látószöget, és 150 m átmérőjű felhőt feltételezve, 5 km. Működési elve FTIR azaz Fourier Transformációs IR (infravörös) mérésen alapszik, vagyis az infra vörös tartományban (0,7-1,5 μm) vett jelalakon végzett mintavételezést és ezen jelalak diszkrét pillanat értékeit alkotó szinuszos komponenseinek frekvencia és amplitúdó meghatározásán alapszik. „Különböző funkciós csoportok, különböző karakterisztikus frekvenciákon nyelnek el, így a kapott IR spektrum az adott molekula újlenyomata. Amennyiben vegyi anyag kerül a műszer látószögébe, és megfelelő hőmérséklet különbség van a háttér és a vegyi anyagfelhő között, úgy ezek szignifikáns eltérésként fognak megjelenni a kapott spektrumon. A passzív FTIR mérés érzékenysége nem egy konstans érték, hanem egy a háttér és a cél hőmérséklet különbségétől függő tényező.”[1]

A RAPID alapműszer rendelkezik látható fény (0,38-0,76 μm) tartományában működő érzékelővel is. Jelenleg ez az érzékelő a kezelő számára „csak” kontrol szerepet tölt be, vagyis látja, hogy merre néz az eszköz. A digitális képfeldolgozás gyakran épít a különböző érzékelési tartományokban készített képek fúziójából kapott előnyökre, amit ennél az eszköznél nem aknáznak ki. Egy ilyen megoldás lehetne az optikai megjelenítőben az FTIR érzékelő által detektált szennyező anyag oldalszög szerinti határainak megjelenítése. Ez

viszonylag egyszerű feladat, és nem igényel külön hardver erőforrást, a grafikus megjelenítésnél, ezáltal a kezelő pontosabb képet kap a szennyező felhőből. A fenti gondolatmenetet tovább elemezve, egy digitális képfeldolgozó egység segítségével az optikai kijelzőn nem csak a harcanyag felhő határait lehetne megjeleníteni, hanem a konkrét kiterjedés formáját is. Az Optical Flow eljárás segítségével pedig a detektált felhő képpontjainak elmozdulásából az adott légköri viszonyokra jellemző áramlási paraméterek is meghatározhatók, vagyis merre terjed a szennyeződés. Ezt a képen kis vektornyilakkal lehet szemléltetni. A továbbiakban a digitális képfeldolgozás szemszögéből kívánom szemléltetni a vegyi harcanyag felhő látható fény tartományban történő elemezésének lehetőségeit.

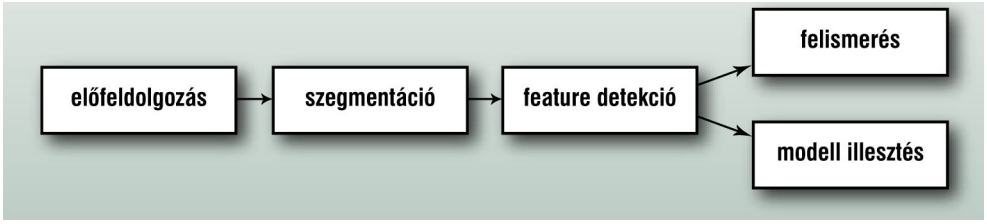
Mérgező harcanyag felhő detektálása

A mérgező harcanyagot kétféleképpen lehet levegőbe juttatni: tüzérségi úton vagy repülő eszközről permetezve. Ez utóbbinál csupán a kibocsájtó eszköz mozgásának detektálására van lehetőség (felismerés), ugyanakkor ez is tartalmazhat lényegi információkat a kezelő számára. Az első módszer alkalmazásánál a robbanásból adódó tűz illetve leggyakrabban füst detektálása komoly képfeldolgozási feladat. A harcanyag felhő nagyon nehezen általánosítható közeg, mert kifejlődhet gyorsan, néhány másodperc alatt, vagy lassan órák alatt. A harcanyag felhő homályosíthatja, szinte elfedheti a háttérből visszaverődő fényt, ilyen a sötét aerosol, illetve szétszórhatja különböző irányokban, a képen intenzitásváltozást okozva, ilyen a fehér aerosol. A felhő lehet vékony és átlátszó, vagy vastag és texturált akár egy zárt objektum.
A korai felhő-detektáló algoritmusok a teljes képen próbáltak jellemzőket detektálni, pl.: kontraszt változás detektálásával, élek eltűnésének figyelésével, a kép fényesség értékeinek statisztikai analízisével. A gyakorlatban ezen algoritmusokra épülő alkalmazások megbízhatatlanok voltak, mert egy parányi változás a képen túl sok tényezőtől függhet., pl.: egy objektum elmozdul, vagy kikerül az érzékelő kamera látószögéből. Ezért komplexebb eljárásokat alkalmaztak, mint pl.: a geometriai jellemzők változásának figyelése.
Melyek azok a következetesen előforduló jellemzők, amelyek a harcanyag felhőkkel együtt jelenek meg a képen? Fizikailag a felhő egy aeroszol, amely az égés/robbanás helyéről terjed. Generálódásának mértéke nagyban függ az égés intenzitásának a mértékétől. Az égéshez hő kibocsájtással társul, mely befolyásolja a harcanyag felhő irányát és sebességét, amit természetesen a környezet is befolyásol, pl.: aktuális szélirány.

Digitális képfeldolgozás

A következőkben, általánosságban áttekintésre kerül, hogyan működnek a számítógépes képfeldolgozó algoritmusok. Bár elsőre nem szembetűnő, de e problémák megoldása hasonló lépésekkel történik, lásd 2. ábra. Szinte mindig célszerű a képeket egyszerű transzformációkkal, szűrőkkel előfeldolgozni. Az így kapott kép valószínűleg tartalmaz fontos és lényegtelen területeket is. Ezek a szegmentáció során kerülnek szétválasztásra egymástól. Így megkaptuk a kép számunkra fontos területét, amely ugyan kevesebb, de még mindig pixelek ezreit (akár millióit) jelentheti, ami a legtöbb algoritmus számára túl sok feldolgozandó adatot jelent. A sűrű „képpont felhőből” kezelhető mennyiségű adatot az ún. featureök, vagy „vizuális jellemzők” kinyerésével kapunk. Ez legtöbbször vonalak, sarkok vagy egyéb szempontból speciális elemek detektálását jelenti. Így már nem pixelekkel, hanem kezelhető mennyiségű képi jellemzővel kell dolgoznunk. Ezek alapján már megkereshetőek az előre eltárolt adatbázisban a jellemzőkhöz legjobban hasonlító objektumot (felismerés), vagy kiszámíthatjuk a legjobban illeszkedő (mozgás, pozíció) paramétereket. Érdemes

figyelembe venni, hogy a képi jellemzők kinyerése során hamis találatokat is kaphatunk, amiket fel kell ismerni, és ki kell szűrni az adathalmazból.



2. ábra. A számítógépes képanalízis fázisai

Előfeldolgozás, szegmentálás

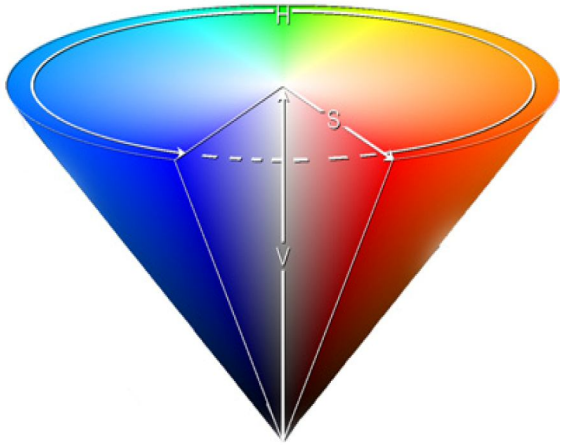
A képszegmentálás alapvető célja, hogy a képnek olyan reprezentációját adja, amely egyszerűen feldolgozható és elemezhető automatizált módszerekkel. [5] Ez legtöbbször a képen található releváns objektumok elkülönítését és címkézését jelenti. A magasabb szintű képértelmezés így jelentősen redukált adatmennyiséggel és egyben jól definiált szemantikával rendelkező reprezentáción végezhető. A továbbiakban két féle szegmentálási eljárást mutatok be, mely homogén objektumok detektálására alkalmas.

1. Intenzitás alapú szegmentálás

Az egyik legegyszerűbb szegmentálási eljárás szerint az objektumokat az intenzitásuk alapján jelöljük ki, vagyis kijelölünk egy intenzitáshatárt, amely feletti intenzitású pixeleket objektumhoz tartozónak, az alattiakat pedig háttérnek (vagy irrelevánsnak) tekintjük. Hátrány, hogy bonyolultabb, inhomogén környezetben pontatlan szegmentáláshoz eredményez.
Hisztogram-alapú adaptív küszöbérték alkalmazásával általában lehet javítani a szegmentálás minőségén. Ezen eljárások közt találhatóak olyanok, amelyek valamilyen heurisztika alapján állapítják meg a hisztogram jellemzőiből a küszöbértéket. Ezen kívül léteznek olyan eljárások is, amelyek matematikai alapon, valószínűségi modelleket alkalmazva határozzák meg az ideális küszöbértéket.

2. Szín alapú szegmentálás

A szín alapú szegmentálás elgondolása szerint, a releváns objektumokat színük alapján tudjuk elkülöníteni és lokalizálni. Egy színes kép digitális megjelenítése és tárolása a képpontonkénti (pixel) színintenzítás érték alapján történik. Ezt az intenzítás értéket általában háromdimenziós vektorral írjuk le. Ezen vektortér komponenseinek meghatározása az alkalmazott szín tér alapján változhat [6].
Az additív képmegjelenítés, pl.: monitor, és képtárolás, pl.: avi fájl, az RGB (Red, Green, Blue) szín teret használja. Azonban a képfeldolgozási algoritmusok gyakran más színtereket alkalmaznak, bizonyos képi jellemzők kinyerésére. Az egyes színterek közötti transzformáció, jól definiált, szabványos eljárásokkal történik. Szín alapú szegmentálásra leggyakrabban a HSV (Hue, Saturation, Value) szín teret használjuk. Az alábbiakban bemutatom a HSV szinteret valamint az RGB, és HSV színtér közötti konverziót.
HSV színtér
Legtöbb esetben a HSV színteret tekinthetjük egy intuitív színi leírásmódnak, mivel olyan fogalmakat használ, melyek jobban illenek az ember gondolati színtársításához.



3. ábra. A HSV szín tér (MATLAB Help)

Hue: A pixel színárnyalata a saját alapszínére vonatkozik, pl.: vörös, sárga, ibolya vagy magenta. Ez a 0-tól 360-ig terjedő skálán fordul elő; utalva a színnek a színskálán való fokokban megadott helyére, ezt a 3. ábrán a kúp alapján látható.
Sarutation: A telítettség a pontos színezet fényessége vagy tisztasága, amely jelen van a pixelben. Mint ahogy a 3. ábrán látható a színkör kerületének színei teljesen telítettek, továbbá a színkör középpontja felé haladva csökken a telítettség mértéke.
Value: A szín élénkségét jelenti, de valójában a vörös, a zöld és a kék értékek maximumát jelenti. Ezt a pixel értéket a harmadik axis mentén ábrázolják. A legkisebb ilyen értékkel a kúp alján elhelyezkedő fekete, míg a legmagasabb élénkségi értékkel következésképpen a vele szemben elhelyezkedő fehér rendelkezik. Mivel az emberi szem az élénkebb színeket jobban meg tudja különböztetni, ezért henger helyett, kúpként lehet ábrázolni ezt a szín teret.
Az RGB színtérből HSV-be való áttérés egy nemlineáris transzformációval valósítható meg. Az alábbiakban feltesszük, hogy R, G és B [0,255] közti értékeket vehet fel, és H-t, S-t és V-t a [0,360], [0,255] illetve [0,255] intervallumon belül keressük. Továbbá legyen min=min(R,G,B), és max=max((R,G,B

$$H=\begin{cases} \dfrac{60*(G-B)}{\max(R,G,B)-\min(R,G,B)}+0, ha \max(R,G,B)=R, G\geq B \\ \dfrac{60*(G-B)}{\max(R,G,B)-\min(R,G,B)}+360, ha \max(R,G,B)=R, G<B \\ \dfrac{60*(B-R)}{\max(R,G,B)-\min(R,G,B)}+120, ha \max(R,G,B)=G \\ \dfrac{60*(R-G)}{\max(R,G,B)-\min(R,G,B)}+240, ha \max(R,G,B)=B \end{cases} \quad (1)$$

$$S=\begin{cases} 0 & ha \max(R,G,B)=0 \\ 1-\dfrac{\min(R,G,B)}{\max(R,G,B)} & ha \max(R,G,B)\neq 0 \end{cases} \quad (2)$$

$$V=\max(R,G,B) \quad (3)$$

A konverzió után már megfogalmazhatóak olyan küszöbözési feltételek, amelyek hatékonyan kihasználják az új színtérbeli reprezentáció előnyeit, pl.: fényintenzitás változás detekció. Kiegészítő szelekciós kritériumként a kontrasztgyengítést lehet megemlíteni, vagy az objektumok határvonalainak a halványítását.

Képi jellemző kinyerés

Az előfeldolgozott és szegmentált képek már közvetlenül alkalmasak lehetnek arra, hogy bizonyos algoritmusok felismerjék vagy kövessék az azokon látható objektumokat. A gyakorlatban azonban ez kevéssé jellemző, ugyanis még így is képpontok ezreit, netán millióit kell feldolgozni, ami a legtöbb módszer számára még mindig kezelhetetlen mennyiség.
A karakterisztikus jegyek számtalan hatékony, már-már standardnak tekinthető algoritmust ismert. A legtöbb módszer a szomszédos képpontok különbségén, azaz a „képfüggvény deriváltján" alapszik. Matematikailag viszonylag jól megfogalmazható, hogy milyen feltételeknek kell teljesülniük az éleken és a sarkokon található képpontokban. Szintén nem nehéz egyenes vonalakat, vonalak metszéspontjait, köröket és egyéb szabályos geometriai formákat megtalálni a képen.
Azonban az olyan nehezen definiálható objektumokat, mint egy aeroszol felhő, speciális algoritmusok segítségével lehet csak meghatározni. Ilyen speciális algoritmus lehet: az optical flow, vagy a polarizációs elven alapuló felhő detektálás.

Optical flow

Mozgó objektumok követése video felvételeken izgalmas kihívás a digitális képfeldolgozás terén. Egy képsorozatban minden egyes képpont követése igen nehéz feladat. A két legfontosabb probléma a számítás komplexitása (azaz a több millió képpont feldolgozása), valamint az, hogy legtöbbször nem is lehet egyértelműen megmondani, hogy mi a jó megoldás. Ez utóbbi első hallásra furcsának tűnhet, de sajnos, ami az embernek egyértelmű, az a számítógép számára nem az. Pl.: ha egy képsorozaton egy teljesen homogén, azaz egyszínű részt próbálunk lekövetni, az algoritmus nem képes megmondani, hogy milyen irányban mozognak a pixelek. Az ilyen eldönthetetlen helyzetek feloldására az optical flow algoritmusok bizonyos előfeltételekkel élnek, melyek – bár nem mindig állják meg a helyüket – lehetővé teszik a megoldást, ami természetesen nem biztos, hogy tökéletes lesz. Az egyik legfontosabb ilyen feltételezés az, hogy a szomszédos pixelek mozgása hasonló. Az optical flow gyakorlatilag egy irányokat tartalmazó képet jelent, ahol minden pixelhez hozzárendelünk egy 2 dimenziós mozgásvektort. Ha a kép pixeleit e vektorok mentén elmozgatjuk, akkor – elvileg – pontosan a következő képkockát kapjuk. Ezen vektorok kiszámítása nem képpontonként történik, hiszen ez egyrészt kezelhetetlenül lassú lenne , másrészt a homogén képrészekkel nem is tudnánk mit kezdeni. Hatékonyabb megközelítés, ha a képet blokkokra bontjuk – akár előfeldolgozás eredményeként megkapott foltszerű terület – és először ezek közötti elmozdulást figyeljük, majd rekurzívan a megfelelő ponton belüli mozgásokat térképezzük fel, az adott objektum újradarabolásával.

Polarizációs elven alapuló felhődetektálás

Ez egy igen kézenfekvő, viszonylag egyszerű eljárás. A módszer lényege, hogy feltérképezi a harcanyag felhőn keresztül, és a felhő környezetéből érkező fény irányát, polarizációs fokát, ezzel megkapva a teljes kép polarizációs mintázatát. Ennek segítségével adott időpontban megállapítható a képen a harcanyag felhővel fedett terület nagysága.
A Napból érkező fény a hullámhosszánál sokkal kisebb légköri részecskéken szóródik. Kevésbé szóródik a hosszabb hullámhosszú, vörös fény, és jobban a rövid hullámhosszú, kék fény. Polarizációkor a fénysugárra merőleges irányban poláros fény jön létre, azaz a

fényhullámnak lesz kitüntetett rezgési síkja. Ez történik akkor, amikor a napfény áthalad a felhőn. A felhők mögül érkező fény polarizációjának mértéke függ a napszaktól és attól, milyen irányból jön a sugár. A kép polarizációs mintázata azt jelenti, hogy a mérések során kapott fénypolarizáció eloszlását (fokát és irányát) színkódokkal térképesen ábrázolhatjuk. [4]

Felismerés, modell illesztés

A karakterisztikus jegyek azonosítása után általában nem több mint néhány száz leíró, avagy tulajdonság vektor tömöríti magába a feldolgozandó képi információt. Ez már sokkal kezelhetőbb, mint sok millió RGB képpont! Nem meglepő módon a gépi látás különböző alkalmazásai meglehetősen más és más módon dolgozzák fel ezt az információmennyiséget, de a két legnagyobb problémakör kétségkívül a felismerés és a modellillesztés.

A felismerés – legyen az célpont – a legtöbb esetben nem egy adott objektum felismerését jelenti, hanem egy – akár igencsak terjedelmes – adatbázisban, a legjobban illeszkedő elem megtalálását. Egy mérgező harcanyag felhőt permetező helikopter felismerése esetében ez azt jelenti, hogy a megtalált leírók sorozatát, azaz tulajdonság vektort kell összehasonlítani az adatbázisban található tulajdonság vektorokkal. A gyengébb rendszerek gyenge pontja legtöbbször a nem megfelelő leírók használata, illetve azok sikertelen és pontatlan detektálása. A felismerő rendszerek gyakran használnak tanuló algoritmusokat. Ez azt jelenti, hogy a téves és a sikeres felismerésből is tanul a rendszer, módosítja belső „állapotát”, így a továbbiakban egyre jobb felismerési valószínűséggel fog működni. Ezek a rendszerek nem is feltétlenül igényelnek kezdeti adatbázist, helyette be lehet őket tanítani. A tanuló rendszerek lelke legtöbbször egy neurális háló, ami – az agyunkhoz hasonlóan – nem más, mint elemi „kapcsolók”, neuronok igen nagy és összetett hálózata. A hálózat bemenete a tulajdonság vektor (leírók sorozata), kimenete pedig lehet akár egy, akár több igen/nem kapcsoló. A betanítás szakaszában különböző képeket „mutatunk” a rendszernek, és figyeljük a kimenetet. Megfelelően nagyszámú és tartalmú kép, valamint optimálisan kialakított háló és képi jellemzők használatával a rendszer képes lesz sikeresen felismerni azokat a képeket is, amelyek nem szerepeltek az eredeti tanító halmazban! Jellemzően akkor érdemes ilyen megközelítést alkalmazni, ha nem teljesen világos, hogy melyek a karakterisztikus jegyek, milyen tulajdonságok alapján lehet egyértelműen felismerni a cél-objektumot, mint például egy mérgezőanyag felhő. Természetesen nagyon körültekintően kell alkalmazni ezeket a tanuló algoritmusokat, hiszen sok olyan tényező van, ami befolyásolja a működést.

Az, hogy tudjuk, mi van a képen, azt jelenti, hogy rendelkezünk egy modellel, amely alapján meg tudjuk mondani, hogy kitalált paraméterek illeszkednek-e a mérésekhez, vagy nem. Az autonóm felderítő eszköz például, tudja, hogy körülbelül hogy néz ki egy adott haditechnikai eszköz többféle látószögből, és ezt össze is tudja hasonlítani a mérésekkel (azaz a légi felvételekkel). Ezek a feladatok is jellemző leírók detektálásával kezdődnek, az ismeretlen paraméterek kinyerése pedig általában két lépésben történik:

- Az első lépésben, ha mód van rá, speciális szabályok alapján megmondjuk, hogy körülbelül melyek a helyes paraméterek: nagyjából merre van a detektál felhő, hozzávetőlegesen hol áll a harcjármű stb.
- A második lépésben standard matematikai eszközökkel finomítjuk ezt a megoldást, azaz megkeressük azokat a paramétereket, melyek minimalizálják a különbséget a mért jellemzők, és a modell között.

A modellillesztés problémájánál is alkalmazhatóak tanuló módszerek.

Összegzés

„A vegyi pontfelderítésre széleskörűen alkalmazott ACADA (Automatic Chemical Agent Monitor – Automata vegyi ágens monitor) felváltására fejlesztik a JSLSCAD (Joint Service Lightweight Integrated Stand-off Chemical Agent Monitor – Egységes Könnyű integrált vegyi ágens távmonitor) műszert. Lehetőséget nyújt a passzív távfelderítő üzemmódra és képes menet közbeni kimutatásra is. Alapkiépítésében a rendszer súlya mintegy 20kg. A változó igényeknek megfelelően átalakítható. Páncélos járművekbe építhető változata ellátható 360° x60° tartományban üzemelő letapogatóval. Helikopterre, illetve pilóta nélküli légi járműre gömbcsuklóval szerelhető fel.”[3]
Tehát megállapítható, hogy az utóbbi évtizedekben a harcanyag felhő optikai mélység és a felszín visszaverő képességének vizsgálatára a passzív infra eszközök kerültek előtérbe, kis tömegük és hordozhatóságuk miatt.
Véleményem szerint az FTIR elven működő távérzékelőt hatékonyan ki tudja egészíteni a látható fény tartományban működő érzékelő rendszer (kamera+szoftver), kihasználva a képfúzió adta lehetőségeket, figyelembe véve az anyagi és technológiai lehetőségeket.
A Magyar Honvédség rendelkezik RAPID típusú távérzékelővel, mely alkalmazhatóságának területeit meg kell vizsgálni. Ezen vizsgálathoz kívántam lehetőségeket bemutatni, amelyek a számítógépes képfeldolgozásban rejlenek. Autonóm rendszerek, pl.: UAV kialakításánál a fentebb ismertetet algoritmusok célhardveren – FPGA (Field Programable Gate Array) alapú kártyákon – is megvalósíthatók.
A polarizációs elven működő távdetektálás nem csak egy RAPID típusú eszköz kiegészítése lehet, hanem olyan autonóm mérő állomásoké, mint amelyek az AMAR rendszert alkotják, ezáltal még teljesebb kép alakítható ki a környezetről, járulékos meteorológia adatok – égbolt felhő telítettsége – formájában.

FELHASZNÁLT IRODALOM

[1] RAPID Manual – HUN.pdf, 25. o.

[2] Dr. Halász László: Vegyi távfelderítő berendezések kifejlesztése az MH HTI-ben. Haditechnika 1993/1 2-8. o.

[3] Juhász László mk. őrnagy, Pintér István mk. alezredes: Az ABV felderítő eszközök fejlődési irányai a 21. század első évtizedében

[4] http://meteo21.blogter.hu/217248/magyar_felhodetektalo_muszer_az_elte-rol

[5] Gonzalez, Woods, „Digital Image Processing”, Addison-Wesley, 1993, 93-104 o.

[6] Sergyán Szabolcs, Color Content-based Image Classification, 5th Slovakian-Hungarian Joint Symposium on Applied Machine Intelligence and Informatics, January 25-26, 2007, 430 o.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Négyesi Imre
negyesi.imre@zmne.hu

INFORMATIKAI RENDSZEREK OKTATÁSA A KATASZTRÓFAVÉDELMI SZAKIRÁNYON

Absztrakt

Ez a publikáció a „Vegyivédelmi szolgálat létrehozásának 60. évfordulója” alkalmából szervezésre került tudományos konferenciára készült, és a meghirdetett témák közül a „Vegyivédelmi oktatás, kiképzés” témakörhöz kapcsolódik. Sokszor elhangzott már az a mondat, hogy az információs társadalom korában az élet minden területén használt informatikai rendszerek megkönnyítik a vezetői döntések meghozatalát és a döntésekben meghatározott feladatok végrehajtását. Ezt a mondatot figyelembe véve azt a célt tűztem ki magam elé, hogy rámutassak az információs és az informatikai rendszerek közötti különbségekre, valamint rávilágítsak arra is, hogy mekkora jelentősége lehet a leendő és a már szervezeti keretekben dolgozó katasztrófavédelmi szakemberek képzése során az informatikai rendszerek bemutatásának. Bemutatom mindezek mellett azokat a Magyar Honvédségnél követendő fejlesztési trendeket és stratégiákat, amelyből látható, hogy a Magyar Honvédség feladatrendszere rendkívül sokrétű, sok ponton kapcsolódik a civil szférához (pl. katasztrófavédelem) és mindezen feladatok végrehajtását különböző informatikai rendszerek segítik, amely rendszerek a civil szférában is felhasználhatók.

This publication got to organizing on the occasion of „The 60th anniversary of the chemical protection service's formation” onto a scientific conference been made, and from among the announced topics the chemical protection education, training are attached to a topic. That sentence was over already many times, that the informatics systems used on all of the areas of the life in the information society's age facilitate the making of the managerial decisions and the execution of the tasks defined in the decisions. This sentence I pinned it up taking that aim into consideration in front of myself in order to point at it the informational one and onto the differences between the informatics systems, and let me highlight his how large a significance the prospective one may be and in the course of the training of the specialists of catastrophe management working in organizational frameworks already for the presentation of the informatics systems. I present those development trends to be observed at Hungarian Defence Forces and strategies beside all these, from which visible, it concerns the civil sphere on many dots that Hungarian Defence Forces duty system is exceptionally manifold (catastrophe protection) and different informatics systems help in the execution of tasks on all this, that systems in the civil sphere utilizable.

Kulcsszavak: *informatikai rendszerek, informatika, információs rendszerek, tábori informatikai rendszer ~ informatics systems, informatics, informational systems, field informatics system*

BEVEZETÉS

Ennek a publikációnak és a hozzátartozó előadásnak a létrejöttét több tény indokolta. Az egyik egy általános össztársadalmi érdek, amelyet a Magyar Információs Társadalom Stratégiája (a továbbiakban MITS)[1] című dokumentumból levezethetünk. A MITS által megfogalmazott első cél, mindenki előtt világossá kell tenni, hogy Magyarország számára nincs más alternatíva, mint belépni az információs korba**,** annyira intenzíven és innovatívan, amennyire erőnkből telik. A jelenlegi témánkhoz kapcsolódik a MITS készítésének negyedik célja, amely célként tűzte ki azt is, hogy megvalósuló stratégiaként bebizonyítsa az informatika, az információs és kommunikációs technológia nem pusztán lehetőség, hanem hatékony eszköz. A MITS-ben megfogalmazásra került informatikai jövőkép természetesen nyomon követhető más stratégiákban is, amelyek közül csak egyet emelek ki.

A katasztrófavédelemről szóló 1999. évi LXXIV. törvény végrehajtását szolgáló jogszabályok körében megjelent a 48/1999. (XII. 15.) BM-rendelet, amelynek 10. § (1) c) bekezdése az OKF főigazgatójának feladataként határozza meg a Magyar Köztársaság katasztrófaveszélyeztetettségének elemzésén alapuló, a katasztrófák hatásai elleni védekezésre vonatkozó nemzeti stratégia kidolgozását. A megalkotásra került stratégiában az ún. egyes stratégiai elemek között szerepel többek között a megkövetelt létszámú és megfelelő szinten felkészített humánerő biztosítása, illetve a harmonikus információáramlás feltételeinek megteremtése is. Ez a két stratégiai elem, amelyre dolgozatomban kitérek, tehát a humánerő felkészítése a ZMNE-n és a megfelelő informatikai háttér biztosítása a feladatok végrehajtásához.

A másik indoka a publikáció megírásának személyes jellegű. Eredeti végzettségem szerint vegyivédelmi tiszt vagyok és ezáltal szívemen viselem a vegyivédelmi szolgálat jelenlegi tevékenységét is. A másik személyes ok, hogy a jelenlegi beosztásomban (ZMNE BJKMK Informatikai és Hírközlési Intézet, Informatikai tanszék, tsz. vez. h.) én kaptam azt a feladatot, hogy tantárgy-felelős oktatóként tanítsam a „Katasztrófavédelem informatikai rendszerei” című tantárgyat, amelynek tartalmáról a későbbiekben részletesebben is szólni fogok.

A harmadik ok, hogy szeretném bemutatni a Magyar Honvédség informatikai rendszereinek azon fejlesztési irányait és stratégiáit, amely fejlesztésekhez kapcsolódhatnak a katasztrófavédelemben használt informatikai rendszerek is. Mindezek mellett egy rövid kitekintést is teszek a más hadseregekben használt informatikai rendszerek felé, amely kitekintés egyben egy elérendő célt, egy jövőképet is jelenthet az informatikai rendszerek fejlesztéséhez.

Természetesen a publikációban szereplő elemek mindegyike csak egy figyelemfelkeltésnek tekinthető, amely bemutatja, hogy milyen elemekkel lehetne bővíteni a jelenleg oktatott tantárgyak belső tartalmát.

INFORMATIKAI TANTÁRGYAK A VÉDELMI IGAZGATÁS SZAKON

Az Informatikai tanszék döntése alapján a Védelmi igazgatási BSc és MSc szakon létrehozásra került új tantárgyak tantárgyfelelőse és egyben oktató tanára a kezdetektől fogva én vagyok. A tantárgyak a BSC képzésben a katasztrófavédelmi védelmi igazgatási

szakirányon „Katasztrófavédelmi informatikai rendszerek” (tantárgykód: ZNEBK104102) néven, az (önkormányzati) védelmi közigazgatási szakirányon „Önkormányzati informatikai rendszerek” (tantárgykód: ZNEBK104101) néven, a Védelmi igazgatási mesterszakon „Informatikai rendszerek” (tantárgykód: ZNEBK106111) néven kerülnek oktatásra a nappali és levelező képzésben egyaránt. Mindegyik tantárgy oktatásának fő célja, hogy a hallgatók ismerkedjenek meg a védelmi informatikai rendszerek, alkalmazások alapfogalmaival, főbb típusaival és azok jellemzőivel, valamint alkalmazási lehetőségeivel a katasztrófavédelemben.

Az eltérő óraszámok miatt jelentős eltérések lehetnek az oktatásra kerülő tananyag tekintetében. Az informatikai rendszerek, alkalmazások alapjai, a kapcsolódó alapfogalmak és a fejlesztési irányok, stratégiák mindhárom tantárgy esetében oktatásra kerülnek. A katasztrófavédelmi szakirányon ezen kívül rövid áttekintést nyújtunk a katasztrófavédelmi (általános veszélyhelyzet kezelési, nukleáris baleset-elhárítási, súlyos ipari baleset-kezelési, segélyhívó, viharjelző) informatikai rendszerekről és alkalmazásokról, a veszély- és katasztrófahelyzetek megelőzésének, kezelésének informatikai támogatásáról, a katasztrófavédelem informatikai rendszerével szemben támasztott követelményekről, a katasztrófavédelmi informatikai rendszerek, alkalmazások és adatbázisok helyzetéről Magyarországon és az Európai Unióban, valamint a katasztrófavédelem informatikai rendszerének fejlesztési irányairól. A önkormányzati szakirányon bemutatjuk az önkormányzatok felépítését, informatikai ellátottságát, az elektronikus szolgáltatások elterjedését, elérhetőségeit, szolgáltatásait, valamint szót ejtünk az adat- és titokvédelem jelentőségéről is. A MSc szakon tovább bővítjük a két BSc szakirányon már megszerzett ismereteket, konkrét rendszerek bemutatásával és külföldi példák ismertetésével.

A szűkös órakeretek (különösen a levelező tagozaton) azonban nem teszik lehetővé a téma átfogó vizsgálatát. A magas kurzus-létszámok miatt pedig gyakorlatilag mellőznünk kell a szemináriumok megtartását, amelyeken belül a személyes konzultációkon sok olyan kérdés felvetődhetne és megtárgyalásra kerülne, amelyek alapján a tapasztalatok összegzésével egy valóban a realitásokhoz közelítő jövőkép alakulhatna ki a hallgatókban a témával kapcsolatban. Az első probléma, amelynek tárgyalását nem kerülhetjük ki a vonatkozó (elsősorban NATO) irodalmak angolról magyarra történő fordítása során keletkezett. Konkrétan ez a problémakör az információs-rendszer és az informatikai-rendszer fogalmának meghatározásakor keletkezik, ami már azt is magával hozza, hogy tulajdonképpen már az oktatásra kerülő tantárgyak neve sem teljesen helytálló. (Természetesen a fogalmak meghatározása során fellépő ellentmondások a tantárgyi-tartalom pontosításával feloldásra kerültek.)

AZ INFORMÁCIÓS-, ÉS INFORMATIKAI RENDSZEREK FOGALMA

A kiindulási pontok az információs rendszerek és az informatikai rendszerek fogalmának meghatározása jelenti, amely meghatározásokhoz NATO dokumentumokat használhatunk. Az információs tevékenységeket megvalósító technikai rendszerekhez kapcsolódó fogalmak közé az information system, communication system, illetve a communication and information systems fogalmak tartoznak, amelyek definíciói a katonai szakirodalomban különböző változatokban fordulnak elő:

- „information system (IS): Eszközök, módszerek és eljárások, illetve működtető személyzet, információfeldolgozási funkciók megvalósítására létrehozott rendszere.”[2]
- „communication system (CS): Eszközök, módszerek és eljárások, illetve működtető személyzet, információátviteli funkciók megvalósítására létrehozott rendszere.”[2]

- „communication and information systems (CIS): A kommunikációs és az információs rendszerek – eszközök, módszerek és eljárások, illetve működtető személyzet információátviteli, illetve információfeldolgozási funkciók megvalósítására létrehozott rendszereinek – összefoglaló megnevezése.”[3]
- „communications and information system: Eszközök, módszerek és eljárások, illetve működtető személyzet meghatározott információtovábbítási és információfeldolgozási funkciók megvalósítására létrehozott rendszere.”[4]
- „communication and information systems (CIS): A kommunikációs és az információs rendszerek összefoglaló megnevezése."[2]

A hivatkozott szabályozókban szereplő fenti három fogalom magyar megnevezésére több változattal is találkozhatunk. A NATO kézikönyvek ezen kifejezések fordításakor az „információs”, illetve a „távközlési” jelzőket használják. Az AAP-31 magyar fordítása ugyanerre az „informatikai” és „információs”, illetve a „híradó” kifejezéseket tartalmazta, végül az AJP-01(A) változat magyar fordításában a „távközlési” és a „tájékoztató” jelzők szerepeltek. A magyar katonai szakirodalomban emellett egyre gyakrabban találkozhatunk a 'kommunikációs' jelző alkalmazásával is. A Magyar Honvédség alapvető doktrínáiban az „informatikai rendszer”, a „híradó rendszer”, illetve a „híradó és informatikai rendszerek” kifejezések kerültek elfogadásra és alkalmazásra. Az információs rendszer és az informatikai rendszer kifejezések a Magyar Honvédségen belül a korábbiakban eltérő tartalmú fogalmakat jelöltek. Az informatikai rendszer kifejezéssel a védelmi (katonai) informatika egy adott szervezet egészére, információfeldolgozási folyamataira és tevékenységeire, az ezt támogató eszközrendszerre és a közreműködő személyzetre vonatkozó fogalmat jelölt, míg információs rendszer alatt ezzel szemben a funkcionális szempontok által összetartozó információs tevékenységek, valamint az ezek megvalósítását támogató erőforrások összességét értette.

A NATO szóhasználatban is kimutatható ez a tartalmi kettősség, ugyanis az information system (IS) kifejezés egyaránt használatos egy teljes szervezet egységes „informatikai rendszerének” megjelölésére is. Mindezek alapján a magyar katonai informatikai terminológia megtartotta mindkét fogalmat (annak ellenére, hogy nem tartozik hozzájuk eltérő angol megnevezés), mert így eltérő kifejezéssel lehet megjelölni a Magyar Honvédség, vagy egy harckocsi zászlóalj informatikai rendszerét, vagy egy konkrét pénzügyi információs rendszert. (Ugyanakkor ez azzal a következménnyel jár, hogy konkrét angol megnevezések magyarra fordítása során a tartalom alapján kell eldönteni, hogy melyik magyar kifejezés használata a megfelelő.) A magyarról angolra történő fordítás során hasonló probléma nem merül fel, legfeljebb egyes esetekben megfelelő jelzők – (organizational) information system, vagy (functional) information system – alkalmazása válhat szükségessé.

Mindezek alapján kimondhatjuk, hogy a „köznapi” használatban az információs rendszerek és az informatikai rendszerek fogalmat ekvivalensnek tekinthetjük. Ez a tény egyúttal indokolja azt is, hogy miért használjuk az oktatott tantárgyak címében az informatikai rendszer kifejezést, de az oktatás során mindenképpen szükséges lesz rávilágítani a két fogalom közötti eltérésekre is.

INFORMATIKAI FEJLESZTÉSI IRÁNYOK ÉS STRATÉGIÁK

Magyar Köztársaság Nemzeti Katonai Stratégiája [5] kimondja, hogy a Magyar Köztársaság biztonságára – az Alkotmányban vagy egyéb jogszabályokban meghatározottak szerint katonai eszközöket vagy közreműködést esetlegesen igénylő – kockázatot jelenthetnek:

- az ország területén és környezetében előforduló ipari és természeti katasztrófák, környezetszennyezések, járványok;
- a kritikus infrastruktúra elleni támadások;
- az instabil országok belső feszültsége következtében kialakuló, a szervezett bűnözéssel összefonódó nagyobb méretű migráció és illegális kereskedelem;
- a térség egyes országaiban illegálisan, illetve ellenőrizetlenül tartott nagy mennyiségű fegyver, lőszer és robbanóanyag.

A stratégia kimondja továbbá, hogy a Magyar Köztársaság kormánya a biztonságot átfogó módon értelmezi, amely a politikai és katonai tényezőkön túl magában foglalja annak gazdasági, pénzügyi, energiaellátási, rendvédelmi, emberi jogi és kisebbségi, információs és technológiai, környezeti, demográfiai és civilizációs, közegészségügyi, valamint nemzetközi jogi dimenzióit is. A Magyar Köztársaság kormánya a biztonság-és védelempolitikát a különböző kormányzati intézmények közös feladatának tartja és ezen belül meghatározza a Magyar Honvédség feladatát.

A Magyar Honvédség a Magyar Köztársaság katonai védelme és a NATO kollektív védelméből fakadó feladatok ellátása, valamint a nemzetközi műveletekben való részvétel mellett:

- felkészülten közreműködik az arra kijelölt és felkészített erőkkel a nemzetközi terrorizmus elleni harcban a NATO és az EU koncepcióival összhangban;
- a magyar haderő hazai igénybevétele, valamint külföldi alkalmazása esetén képességeivel közreműködik, illetve hozzájárul a természeti és ipari katasztrófák elhárításához, a következmények felszámolásához, humanitárius vészhelyzetek kezeléséhez, otthonukat elhagyni kényszerültek evakuációjának támogatásához, a kitelepült személyek megsegítéséhez. Bizonyos esetekben szükségessé válhat a polgári erők és tevékenységek támogatása;
- biztosítja a két- és többoldalú nemzetközi katonai kapcsolatok fenntartását, fejlesztését, illetve a változó biztonságpolitikai helyzethez történő folyamatos adaptálását, a szükséges információk elérhetőségét és azok cseréjét, megosztását, a kölcsönös kiszámíthatóság és hitelesség erősítését;
- hozzájárul a béke és biztonság fenntartásához, a szerződő felek közötti bizalom erősítéséhez a fegyverzet- ellenőrzésről, a bizalomerősítésről szóló nemzetközi egyezményekben és más megállapodásban foglalt kötelezettségek teljesítéséből a Magyar Honvédségre háruló feladatok végrehajtásával.

Mindezen feladatok végrehajtása érdekében képességalapú haderőfejlesztést kell megvalósítani, amely lehetővé teszi a hatékony reagálást a biztonsági környezet változásaira. Ezen belül a hadfelszerelés fejlesztésének legfontosabb feladatai:

- a tábori híradó és informatikai rendszerek rendszerszemléletű fejlesztése, a hálózatalapú működés kialakításának biztosításával;
- a szárazföldi erő mobilitásának, védettségének és tűzerejének növelése;
- a meglévő helikopterek modernizációja és újak beszerzése;
- a stratégiai légi szállítókapacitás biztosítása;
- a katonák egyéni felszerelésének korszerűsítése;
- a technikai felderítőeszközök rendszerbe állítása.

A törvényi meghatározásokból egyértelműen kitűnik, hogy a Honvédelem nem csak a Magyar Honvédség feladata, ezért ha már működő informatikai rendszereket, vagy azok jövőbeni fejlesztésének lehetőségeit vizsgáljuk ezt csak az alapfogalmak egységes értelmezése mellett tehetjük. Ez is indokolta tehát az előző fejezetben leírt meghatározásokat, amelyeket a Magyar Honvédség, egyetértésben a NATO szabványokkal, használ és egyben indokolja a katasztrófavédelmi szakirányon oktatott tantárgyak létjogosultságát is.

TÁBORI INFORMATIKAI RENDSZEREK

A Magyar Honvédség infokommunikációs rendszereinek kialakításához, a rendszertechnológia területén meg kell ismerkednünk a „közműszerű IT-szolgáltatás" fogalmával, mert ez jelenti a fejlesztési trendek fő irányát. A közműszerű IT-szolgáltatás úgy határozható meg, mint egy olyan stabil, megbízható, gyakran a szolgáltatás minőségére vonatkozó megállapodásokkal külön is garantált, tömegigényeket kielégítő (ezért költséghatékony) szolgáltatása az informatikai kapacitásoknak és funkcióknak, amely mögött korszerű, hatékonyan működtetett IT-infrastruktúrák állnak.

Kapcsolódó fogalom az informatikai közmű fogalma, amely magában foglalja a következőket:

- Infrastrukturális közmű: az infrastruktúra-hosting (hosting infrastructure services, HIS) vagy rendszerinfrastruktúra üzemeltetés (System Infrastructure Service Provision, SISP),
- Szoftverközmű: az alkalmazás-hosting vagy alkalmazásüzemeltetés (application service provision, ASP)

A mikroelektronika forradalma, a személyi számítógépek megjelenése, majd ezt követően az informatikai eszközök korábban elképzelhetetlen, máig nem lassuló elterjedése azzal a következménnyel járt, hogy az információtechnológiai fejlődés során a katonai alkalmazás az élenjáró, kiemelt szerepét nagyrészt elvesztette és a legtöbb területen követő szerepbe kényszerült. Napjainkban a minőségi és hatékonysági követelmények teljesítése már elsősorban a kereskedelmi forgalomban kapható[1] informatikai eszközökre, megoldásokra alapozva lehetséges.

Azonban nem minden eszköz kapható kereskedelmi forgalomban, ezért a Magyar Honvédségen belül a legjelentősebb fejlesztési irányt, ahogyan az a Magyar Köztársaság Nemzeti Katonai Stratégiájából is kiolvasható a tábori híradó és informatikai rendszerek fejlesztése jelenti. Mindezek a tábori informatikai eszközök olyan speciális kivitelű informatikai eszközök, amelyek sajátos megoldásai többek között elsősorban olyan környezeti feltételek, veszélyeztetések következményeinek csökkentését, kiküszöbölését szolgálják, mint: leejtés, rázkódás (vibráció), kiömlő folyadék, különböző környezeti tényezők káros hatásai, elektromágneses hatások, tehát minden olyan külső (elsősorban meteorológiai) hatás, csapadék (eső, hó, jégeső, stb.), szél, köd, por, homok, rendkívül magas, vagy alacsony hőmérséklet, hirtelen hőmérsékletváltozás, nyirkosság (nedvesség, páratartalom), sókicsapódás, stb. Kibírják a víz alá merülést, a jégtömbbe zárást, működőképesek maradnak extrém terepen mozgó járművön. Tehát kibírnak minden olyan hatást, amely előfordulhat egy műveleti területen történő feladat-végrehajtás során.

[1] Commercial-off-the-shelf (COTS) = "polcról levehető"

Az informatikai rendszerek szempontjából, ezért három különböző fejlesztési irányt különböztetünk meg, amelyek mindegyike kapcsolódik a civil szférához is és ennek megfelelően kapcsolódik a katasztrófavédelemhez is. Ez a három főirány: [6]

- a tábori körülmények között telepített;
- a harcjárművekben, gépjárművekben telepített;
- és az egyes katonákat közvetlenül támogató, egyéni informatikai eszközök.

A tábori (telepített/áttelepülő) vezetési pontokon történő alkalmazási mód alapvetően a háborús katonai műveletek esetében jellemző, de – különösen alacsonyabb vezetési szinteken – előfordulhat válságreagáló műveletekben is. A tábori körülmények közötti alkalmazás, az irodai alkalmazástól eltérő környezeti feltételek sajátos követelményeket támasztanak az informatikai eszközökkel szemben is. Mivel egy adott katonai szervezet alkalmazására sor kerülhet különböző körülmények között, így informatikai eszközrendszerének egyaránt alkalmazhatónak kell lennie hosszabb időszakra telepített, vagy időszakonként történő áttelepítés esetében is.

A harceszközökben, harcjárműveken történő alkalmazás két különböző, egymástól rendeltetésében és megoldásaiban is eltérő formában lehetséges. Az első csoportot az eszközökben, járműveken és azokon kívül egyaránt alkalmazható, önálló informatikai eszközök képezik, amelyek alapvető képességeiket és jellemzőiket tekintve azonosak a tábori vezetési pontokon, vagy az egyes harcosok által alkalmazott eszközökkel. Ezek rendeltetése, felhasználása és funkciói lényegében függetlenek a hordozóeszköztől. A második csoportba az adott eszközökbe, járművekbe beépített azon eszközök képezik, amelyek rendeltetése elsődlegesen a harceszköz alaprendeltetés szerinti működéséhez kapcsolódik. Ezek közé többek között különböző információgyűjtő (érzékelő), információtovábbító (kommunikációs), illetve a fegyverrendszer/eszközrendszer kezelésében, a harcvezetésben, valamint a helyzetismeret fenntartásában szerepet játszó információ,-beviteli, feldolgozó és megjelenítő eszközök tartoznak.

Mindezek a tábori informatikai eszközök olyan speciális kivitelű informatikai eszközök, amelyek sajátos megoldásai többek között elsősorban olyan környezeti feltételek, veszélyeztetések következményeinek csökkentését, kiküszöbölését szolgálják, mint: leejtés, rázkódás (vibráció), kiömlő folyadék, különböző környezeti tényezők[2] káros hatásai, elektromágneses hatások. A káros hatásokkal szembeni ellenállóságnak különböző szintjei lehetnek, ennek megfelelően általában három kategóriát különböztetnek meg.

A részben ellenálló (semi-rugged, ruggedized) készülékek túlnyomó többségében kereskedelmi forgalomban kapható részegységekből álló készülékek, amelyeket célirányosan és lényeges mértékben módosítottak a speciális körülmények között történő felhasználás céljaira. A teljesen ellenálló (fully rugged) eszközök teljes egészében és minden összetevőjükben, sőt azok elhelyezésében is a speciális körülmények közötti alkalmazásra lettek kialakítva. Végül a kiemelten ellenálló (ultra rugged) eszközök különösen extrém körülmények között[3] is tartósan működőképesek.

A harmadik fejlesztési irányt az egyes katonákat, harcosokat közvetlenül támogató alkalmazások jelentik, amelyek egyik legfontosabb sajátossága, hogy az informatikai funkciókat, szolgáltatásokat biztosító eszközöket a felhasználónak – a települési helyét, harc- vagy szállítójárművét elhagyva – magával kell vinnie, magán kell viselnie, személyes

[2] Csapadék (eső, hó, jégeső, stb.), szél, köd, por, homok, rendkívül magas, vagy alacsony hőmérséklet, hirtelen hőmérsékletváltozás, nyirkosság (nedvesség, páratartalom), sókicsapódás, stb.

[3] Kibírják a víz alá merülést, a jégtömbbe zárást, működőképesek maradnak extrém terepen mozgó járművön.

felszerelésének részét kell képeznie. Hasonló igények számos, nem katonai alkalmazási területen (pld. rendőri járőrözés, határellenőrzés, katasztrófa-elhárítás, geodéziai felmérések, helyszíni hibaelhárítás) is felmerülnek, azonban ezeket a speciális (terepi) kivitelű, sőt egyre inkább a hagyományos notesz,- vagy kézi-számítógépek általában kielégítik.

INFORMATIKAI BIZTONSÁG

Ebben a fejezetben egy olyan kapcsolódó témával foglalkozom, amelynek oktatása sajnos nem szerepel a katasztrófavédelmi szakirány tantárgyi listájában, ugyanakkor nagy szükség lenne az oktatására.

Életünkben egyre nagyobb szerepet játszanak a számítógépek és az azokat hálózatba kötő telekommunikációs rendszerek. A munkavégzést és az életet irányító információk számítógépes rendszerekre kerülnek, így a tőlük való függés egyre nagyobb és nagyobb lesz. A világhálózat, az Internet terjedésével a kommunikáció és a világban való tájékozódás módja is megváltozik. Ebben a cyberspace-nek nevezett világban az információ valódi értékké vált, és annak védelme elengedhetetlen.

A számítógépes rendszerek bonyolultsági foka egyre inkább nő. Még a legjobb szakemberek sem ismerik részletekbe menően a pontos működési mechanizmusokat, így rendkívül nehéz arról meggyőződni, hogy egy rendszer tényleg úgy működik-e, ahogy kellene, valóban biztonságos-e. Egy átlagos felhasználó, aki még ennyire sem ismeri a számítógépet, nehezen tudja eldönteni, hogy egy adott rendszert használva mennyire van kiszolgáltatva a számítógépen keresztül rosszindulatú embertársainak. Ezen felül az egyes természeti tényezők (tűz, víz, villámcsapás...) és a hardver-meghibásodások is komoly fenyegetést jelentenek a rendszer folyamatos működésére nézve, az adatok megsemmisülése mindennapos veszély. Ez a bizonytalanság bizalmatlanság kialakulásához vezet, és jelentős negatív hatása van a számítógépes rendszerek terjedésére.

A kiindulásnak tekinthető biztonság, mint fogalom pontos meghatározása nehéz. Különböző szituációkban különbözőképpen értelmezhetjük. A fő értelmezési gondot talán az időbeliség furcsa megfogalmazása jelenti. Általában arról beszélünk, hogy valami biztonságban van, és ezalatt mégis azt értjük, hogy a – közeli vagy távolabbi – jövőben nagy valószínűséggel nem történik vele semmi rossz. Illetve ha netán mégis történne, akkor azt valahogyan ki tudjuk küszöbölni, és a jó állapotot rövid időn belül vissza tudjuk állítani. Megpróbálunk olyan események ellen felkészülni, amelyek eddig még nem is biztos, hogy megtörténtek, és ha meg is történtek nagyon ritkán, az előfordulási gyakoriságuk kicsi. Ezért elméletileg sem várható el egyetlen rendszertől sem, hogy teljesen, 100%-ig biztonságos legyen, hiszen a ritka, kiszámíthatatlan, előre nem látható eseményeket nem lehet teljes körűen számba venni. Az informatika körében a biztonság különösen összetett, ugyanis itt nem elegendő, hogy egy rendszer jó, működőképes állapotban maradjon, hanem azt is meg kell gátolni, hogy bizalmas információk a rendszeren kívülre jussanak. Ezt a követelményt hagyományos fizikai fogalmakkal nem tudjuk leírni, a logikai követelmények teljesülését pedig nagyon nehéz igazolni.

A biztonság fogalmával szorosan összekapcsolódik, de egyben élesen el is válik tőle a biztonságérzet és a veszélyérzet fogalma. Aki nem törődik a biztonsági kérdésekkel, azt előbb-utóbb komoly kár fogja érni. Ennek eredményeképpen nem fog megbízni a számítógépekben, csak félve, korlátozottan fogja tudni azokat használni, ami így vagy úgy, de a munka hatékonyságának kárára megy majd. Ezért rendkívül fontos az informatikai

biztonság oktatása, a tudatos veszélyérzet és a megfelelő, megalapozott biztonságérzet kialakítása.

Míg a biztonság fogalma pozitív oldalról közelíti meg a kívánt állapotot, addig a kockázat gyakorlatiasabb szemlélettel dolgozik: egy adott rendszert fenyegető veszélyeket veszi számba, és az általuk okozott károkat próbálja megbecsülni, összegezni. Gyakorlati szempontból a kockázat nem más, mint adott idő alatt a rendszert ért nem kívánatos eseményekből keletkező kár várható értéke. Informatikai rendszerek esetén – mivel a károk áttételesen továbbterjednek, és ez a hatás nehezen mutatható ki pénzben – a kockázat pontosan nem állapítható meg a gyakorlatban. Ezért inkább csak kockázatbecslést szoktak alkalmazni. Minden nehézség ellenére, az egyes fenyegető tényezők kockázatbecslése azért az informatikai biztonság területén is jól kijelöli azon leggyengébb láncszemeket, ahol a védelmet célszerű erősíteni. Azt szokás mondani, hogy a biztonság nem más, mint tudatos kockázatvállalás. Sokkal jobb ugyanis félni, mint megijedni, azaz jobb az ismert veszélyeket – mérlegelve a védekezés költségeit – tudatosan felvállalni, mint a veszélyeket meg sem ismerni.

A magyar szakmai szóhasználatban élesen elkülönül egymástól az adatbiztonság és az adatvédelem fogalma. Az adatvédelem a személyes adatok jogi értelemben vett (törvényekkel, szabályzatokkal való) védelmét jelenti, míg az adatbiztonság fogalma magát a technikai védelmet fedi. (Például az üzleti titkok védelméről szóló törvény az adatvédelem témaköréhez tartozik, míg a rejtjelezési algoritmusok az adatbiztonság fogalomköréhez kapcsolódnak.) Szokás még a számítógépes rendszerek és a bennük tárolt információk biztonságát informatikai biztonságnak is nevezni. Ez utóbbi az információk sértetlenségével, bizalmasságával éa rendelkezésre állásával foglalkozik. [7]

Mind a felhasználók, mind a gyártók részéről jogos igény, hogy a biztonsági termékeket objektív módon össze lehessen hasonlítani, azok biztonsági szintje valamilyen módszerrel mérhető legyen. Ennek az igénynek a kielégítésére több nemzeti és nemzetközi szervezet is elkészítette a maga kritériumrendszerét, amellyel az egyes termékek úgynevezett biztonsági osztályokba sorolhatók. A besorolást minden esetben egy független testület végzi, amely garancia a megítélés objektivitására. A követelményrendszereknek való megfelelőség elbírálása során általában nem a végterméket vizsgálják, hiszen egy összetett számítógépes rendszerben a hibakeresés negatív eredménye még nem garantálná a biztonságot (attól, hogy adott idő alatt nem találtak hibát, még könnyen lehet akár súlyos biztonsági rés is egy rendszerben). Ezért inkább a fejlesztés folyamatát, az abba épített védelmi, ellenőrző mechanizmusokat minősítik. Ennek megfelelően a biztonsági minősítések az alkalmazott védelmi eljárásokon, biztonsági funkciókon túl, alapvetően a fejlesztés minőségbiztosítását vizsgálják illetve osztályozzák.

A fenti fogalomkörök jól rávilágítanak arra, hogy az informatikai biztonság témakörét milyen sok különböző irányból lehet megközelíteni. Ahhoz, hogy a biztonságot kezelni tudjuk, hogy valós alapokon nyugvó biztonságérzetet illetve bizalmat alakítsunk ki, fontos a fenti főbb irányelvek megértése és az alapvető, hosszabb távon is igaz szabályszerűségek illetve működési mechanizmusok megismerése.

A biztonság fogalmát szokás további részfogalmakra bontani a pontosabb megfogalmazás és kezelhetőség kedvéért. Az egyik ilyen széles körben elfogadott megközelítés a biztonságosságot a

- bizalmasság (confidentiality)

- sértetlenség (integrity)
- rendelkezésre állás (availability)

követelményekkel jellemzi. (Az angol kifejezések kezdőbetűinek összeolvasásából erre a módszertanra CIA követelményrendszerként szokás hivatkozni.)

A bizalmasság követelménye azt rögzíti, hogy egy adott információt csak az arra jogosultak ismerhetnek meg. Ezt az ideális követelményt a gyakorlatban árnyaltabban úgy fogalmazhatjuk meg, hogy illetéktelen személy csak aránytalanul nagy erőbefektetéssel, költséggel, vagy aránytalanul kis valószínűséggel legyen képes az adott információhoz hozzájutni. A bizalmasság biztosítására szokás hozzáférés-védelmi rendszereket és/vagy rejtjelezési eljárásokat használni, amelyek gyakorlatilag kizárják az illetéktelen személyek hozzáférését az adott információhoz (amennyiben a rejtjelkulcs titkossága biztosított).

A sértetlenség követelménye azt rögzíti, hogy egy adott információt vagy rendszert csak az arra jogosultak változtathatnak meg. Mivel az elektronikus adatok módosítását megakadályozni gyakorlati nehézségekbe ütközik (az üzenetek a zaj következtében akár véletlenül is módosulhatnak a hálózaton áthaladva), ezért a hangsúly a sértetlenség esetében tipikusan a módosítás észlelésén, illetve javításán van. A sértetlenség követelményéhez szorosan kapcsolódik az adatkonzisztencia, a hitelesség és letagadhatatlanság fogalma is. A sértetlenség biztosításához a bizalmasságnál említett eljárások, hozzáférésvédelmi rendszerek, illetve a kriptográfia módszerei (tipikusan digitális aláírás) alkalmazhatók elsősorban, de ebbe a körbe tartozik a víruskereséstől a konzisztencia-vizsgálatig terjedő védelmi megoldások széles tárháza is.

A rendelkezésre állás követelménye azt rögzíti, hogy egy adott rendszernek milyen megbízhatósággal kell ellátnia a feladatát. Ez a fogalom körülírható olyan objektív statisztikai jellemzőkkel, mint az üzemidő, a rendelkezésre állási tényező és a sebezhetőségi ablak. Mivel a rendelkezésre állást véletlen események (meghibásodás, tűz, víz, betörés) is fenyegetik, de akár támadók tevékenysége sem zárható ki, a fenti statisztikai jellemzők garantálása érdekében határozott védelmi intézkedéseket kell megtenni.

Egy rendszeren belül a legnagyobb veszélyforrást általában a belülről érkező támadások jelentik. Egy szervezeten belül az ilyen támadások elkövetői jellemzően belső munkatársak, vagy a támadást azok segítségével hajtják végre, ezért rendkívül fontosak azok a technikai védelmeken túlmutató intézkedések, amelyek az úgynevezett humán biztonság megteremtésére irányulnak. Sok esetben ezek egyszerű alapelvek, amelyek betartása adott esetben kényelmetlennek tűnik, de hosszú távon egyértelműen meghozza gyümölcsét.

A tapasztalat szerint komoly veszélyt jelent, ha egy személynek olyan jogosultságai vannak, amellyel mások engedélye, illetve tudta nélkül végrehajthat visszaéléseket. Ilyenkor aztán akár hosszabb időn keresztül folytatólagosan is elkövethetőek olyan mértékű visszaélések, amelyek sokáig rejtve maradhatnak. Tipikus összeférhetetlen jogkör például egy rendszer fejlesztője – aki módosításokat eszközölhet egy programban – illetve annak üzemeltetője – aki használja az adott rendszert –, ugyanis a program módosításával szinte bármit megtehet a rendszerfejlesztő, bármilyen visszaélés nyomait leplezni képes, ha a működtetést is ő figyeli. (Ilyen összeférhetetlen jogkörök lehetnek a pénzügyi utalványozást előkészítő és azt jóváhagyó, a hozzáférési jogosultságokat állító adminisztrátor és a rendszer felhasználója, az adatbázis adminisztrátor és az adatfeltöltő, illetve általában egy kritikus műveletet elvégző és az azt jóváhagyó, engedélyező szerepköre.

Bár sok esetben jóval egyszerűbbnek, kényelmesebbnek tűnik, hogy ugyanaz a személy oldjon meg egymásra épülő feladatokat, nem szabad ezt a kompromisszumot megkötni, hanem biztosítani kell, hogy összeférhetetlen szerepköröket különböző személyek lássanak el. Az előbbiekben röviden ismertetett elveknek a konkrét megjelenése a katasztrófavédelmi feladatok végrehajtása során is biztosra vehető. Ugyanakkor én magam azért nem írtam konkrét példát az elvek mellé, hogy ezzel is jelezzem az órai szemináriumok egyik esetlegesen megtárgyalandó kérdéskörét.

A feladatok hatékony módon történő végrehajtásának elengedhetetlen feltétele, hogy az információk áramlása, vagyis a biztonságos kommunikáció létrejöjjön. Amikor két távoli fél biztonságosan szeretne kommunikálni egymással, a konkrét esetektől függően jelentősen eltérő követelmények állhatnak elő. Az, hogy mit tekintünk biztonságosnak, mindig az adott helyzeten múlik. Előfordulhat például, hogy a másik fél megbízható azonosítása alapkövetelmény, de lehet, hogy éppen az anonimitás (a személyazonosság elrejtésének) biztosítása a kulcskérdés.

A lényegesebb biztonságos kommunikációt jellemző tulajdonságok, illetve követelmények a következőek:

- **Biztonságos nyugtázás:** Annak garantálása, hogy két fél egy kritikus művelet, úgynevezett tranzakció végrehajtásáról (pl. bankátutalásról) úgy meg tudjon győződni, hogy mindkét fél végrehajtottnak, vagy mindkét fél félbeszakadtnak tekintse az adott tranzakciót, azaz felemás, vagy bizonytalan állapot ne fordulhasson elő. Látni fogjuk, hogy egy intelligens támadó esetén, ha az a nyugtázási protokollt (a nyugtázás üzeneteinek sorrendjét, szabályrendszerét) ismeri, csak egy megbízható harmadik fél bevonásával oldható meg e követelmény teljesítése. Bizonyítható, hogy nem készíthető olyan protokoll, amellyel pusztán két fél egymás között meg tudna egyezni egy közös tranzakció végrehajtásáról.
- **Sértetlenség:** Annak garantálása, hogy hibamentesen (változás nélkül) ér célba egy elküldött üzenet, vagy legalább is egy esetleges módosulás felismerhető, mert ekkor még mindig elküldhető újra a helyes üzenet.
- **Hitelesség:** A sértetlenség önmagában még nem garantálja, hogy az üzenetet valóban az küldte, akit feltételezünk, pusztán azt, hogy az üzenet a hálózati továbbítás során nem sérült. A hitelesség a sértetlenségen felül a *vevő fél felé* azt is garantálja, hogy az adott üzenet a feltételezett küldőtől származik, és annak tartalma nem módosult.
- **Letagadhatatlanság:** A letagadhatatlanság a hitelességnél annyival több, hogy ez esetben nemcsak a vevő felé, hanem *tetszőleges harmadik személy felé* is igazolható, hogy egy adott üzenetet (megrendelést, nyilatkozatot) a valódi küldő küldte, tettét letagadni nem tudja. A vevő felé biztosított hitelesség biztosítható olyan, úgynevezett szimmetrikus aláírással is, amely esetben az aláírást mind a küldő, mind a vevő el tudja készíteni. Ekkor a vevő tudja, hogy az aláírást nem ő készítette, így biztos lehet benne, hogy az csak a küldőtől származhat. Külső fél felé azonban ezt nem tudja bizonyítani, hiszen nincs garancia arra, hogy az aláírást nem ő készítette el. A letagadhatatlanság követelményét csak az úgynevezett aszimmetrikus vagy nyilvános kulcsú kriptográfia módszereivel lehet biztosítani, amikor már egy harmadik fél felé is bizonyítható, hogy az aláírást ki készítette.
- **Bizalmasság:** A biztonságos kommunikáció fogalmán legtöbben a bizalmasság, vagyis a titkosság biztosítását értik. Kriptográfiai módszerekkel ugyanis elérhető, hogy olyan formában kódolva továbbítódjon egy üzenet, hogy azt egy

támadó lehallgatva, a titkos kulcs ismerete nélkül ne értse meg, illetve szigorúbb esetben magának az üzenetnek a tartalmára még valószínűségi alapon se tudjon következtetni.

- **Távoli azonosítás:** Amennyiben két fél személyesen még nem találkozott, illetve kettejük között nincs biztonságos (manipulálhatatlan, lehallgathatatlan) csatorna, amely szerepet személyes találkozó esetén a levegő tölthetne be, akkor egyéb módszerekkel, tipikusan külső szereplő(k) bevonásával kell biztosítani, hogy őket egymásnak biztonságosan mutassák be, és a későbbiekben hitelt érdemlően tudják egymást azonosítani. Gyakorlatban a távoli azonosítást az úgynevezett elektronikus igazolványok rendszerével, illetve ezen igazolványok hitelességét biztosító PKI[4] infrastruktúrával oldják meg.
- **Anonimitás:** Bizonyos alkalmazások esetén az azonosítással ellentétesen éppen az anonimitáson, a kommunikáló fél személyazonosságának elrejtésén van a hangsúly. Például senki nem szeretné, ha bankja vásárláskor nyomon követné, miket vett, hiszen ez már nem a pénzintézet hatásköre, de hasonló problémákat vet fel a titkos szavazások megvalósítása is. Az anonimitás több szinten biztosítható (a visszakövethetetlen szinttől az álnevekig), mely szintekhez más és más módszerek tartoznak.

A fenti szempontokon túl további elvárások is megfogalmazhatóak a biztonságos kommunikációval szemben, mint például a forgalom titkossága (azt se lehessen kideríteni, hogy ki, kivel, mennyit kommunikál) vagy akár az elárasztásos támadással[5] szembeni védettség. A biztonságos kommunikáció feltételrendszere így rendkívül összetett. Fontos tehát minden építőelemével pontosan tisztában lenni, és mindig az adott alkalmazásnak legjobban megfelelő megoldást alkalmazni.

Összefoglalva egy kommunikáció biztonsága többek között a következő szempontok szerint ítélhető meg: biztonságos nyugtázás, sértetlenség, hitelesség letagadhatatlanság, bizalmasság, felek azonosítása, vagy éppen a biztosított anonimitás. Mivel a különböző alkalmazások jelentősen eltérő követelményeket fogalmazhatnak meg a „biztonságos kommunikációval" szemben, ezért fontos, hogy az egyes jellemzőket pontosan megfogalmazzuk, és azokra építve határozzuk meg egy adott esetben a már pontosított követelményeket.

Még egy témát kell röviden érintenünk a felhasználó-azonosítást, mert az minden informatikai biztonsági rendszer alapja. Bármilyen szabályt, bármilyen védelmet csak arra építve lehet készíteni, hogy a felhasználókat megfelelő megbízhatósággal azonosítani lehet. Sajnos azonban pont ez a funkció az, amelyet kellő biztonsággal megvalósítani nehéz, így a legtöbb esetben ez jelenti egy rendszer leggyengébb pontját. Ezért aztán precíz kidolgozására különös gondot kell fordítani. A felhasználók azonosítása alapvetően három módszerrel oldható meg: tudás, birtok és biometria alapú eljárással. Mivel mindhárom módszernek vannak gyenge pontjai, ezért a biztonságos azonosításhoz legalább két módszer együttes és egymástól független alkalmazása javasolt.

Nézzük meg, hogy milyen azonosítási alapmódszereket ismerünk. Egy személyt több jellemzője alapján is azonosítani lehet. A különböző lehetséges azonosítási elvek közül három alapmódszer alakult ki az informatikai rendszerek esetében: egy felhasználót az alapján azonosíthatunk, hogy mit tud, mi van nála, illetve hogy fizikai-biológiai értelemben kicsoda.

[4] Public Key Infrastructure = nyilvános kulcsú infrastruktúra

[5] denial-of-service attack

Mindegyik módszernek megvannak az erősségei és gyengéi. A kellő biztonsági szint eléréséhez ezért azt szokás mondani, hogy együttesen (egy időben, egyszerre) kell legalább két, eltérő elven alapuló módszert egymástól függetlenül alkalmazni. A függetlenség kihangsúlyozása azért fontos, mert az egymástól függő megoldások nemhogy erősítenék, de még akár gyengíthetik is egymás hatását.

Az alkalmazott módszereket használhatóságuk, áruk és egyéb tulajdonságaik alapján jellemezhetjük.

A tudás avagy jelszó alapú azonosítás olyan információra épül, amelyet kizárólag a védelem tárgyához jogosult személyek ismernek, tehát voltaképpen arra, hogy egy-egy felhasználó mit tud. Előnyös, hogy használata egyszerű, olcsó, de hátrányos, mert a tudás észrevétlenül másolható és tulajdonítható el és igazán erős védelmet jelentő jelszavak megjegyzése az ember számára nehéz.

A birtok avagy kulcs alapú azonosítás a felhasználó birtokában lévő tárgyra épül, vagyis arra, hogy a felhasználónak mije van. A kulcs megvalósítása lehet fizikai jellegű (hasonlatos akár ahhoz, amely a lakásunk bejáratát zárja) vagy lehet egy logikai bitsorozat, azonban ami igazán fontos, hogy szerkezetét, felépítését tekintve más tárgyaktól jól megkülönböztethető legyen. Előnyös módszer, mert a használata általában egyszerű, az olcsótól a drágáig terjednek az árak, de hátrányos, mert eltulajdonítható és védekezni kell a másolás.

A biometria alapú azonosítás a felhasználó valamilyen tulajdonságára épít, közvetlenül azt vizsgálja, hogy a felhasználó fizikai-biológiai voltában kicsoda. Előnyös, hogy egyes esetekben nehézkes, de megfelelő megvalósítás esetén nagyon megbízható, de hátránya, hogy az egyszerű megvalósítások általában könnyen kijátszhatóak, a komoly megvalósítások (például a vizsgált minta élőségének megállapítása) drágák, illetve jogi, adatvédelmi (például biometrikus adatok tárolásának helye, módja) és egészségügyi (higiénia) problémái is felléphetnek.

Tekintve, hogy mindegyik felhasználó-azonosítási módszernek vannak kiküszöbölhetetlen, eredendő hiányosságai (a jelszavak leolvashatóak, megtévesztéssel kicsalhatóak, kitalálhatóak; a kulcsok ellophatóak, másolhatóak; a biometria megtéveszthető), nem elegendő egyetlen azonosítási módszer alkalmazása a kellő biztonság szavatolásához, hanem javasolt a módszerek egyidejű, de mégis független kombinációja.

JÖVŐKÉP!?

A előző fejezetekben leírt fejlesztési trendek, a tábori körülmények között is használható informatikai eszközök és különösen az informatikai védelem megvalósítása természetesen rendkívül költségigényes. Ebben a fejezetben mintegy zárásként bemutatok két új eredményt, amelyet az amerikai hadseregben fejlesztettek ki. Az első egy új harci öltözet, amelyet negyven katona próbált és elsősorban az uniformisok digitális hálózatát tesztelték, vagyis azt, hogy harci körülmények között miként tudnak egymással kommunikálni a katonák. (Természetesen nem véletlen a fejezet címében a „?!”, hiszen látható, hogy a költségek miatt a Magyar Honvédségben és a katasztrófavédelmi szervezetekben a fejlesztések sokkal inkább az „álom” kategóriába tartoznak.)

A fő hangsúlyt a katonák biztonságára helyezték, hiszen a golyóálló mellény ezúttal tíz százalékkal nagyobb lett, a harcosok oldalát is védi, sőt, a has alsó tájait is, és nem utolsó sorban valóban golyóálló. Ez a felszerelés ellenáll minden gépfegyver tüzének, mégpedig a

kerámia páncél miatt, és a fejlesztők szerint lehetséges, hogy a becsapódás okozta ütésektől a katona elesik, azonban a testét nem érinti a golyó. Az amerikai hadsereg eddig 150 millió dollárt, mintegy 28 milliárd forintot költött a fejlesztésre. Az egyenruhákban iránykereső rádióadók, és a Google Earth digitális térképéhez hasonló térképek segítik a tájékozódást, továbbá megpróbálják meggátolni, hogy saját embereire nyisson tüzet a tüzérség. A védőszemüvegébe épített bélyegnagyságú képernyőn a katona látja saját helyzetét és bajtársaiét is, továbbá az ellenséges páncélosokat, mégpedig méterre pontosan. A legújabb fejlesztések révén a fegyverek is képesek lesznek az együttműködésre. Ha egy katona lézerrel megjelöl egy ellenséges célt, a hálózaton a többiek is látják.

Az ehhez szükséges számítógépet minden katona magán viseli, mérete egy szokásos laptop harmadára csökkent, és a katona övére csatolják. Az egyik gyenge pont a fejhallgató, amely nagyon gyorsan eltörik. A felszerelésnek komoly súlya van, meghaladja a 33 kilogrammot, ezért a hátizsákot egy kis járműbe teszik, a fegyvereket pedig az eddiginél könnyebb anyagból építik. a fejlesztők már dolgoznak az újabb harci ruha generáción, hiszen itt egy kollekció némileg lassabban készül, mint a nagy divatházaknál. Erről annyit tudni, hogy az anyag színváltós lesz, a nanotechnológián alapul, antibakteriális hatású, és felismeri a vegyi és biológiai fegyvereket, továbbá természetesen golyóálló. Színe fekete, és vékony anyagból készül majd, a 2025-ös divat szerint.

A másik érdekes és egyben jövőmutató hír az informatikai biztonsághoz, elsősorban a biztonságos kommunikációhoz kapcsolódik. A hír, hogy Robert Gates, az Egyesült Államok védelmi minisztere 2009. június 23.-án hivatalosan is bejelentette egy új katonai parancsnokság megalakulását, melynek feladata az USA cyber-biztonságának megteremtése lesz, vagyis röviden hadrendbe állnak az amerikai cyberkatonák.

2009 októbertől már csatasorba is állt majd a Pentagon Stratégiai Parancsnokságának részeként működő Cyber-biztonsági Parancsnokság, igaz a teljes tervezett kapacitást csak 2010 októberére érik majd el. A Pentagon szóvivője, Eric Butterbaugh, a légierő alezredes szerint "ez egy belső átszervezés, melynek lényege, hogy jobban ráirányítsa a fókuszt a katonai hálózatokra, megerősítse és korszerűsítse a Pentagon cyber-képességeit egy egységes parancsnokságon belül". A szervezetet Keith Alexander altábornagy, a National Security Agency (NSA)[6] jelenlegi vezetője irányítja majd.

A Pentagon már eddig is megkapta a kormányzat informatikai biztonsági büdzséjének nagy részét, s már jelenleg is több ezer, "internetes hadviselésre" kiképzett szakemberrel rendelkezik, akik most zömmel az új szervezet ernyője alá kerülnek. Gates tervei szerint a jövőben évi 200 új "cyberbiztonsági" tisztet képez majd ki a Pentagon.

Összehasonlításképp: a Department of Homeland Security (belbiztonsági minisztérium) mindössze 100 dedikált alkalmazottal rendelkezik a civil hálózatok védelmére, s még a jövőre tervezett 260-as szám elérésével is jóval elmaradnak a most létrejövő parancsnokság méretétől. Az illetékesek hangsúlyozták, Pentagon részeként most létrejövő szervezet kizárólag a katonai célú hálózatok védelmével foglalkozik, a polgári infrastruktúra védelme továbbra is a belbiztonsági minisztérium feladata lesz, tehát a hadsereg továbbra sem figyel meg civil hálózatokat. (A Pentagon, illetve a védelmi miniszter kommunikációjában ezúttal sem esett szó arról, hogy az új szervezet a védekezés és elhárítás mellett milyen szerepet kaphat esetleges támadások során.)

[6] Nemzetbiztonsági Ügynökség

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

Látható tehát, hogy az informatikai rendszerek témakör rendkívül szerteágazó. Nem oktathatóak a katasztrófavédelmi informatikai rendszerek kiragadva az információs társadalom egészéből. A katasztrófavédelemben dolgozók mindegyikének tisztában kell lennie az alapfogalmakkal, foglalkozniuk kell a már működő rendszerekkel, a fejlesztési stratégiákkal és az informatikai eszközök biztonságával foglalkozó kérdésekkel egyaránt. Mindezekből következik, hogy ezekkel a kérdésekkel a rendelkezésre álló szűkös órakeretek mellett is foglalkoznunk kell az oktatott tantárgyakon belül. Természetesen tisztában vagyok azzal is, hogy az informatikai rendszerek tantárgy oktatása nem képezi a szakirány legfőbb képzési feladatát. Ezzel a publikációval ezért csak az volt a célom, hogy ráirányítsam a figyelmet az informatikához kapcsolódó tantárgyak oktatásának szükségességére és röviden bemutassam azokat a témákat, amelyekkel az oktatás során jelenleg is foglalkozunk. Az előrelépés lehetőségét látom még abban is, ha a szakirányon oktató más tanár-kollégákkal összehangoljuk az oktatási feladatainkat és ennek eredményeként tovább tudjuk emelni a szakirány oktatásának színvonalát.

FELHASZNÁLT IRODALOM

[1] http://www.magyarorszag.hu/kereses/jogszabalykereso (2009.12.30)

[2] AAP-31(A) NATO GLOSSARY OF COMMUNICATION AND INFORMATION SYSTEMS TERMS AND DEFINITIONS, NATO szótár, a kommunikációs és információs rendszerekhez kapcsolódó kifejezések és fogalom-meghatározások, 1996

[3] AJP-01(A) ALLIED JOINT DOCTRINE Szövetséges Összhaderőnemi Doktrína, 1999

[4] AAP-6(V) NATO GLOSSARY OF TERMS AND DEFINITIONS (ENGLISH AND FRENCH) NATO kifejezések és fogalom-meghatározások (angol és francia), 1995

[5] http://www.magyarorszag.hu/kereses/jogszabalykereso/pf/SearchLaw/paging?__page=3 Katonai strat. (2009.12.30)

[6] Dr. Munk Sándor: Katonai informatika II. Katonai informatikai eszközrendszere, ZMNE egyetemi jegyzet, 61-65, 2003

[7] Dr. Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana. Az információbiztonság egy lehetséges taxiómája. BOLYAI SZEMLE XVII: (4) pp. 137-155. (2008)

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Őze Zoltán
ozezoltan@gmail.com

AZ ABV ESEMÉNYEK HELYZETÉRTÉKELÉSÉT ÉS A DÖNTÉS-ELŐKÉSZÍTÉST TÁMOGATÓ SZÁMÍTÓGÉPES PROGRAMOK

Absztrakt

Annak érdekében, hogy a parancsnokok fel tudják mérni az ABV események hatását a döntéseikre és csapataik további tevékenységére, biztosítani kell számukra az időbeni, pontos és kiértékelt információt ezekről az eseményekről. Az ABV eseményekre vonatkozó információ gyűjtése, értékelése és továbbítása az ABV védelem kiemelkedő jelentőségű feladatát képezi. Az ABV események és a kialakuló „Veszélyes terület"-ek pontos adatainak időbeni biztosítása érdekében került kialakításra az Atom, Biológiai, Vegyi Riasztási és Értesítési Rendszer (ABV RIÉR) képesség. Az ABV RIÉR hatékonyságát növelik a minél pontosabb és gyorsabb veszélyértékelést lehetővé tevő fejlett NATO-kompatibilis számítógépes értékelő programok.

In order to enable commanders at all levels to assess the impact of CBRN incidents on plans and decisions, they must be provided with timely, accurate and evaluated information on these incidents. Collection, evaluation and exchange of information on CBRN incidents form an extremely important part of CBRN defence. To ensure timely provision of the most accurate data on CBRN incidents and the resulting hazard areas, a CBRN warning and reporting capability was established. NATO compatible evaluating softwares enable faster and more accurate evaluation which improves the effectiveness of CBRN Warning and Reporting System

Kulcsszavak: *ABV esemény, helyzetértékelés, ABV RIÉR, számítógépes értékelő program ~ CBRN incident, evaluation, CBRN W&R, evaluating software*

BEVEZETÉS

A Magyar Honvédségnél évek óta használatban vannak azok a döntés-előkészítő és helyzetértékelő számítógépes szoftverek, melyek a NATO irányelvekkel összhangban, kifejezetten a tömegpusztító fegyverek alkalmazása és veszélyes ipari anyagok kiszabadulása esetén segítik a szakemberek munkáját. A legújabb NATO szabályzók - szakértői eljárásként definiálva - már külön hangsúlyt fektetnek az ABV események számítógéppel támogatott értékelésére. Ezek a programok eredményesen segítik elő a gyors, és pontos munkavégzést a Magyar Honvédségnél. A cikk célja ezen programok: az NBC-ANALYSIS, az HPAC, és egy új program, az NBC WaRN rövid ismertetése, összehasonlítása.

AZ HPAC SZOFTVER RÖVID ISMERTETÉSE

A Hazard Prediction and Assessment Capability (HPAC) egy olyan program, amely előrejelzi az atmoszférába jutott veszélyes anyagok civil lakosságra vonatkoztatott hatásait. Továbbá segítséget nyújt a tömegpusztító fegyvereket tartalmazó célpontok megsemmisítésében azáltal, hogy választ ad a veszélyes anyag kiszabadulására. Felhasználja az integrált forrástagokat, nagyfelbontású időjárás előrejelzéseket, terep, talajfedettség adatokat és a megfelelő terjedési algoritmusokat, hogy gyorsan modellezze a kialakult veszélyes területeket, és a lakosságot érő hatásokat.

Az HPAC értékeli az ABV veszélyeket függetlenül attól, hogy a kibocsátás ipari tevékenységből, vagy fegyver használatából származik. [1]

Az HPAC az alábbi veszélyforrásokból készít előrejelzést:

- Nukleáris létesítmény baleset (pl. Csernobil, Ukrajna)
- Atomfegyver alkalmazása (pl. Hirosima, Japán)
- Atomfegyver baleset (pl. Palomares, Spanyolország)
- Radiológiai fegyver incidens („dirty bomb”)
- Vegyi üzem baleset (pl. Bhopal, India)
- Biológiai üzem baleset (pl. Sverdlovsk, Oroszország)
- Vegyifegyver alkalmazása (pl. Kamasiyha, Irak)
- Biológiai fegyver alkalmazása (pl. Yokosuka, Japán)

Röviden összefoglalva a program szimulálja a veszélyes anyagok levegőben való terjedését, áramlását. Megbecsüli a fizikai környezetet ért hatásokat (például a felszíni lerakódást és a levegőben lebegő veszélyes anyag koncentrációt) és a lakosságot ért hatásokat. Feladata az atom-, biológiai-, vegyi- és radiológiai veszélyek hatásainak és a terepen való szétszóródásának előrejelzése a világ bármely területén.

A szoftvert a Defence Threat Reduction Agency (DTRA) készíti az Amerikai Egyesült Államokban. Ez mintegy ötezer főt foglalkoztató ügynökség, amely feladata új technológiák kutatása, fejlesztése és bevezetése az amerikai katonai rendszerbe. A programot fél éves ciklusokban frissítik. [5] Jelenleg a 4,0,4-es verzió hozzáférhető. A DTRA 2002 óta ingyenesen terjeszti a szoftvert a NATO országok számára, és a világ számos pontján oktatják használatát. Mivel a program minősített adatbázisokat használ, ezért internetes regisztrációhoz kötött a használata. A regisztráció magába foglalja néhány titkos Internet oldal használatát és a programot tartalmazó DVD ingyenes postázását. Az aktuális adatbázisok és programfrissítések ezekről az oldalakról tölthetők le ingyenesen. A program használatát minimum fél évre, maximum két évre lehet igényelni. Ez után újabb regisztráció szükséges. A DTRA 24 órás folyamatos telefonos elérhetőséget biztosít a felhasználók számára. [1]

A szoftver rendszer követelményei:

- 500 MHz-es processzor (1 GHz ajánlott)
- 512 MB RAM (1Gb ajánlott)
- 1024 x 768-as felbontású monitor
- DVD+R olvasó
- Internet csatlakozás
- 2,54 GB szabad hely a merevlemezen (a teljes telepítéshez)
- Microsoft 2000, XP, NT 4 (SP6) operációs rendszer

Az HPAC elsősorban finomított döntéstámogatást biztosít, kiegészítve az ATP-45-t, azonban azt nem helyettesíti. Terminusokban adja meg a veszély „legjobb becslését”. Ezen belül is a helyet és kiterjedést, a járulékos emberi hatásokat és a veszély változását. Az HPAC kimeneti értékei valószínűsítettek. A bizonytalanság a turbulencia modell, az időjárási adatok, és az esemény helyének bizonytalanságaiból adódik össze.

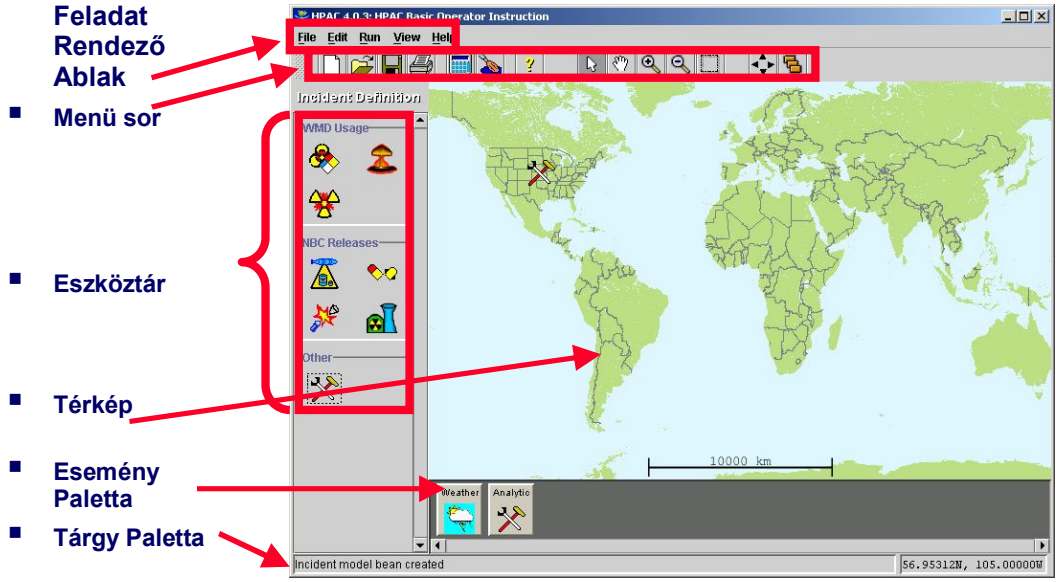
Az HPAC korlátai a következők:

a) A felbontást és a pontosságot a bemeneti adatok korlátozzák. A felszín, földhasználat, populáció és a védelem típusai 1 kilométeres felbontásban adhatóak meg.
b) A városi terjedés, diszperzió csak nyers változat, ugyanis minden városi területet hasonlóan kezel. Nem számol részletes szélváltozékonysággal.
c) Az HPAC kimenete nem determinisztikus. Az HPAC lehetséges kimenetet biztosít, a veszélyt valószínűségként értékeli.
d) A szoftver csak angol nyelven hozzáférhető, és nagyfokú szakmai hozzáértést kíván, ugyanis a térképen megjelenített eredmény minden esetben magyarázatot igényel a félreértések elkerülése érdekében. [1]

Az HPAC modell néhány alapvető komponense:

- *Incidens modellek,* hogy kiszámolhassuk a kibocsátott ABV anyagok karakterisztikáját;
- *Rutinok és adatbázisok*, hogy adatot biztosítson a környezetről beleértve az időjárási és talajfelszíni adatokat;
- *Atmoszférikus terjedési modell*, hogy kiszámolhassuk, hogyan szóródik szét a kibocsátott anyag a környezetben;
- *Az emberi hatások modelljei*, hogy segítsen mennyiségileg meghatározni a személyeket ért hatásokat;
- *Felhasználói felület (Project Editor)*, hogy irányítani tudjuk a komponensek közötti tevékenységet.

A grafikus felhasználói felület (1. ábra) biztosítja az HPAC alkalmazások számára az interaktív szerkeszthetőséget és a különféle nézetek közötti váltást.



1. ábra. Az HPAC grafikus felhasználói felülete [1]

HPAC	
Előnyei	***Hátrányai***
Ingyenes	**Angol nyelvű**
Alkalmazhatóságát tekintve rendkívül sokoldalú	**Magas hardver igény**
Különálló számítógépen használható	**Regisztráció függvénye a hozzájutás**
A Föld egész területére kiterjeszthető értékelések lehetősége	**A minősített adatbázisok miatt nem mindenki használhatja**
Populációs adatbázis használata	**Használata és az eredmények magyarázata nagy szakértelmet kíván**
Biológiai anyagok terjedésének modellezése	**A pontos helyzetértékeléshez sok alapadatra van szükség, és ezek begyűjtése lassú folyamat**
Közúti szállítási balesetek modellezése	
A radiológiai fegyver hatásainak előrejelzése	
Domborzat és felszín fedettség figyelembe vétele	
SCIPUFF terjedési modell	
Veszteségszámítás	
A meteorológiai adatok széles körét felhasználja	
A világ atomerőműveinek teljes adatbázisa	
24 órás technikai támogatás	
Meteorológiai adat szerver használatának lehetősége	
Kiválóan alkalmas szakemberek és felső vezetők gyors tájékoztatására	
Részletes program dokumentáció és hatékony help menü	

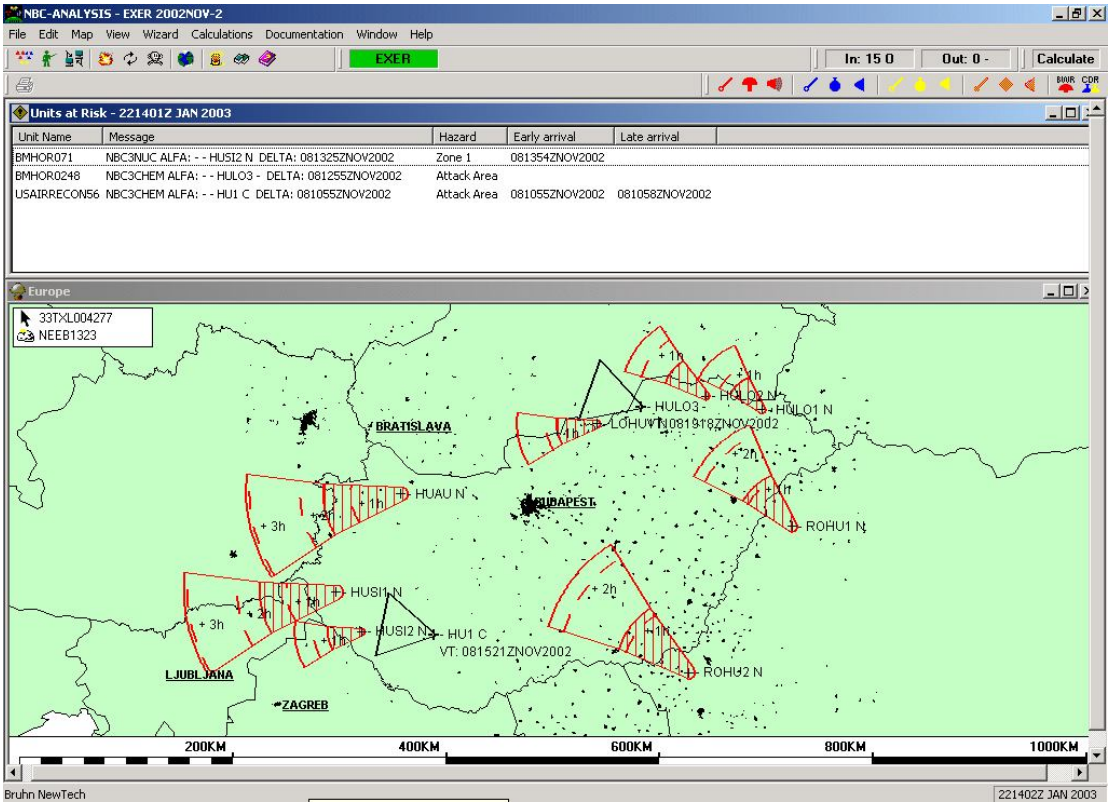
1. Táblázat. Az HPAC előnyei és hátrányai (készítette: szerző)

AZ NBC-ANALYSIS SZOFTVER RÖVID ISMERTETÉSE

Az NBC ANALYSIS program szerepe a katonai ABV szakértékelésben hasonló, mint a RODOS szerepe a katasztrófa-elhárításban. A program rendeltetése, hogy az automata és hagyományos felderítőrendszerek által nyújtott, az ABV eseményekre vonatkozó információkon alapuló szakértékeléseket hajtson végre, és azokat megjelenítse, adatbázisba rendezze, illetve elvégezze az érintett szervezetek riasztását és értesítését. A NATO-ban elfogadott ATP-45 szabvány elektronikus változata gyakorlatilag ez a program, teljes mértékben igazodik a NATO ABV riasztási és értesítési rendszeréhez, számításait az AEP-45-ben lefektetett matematikai eljárások szerint végzi. [4]

Az NBC ANALYSIS egy komplex döntéstámogató rendszer, hiszen egyesíti azt a folyamatot, mely az ABV felderítés alapadataitól a kommunikáción, szakértékelésen keresztül az értékelt információk megjelenítéséig és az érintett, illetve a veszélyeztetett szervezetek riasztásáig, illetve tájékoztatásáig terjed. [1]

Mivel ez a rendszer alapvetően katonai felhasználásra készült, ezért elsőrendű fontossággal bír a kommunikáció gyorsasága, pontossága, megbízhatósága. A rendszer gyakorlatilag ugyanabban a formában kerül telepítésre a mobil járőrökön, stacioner állomásokon és értékelő szerveknél, ugyanazokkal az értékelő és térinformatikai adatbázisokkal rendelkezik és csak az egyes ABV eseményekre, szakértékelésekre, tájékoztatásokra és riasztásokra vonatkozó rövid, tömörített biner adatcsomagokkal dolgozik. Emiatt a továbbításra kerülő adatok néhány kB-os nagyságrendűek, melyek biztosítják a gyors és megbízható adatforgalmat, harctéri körülmények között is. [1]



2. ábra. Az NBC-ANALYSIS kezelő felülete és térinformatikai modulja (készítette: szerző)

Az NBC ANALYSIS egy, alapvetően hadműveleti szintű, döntés-előkészítést segítő rendszer, melynek szakértékelései önmagukban erősen elnagyoltak, rendkívül konzervatív becsléssel közelítik az ABV események valóságos paramétereit, tehát egyes események részletes értékelésére alkalmatlan. Mindazonáltal lehetővé teszi az ABV felmérést és szakértékelést végző szervezetek gyakorlatilag teljesen automatizált működését. [1]

A szoftvert az 1985-ben alapított dán Bruhn NewTech cég készíti és forgalmazza. Fő profiljuk az atom-, biológiai-, vegyi- és radiológiai veszélyekkel, eseményekkel kapcsolatos programok fejlesztése, szaktanács adás és tréningek szervezése. Fő szoftverük az NBC-ANALYSIS, amelyet katonai parancsnokságok és civil veszélyhelyzet-elhárítók számára terveztek. A program alkalmas atom-, biológiai és vegyifegyverek alkalmazása és a nem csapásból származó veszélyes kibocsátások (ROTA), valamint toxikus ipari anyagok (TIM) kiszabadulása következtében kialakuló veszélyek előrejelzésére.

Ezenkívül jelentések fogadására és küldésére, továbbá a szükséges riasztások végrehajtására. Jelenleg a program 11,0 –ás verziója vásárolható meg. A fellépett igények miatt, a cég elkészítette az NBC-ANALYSIS azon változatát, amely közvetlenül fogadja az HPAC eredményeit. Így tovább pontosíthatóak az NBC-ANALYSIS eredményei és mivel a layerek egymásra helyezhetők, akár együtt is szemléltethetik a kialakult helyzetet.

A szoftver használatával biztosítható a gyors és pontos információ jelentése a forrás szinttől a magasabb parancsnokságok felé és vissza. Ennek köszönhetően napjainkban 16 NATO ország, több NATO parancsnokság és számos békepartner (PfP) ország használja. [1]

A programcsomag szolgáltatásai:

- NBC üzenet készítés, küldés, fogadás, feldolgozás,
- Sugáradag és sugárszint számítás,
- Gyakorlatok tervezése,
- Térinformatikai megjelenítés (UTM koordináta rendszer),
- NATO csapatjelzések használata,
- Adatátvitel (LAN, modem, kábel, outlook),
- ABV csapások veszély előrejelzése
- Nem csapásból származó kibocsátások értékelése (ROTA)
- Beépített veszélyhelyzet elhárítási kézikönyv (ERG2000),
- On-line támogatás és update

A szoftver rendszer követelményei [2]:

- Pentium II processzor 300 MHz
- 128 MB RAM
- 1024 x 768-as felbontású monitor
- CD olvasó
- Microsoft Windows 9X, 2000, XP operációs rendszer

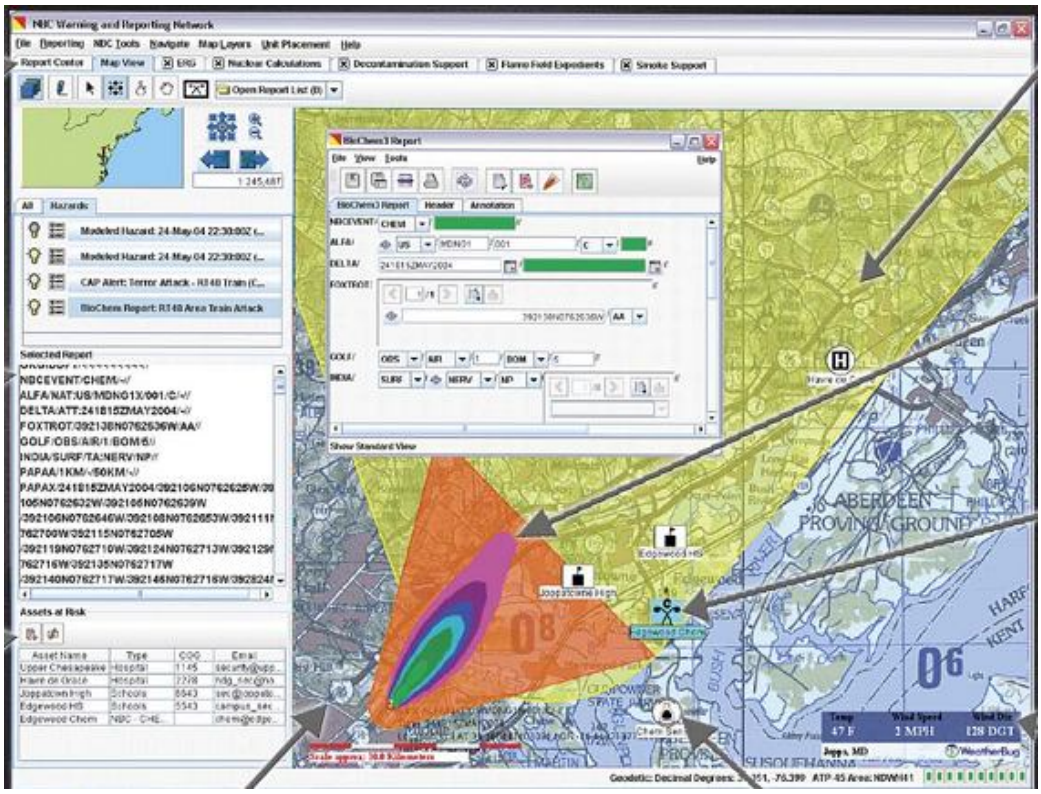
NBC-ANALYSiS	
Előnyei	***Hátrányai***
NATO szabványok teljes körű alkalmazása (ATP-45)	**Angol nyelvű**
Gyors alapadat bevitel	**Drága**
Gyors értékelés és jelentéskészítés, továbbítás	**Csak hardver kulccsal üzemel**
Egyszerű használat, megtanulhatóság	**A grafikus eredményhez nem választható méretarány**
Alacsony hardver igény	**Az értékelésnél nem veszi figyelembe a domborzatot és a felszín fedettségét**
Fejlett kommunikáció és adatfeldolgozás	
Alakulatok, alárendeltek korai riasztása	
24 órás technikai támogatás	
Az HPAC eredmények ábrázolása térképen	
Beépített veszélyhelyzet elhárítási kézikönyv (ERG2000)	
Információ a veszélyeztetett alegységekről	
NATO csapatjelzések használata	
Nem csapásból származó kibocsátások értékelése (ROTA)	

2. Táblázat. Az NBC-ANALYSIS előnyei és hátrányai (készítette: szerző)

AZ NBC WARN SZOFTVER RÖVID ISMERTETÉSE

Az NBC WaRN már régóta az ABV értékelés alapszoftvere az Amerikai Egyesült Államok hadseregében, de csak néhány éve programozták át a NATO szabványoknak megfelelően. A programot előállító amerikai Optimetrics, Inc. Vállalat nem titkolt szándéka volt ezzel, hogy alacsonyabb árával konkurenciát teremtsen a NATO országokban elterjedt NBC- ANALYSIS szoftvernek. A programot 2009-ben több NATO ország, köztük Magyarország rendelkezésére bocsátották tesztelés céljából. Hazánkban a tesztelést az MH GAVIK értékelő állománya hajtotta végre a Dániában megrendezett nemzetközi Brave Beduin 2009 ABV értékelő gyakorlaton.

A szoftver az NBC-ANALYSIS-hoz hasonlóan a gyors , konzervatív értékelésre fekteti a hangsúlyt. Integráltan megtalálható benne az HPAC szoftver, amely képes a veszély realisztikusabb, a terep és a talajfelszín tulajdonságait is számításba vevő értékelésére. Nagy hibája, hogy minden bejövő üzenetet egyenként kell vele értékelni, mely nagyban lelassítja az értékelési folyamatot. Ugyanakkor a szoftvernek vannak ötletes megoldásai, nagyon sok más programmal kompatibilis. Például az üzeneteket egyszerűen áthúzva a Google Earth programba, ott automatikusan ráközelít a csapás helyére és ábrázolja a veszélyeztetett területet a térképen. Összességében azonban elmondható, hogy a program nem váltotta be a hozzáfűzött reményeket: kezelése jóval körülményesebb az NBC-Analysis-énál, és a lassú adatfeldolgozás miatt nem felel meg egy robosztus ABV RIÉR követelményeinek.



3. ábra. Az NBC WaRN szoftver kezelőfelülete [3]

A programcsomag szolgáltatásai:

- NBC üzenet készítés, küldés, fogadás, feldolgozás,
- Gyakorlatok tervezése,
- Térinformatikai megjelenítés (UTM koordináta rendszer),
- NATO csapatjelzések használata,
- Adatátvitel (modem, kábel, e-mail),
- Integrált HPAC program,
- ABV csapások veszély előrejelzése
- Nem csapásból származó kibocsátások értékelése (ROTA)
- Kompatibilis a Google Earth programmal,
- Beépített veszélyhelyzet elhárítási kézikönyv (ERG2008),
- On-line támogatás és update

A szoftver rendszer követelményei:

- 500 MHz-es processzor (1 GHz ajánlott)
- 512 MB RAM
- 1024 x 768-as felbontású monitor
- CD olvasó
- 100 MB szabad hely a merevlemezen
- Microsoft Windows 2000, XP operációs rendszer

NBC-WaRN	
Előnyei	***Hátrányai***
NATO szabványok teljes körű alkalmazása (ATP-45)	**Angol nyelvű**
Gyors alapadat bevitel	**Kissé bonyolult használat, megtanulhatóság**
Fejlett adatfeldolgozás	**Nehézkes kommunikáció**
Beépített veszélyhelyzet elhárítási kézikönyv (ERG2008)	**Az értékelésnél nem veszi figyelembe a domborzatot és a felszín fedettségét**
NATO csapatjelzések használata	**Nehéz adatfeldolgozás, a csapásokat nem lehet külön-külön megjeleníteni a térképen**
Nem csapásból származó kibocsátások értékelése (ROTA)	**Nehéz elkülöníteni az új NBC üzeneteket a régiektől**
Az HPAC eredmények ábrázolása térképen	**Nincs lista a veszélyeztetett alegységekről**
Olcsó	**Nehéz egy általános képet kapni az adott hadműveleti helyzetről**

3. Táblázat. Az NBC WaRN program előnyei és hátrányai (készítette: szerző)

ÖSSZEGZÉS

A vizsgált szoftverek közül az ABV RIÉR-rel szemben támasztott követelményeknek egyedül az NBC-ANALYSIS program felel meg. Az NBC WaRN jelenlegi formájában jelentős új képességet nem kínál, és nem képes az NBC-ANALYSIS kiváltására.

Az HPAC szoftverrel történő értékelés egy realisztikusabb, részletesebb, kevésbé konzervatív veszélybecslést tesz lehetővé, de egy-egy esemény feldolgozása akár több órát is igénybe vehet, emellett kezelése nagyobb szakértelmet igényel.

Mind az NBC-ANALYSIS, mind az HPAC program hasznos a rendszergyakorlatok tervezésénél és magánál a gyakorlatok végrehajtásánál is.

IRODALMI HIVATKOZÁS

[1] Kovács Roland mk. őrnagy: A térinformatika alkalmazási lehetőségei a katasztrófavédelemben - Az HPAC és az NBC-ANALYSIS szoftverek bevezetése Magyarországon (Szakdolgozat), Gödöllő, 2005

[2] http://www.bruhn-newtech.com/defense/products/nbc-analysis 2010. 03. 12.

[3] http://www.nbcwarn.com/feaures_nbc.htm 2010. 03. 12.

[4] STANAG 2103 ATP-45 (AEP-45) Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological, and Nuclear incidents

[5] http://www.dtra.mil/Home.aspx 2010.03.14.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Vágföldi Zoltán
vagfoldi@hotmail.com

A VEGYIVÉDELMI TECHNIKAI ESZKÖZÖK FEJLŐDÉSÉNEK TÖRTÉNETE – A VEGYIFELDERÍTŐ ESZKÖZÖK FEJLŐDÉSE

Absztrakt

A cikkben az önálló magyar vegyivédelmi szolgálat megalakulásától napjainkig (1950-2010) áttekintem a Magyar Néphadseregben (a továbbiakban: MN) valamint a Magyar Honvédségben (a továbbiakban: MH) alkalmazott/rendszeresített vegyifelderítő eszközöket, készülékeket. A vegyivédelem első kezdetleges, de korabeli szempontból nélkülözhetetlen, egyszerű vegyifelderítő eszközétől indulva a mai korszerű berendezésekig bemutatom az eszközök főbb harcászati-műszaki adatait, a fejlődés lépcsőit. Kiemelten foglalkozom a hazai gyártású (többségében hazai fejlesztésű) eszközökkel.

The purpose of this article is to sum up all equipment/instruments of chemical reconnaissance used or employed by the Hungarian Defence Forces and the former Hungarian People's Army from the establishment of the independent Hungarian NBC Defence Service to nowadays (1950-2010). I will present technical data of chemical detectors and stages of its development as from earliest primitive detectors, what was indispensable for that age, to contemporary modern ones. Chemical detectors produced and developed inland will be accentuated in my essay.

Kulcsszavak: *ABV védelem, vegyifelderítő eszköz, mérgező harcanyag ~ NBC defence, chemical detection, CWA (chemical warfare agents)*

Bevezetés

A XX. század első felétől a korszerűen értelmezett vegyi háborúk, az első tervezett „vegyi csapás" (1915 Ypernnél gázpalackból a németek által klórral végrehajtott vegyi támadás a francia csapatok ellen) óta, valamint a hidegháborút követően napjainkig – a vegyi fegyverek gyártását és alkalmazását korlátó egyezmények ellenére- mind a vegyi támadás, mind a vegyivédelem szaktechnikai eszközei – a többi fegyvernemhez hasonlóan – hatalmasat fejlődtek. A vegyivédelmi szolgálat megalakulásától napjainkig a tárgyalt 60 éves időszakot önkényesen két részre bontva bemutatom a vegyifelderítő műszerek fejlődésének,

fejlesztésének főbb irányait és a rendszeresített eszközök néhány főbb harcászati-műszaki paramétereit.

Vegyifelderítő eszközök a 2. világháborútól a „hidegháború végéig” (1950-1989)

Az 1. világháborúban a mérgező anyagok jelenlétét kizárólag érzékszervi úton állapíthatták meg, a helyzet alapvetően nem változott a 2. világháború végéig sem (1945). Próbálkozások történtek ugyan a maradó mérgező harcanyagok (elsősorban kénmustár, kémiai neve: diklór-dietil-szulfid, NATO rövidítése: HD) kimutatására, de ezek a módszerek nem voltak specifikusak (pl. szudán por, lakmusz papír). Közvetlenül a 2. világháború előtt fedezték fel az új típusú (kémiai szerkezetű), magas toxicitású fluorofoszfátok néhány típusát (szarin, foszforsav-észter származék), melyek fizikai-kémiai tulajdonságai a 2. világháború után kerültek nyilvánosságra. Ezen ismeretek alapján nyilvánvalóvá vált, hogy a mérgező harcanyagok (a továbbiakban: MHA) kimutatása csak műszeres úton oldható meg a csapatok védelme érdekében. 1945 után a vegyifegyverek (illetve az un. tömegpusztító fegyverek) elleni védelem Magyarországon is egy újonnan felállított szervezet szakmai irányítása alá került, ezáltal megalakult egy új szolgálati ág, a vegyivédelem, melynek feladatai a hidegháború alatt (1947-1989) jelentősen kiszélesedtek. A vegyivédelmi technikai eszközöket az alábbi 3 csoportba sorolták, osztották fel: [1]

1. védőeszközök (egyéni és kollektív);
2. felderítő eszközök (vegyi- és sugárfelderítő eszközök, beleértve a mintavevő és a tábori meteorológiai eszközöket, felderítő gépjárműveket is);
3. mentesítő eszközök és anyagok (személyi mentesítő, személyi felszerelés és terepmentesítés, fegyvermentesítő anyagok).

A felderítő eszközök fejlődését tekintve a világháborút követően az új fenyegetéseknek (atomfegyver, új típusú mérgező harcanyagok megjelenése) és megnövekedett igényeknek megfelelően szükségesnek látszott a MHA-ok minőségi (kvalitatív) és mennyiségi (kvantitatív) meghatározása a szubjektív észlelés mellett vagy lehetőleg annak teljes kizárásával. Mivel az esetek többségében a levegőben jelen lévő MHA gőzöknek kimutatására van szükség, olyan eszközöket fejlesztettek, amelyekbe a levegő átszívásakor a gőzök adszorbeálódnak egy csőben és megfelelő reagenssel kimutatható a jelenlétük, ugyanis mérgező anyag jelenlétében az adszorbens anyag elszíneződik. Ezek a viszonylag egyszerű eszközök (kimutató csövek) az alábbi irányokba fejlődtek:

- minőségi kimutatás mellett hozzávetőlegesen a koncentrációt is meghatározzák;
- egyszerre (1 helyett) több kimutató csővel működnek;
- lehetőség szerint minden reagens az adszorbensen van (nem kell egyéb művelet, csak átszívatás);
- télen is üzemképesek (0 ºC alatti hőmérsékleten, fűtőpatron segítségével)

A magas toxicitású „idegméreg” hatásmechanizmusú, foszforsav-észter típusú vegyületek tulajdonságainak vizsgálata során kiderült, hogy nem elégséges, ha bizonyos jelek alapján rendelik el a vegyi felderítés végrehajtását és az eredmény alapján döntik el a „vegyi riadó” szükségességét. Ez túlságosan hosszú idő lenne a kis töménységben is „hatásos” (halálos) foszforsav-észter típusú vegyületek esetében, ezért az idegmérgek kimutatását automatizálni kellett.

Mérgező harcanyag megnevezése	**MHA gőzök harcképtelenséget okozó közepes adagja légzőszerveken keresztül (**mg perc/l)	**Cseppfolyós mérgező anyag közepes halálos adagja bőrön keresztüli felszívódással (**mg/kg)
Vx	0,007	0,1
szarin	0,004	25-30
mustár (kénmustár)	0,28	70-100

1. sz. táblázat

Mérgező harcanyagok toxicitásának összehasonlítása [2]

Az 1. sz. táblázatból kitűnik például, hogy a Vx a szarint gőzhatás szempontjából néhányszorosan, csepphatás szempontjából több százszorosan (!) felülmúlja. Külön figyelmet célszerű fordítani az un. V-anyagok és a Vx detektálására, hiszen kis illékonyságú, terepen cseppfolyós állapotban megmarad (maradó MHA), nagy az un. állékonysága (terepen nyáron 2-3 hétig is megmaradhat, rendkívül stabil), az élőerő elpusztítására pedig 270 kg Vx/km^2 mennyiség elégséges és a terep szennyezésénél a legkisebb hatásos mennyiség kb. 0,1 g/m^2. A kifejlesztett automata vegyijelző készülék korszerű változatai nemcsak az idegmérgek, de a többi „számításba vehető” mérgező anyagot is automatikusan mutatják ki.

Az MN vegyivédelmi szolgálatának első 25 éve (1950-1975) alatt elért fejlődését talán legszembetűnőbben a vegyi (és sugárfelderítés) eszközeinek és módszereinek változása jellemezte. Az első vegyifelderítő eszköz 1950-ben nagyon szerény rendeltetésű volt (kis vegyifelderítő készlet, szudán porszóró doboz), a kénmustár kimutatására is csak korlátozottan volt alkalmazható. A „nagy vegyifelderítő készlet” tiszta szilikagéllel (adszorbens) töltött üveg csövecskéket és üvegben tárolt reagenseket tartalmazott (Dräger készülék), bizonytalan működésű gumilabdaccsal szívták át a csöveken a levegőt, ezért csak szükségképpen volt alkalmazható az arzén-hidrogén (AsH_3), a hidrogén-cianid (HCN), foszgén ($COCl_2$) és kénmustár (akkori megnevezéssel M anyag) levegőből történő kimutatására. Az eszköz szilikagél csövecskéire kellett rácsepegtetni a kis üvegekben készletezett reagenseket (6 féle). Ha egyik csőnél sem mutatkozott színváltozás, azt jelentette, hogy a keresett mérgező anyagok érzékelhető koncentrációban nincsenek jelen.

Ezt követte a szovjet PHR-46 itthon gyártott változata. A szovjet készülék kimutató csöveiben a különféle reagensek üvegampullában, a csövekben voltak elhelyezve, a levegő átszívatása után egy szeggel kellett eltörni az ampullát és ráfolyatni a szilikagélre. A megoldás a végrehajtás szempontjából jobb, de továbbra is sok időt vett igénybe a levegő átszívatása.

Ezután a 66M VFK következett, amiben egyszerre hat előre melegített csövön keresztül szívatták át a levegőt. A kimutatás így gyorsabb lett, de a kimutató csöveket egyenként kellett feltörni. A hozzá tartozó kimutató csöveket Magyarországon fejlesztették, belső ampulla nélküliek - az enzimet tartalmazó idegméreg cső kivételével - és a reagens száraz állapotban volt a tölteten. Ezáltal a csöveken több órán át lehetett a vizsgálandó levegőt átszívni, biztosítva annak folyamatos ellenőrzését és megteremtve a lehetőséget a Folyamatos Vegyi Jelző. (a továbbiakban: FVJ) kifejlesztésére.

A 66M VFK vegyifelderítő készlet rendeltetése levegőben, terepen, harceszközökön, felszereléseken és más tárgyakon lévő mérgező harcanyagok kimutatása. Fő részeit tekintve horddobozból, kéziszivattyúból, melegítő berendezésből, mintavevő lapátból és kimutató csövekből állt. A mintavevő csövek érzékenysége szarinra 10^{-3} mg/l, HCN-klórciánra $5x10^{-3}$ mg/l, kénmustárra $2x10^{-3}$, foszgénre $5x10^{-3}$ mg/l, szománra $5x10^{-7}$ mg/l volt.

Alkalmazása szempontjából a szarin csővel 60 szívatást, a szomán csővel 40 szívatást követően a többi csővel 150 szívatást végeztek és értékelték a színváltozást a mellékelt színmintával összehasonlítva.



1. Kép. 66M VFK

A tömegspektrométerek és a robotrepülőgépek korában ezek a kezdetleges eszközök mai szemmel is fontosak voltak, mert a „semmit” váltották fel „valami” egyszerű eszközzel.

Kialakításuk, használatuk, gyártásuk adta az első tapasztalatokat a további fejlesztésekhez. „A vegyivédelem területén a fejlesztés első, határozott célokat kitűző időszaka 1953-ban indult el, ekkor valósult meg az első, kimutató csövekkel működő vegyifelderítő készülékek gyártása és kezdődött meg a sugárzásmérő műszerek gyártásra való felkészítése. A vegyifelderítés eszközeibe az 1958-62 közötti időszak szerény, de fontos előrelépést jelentett. Megkezdődött a csapatok ellátása a korszerűnek számító, téli üzemeltetésre alkalmassá tett, több kimutatócső együttes használatát biztosító vegyifelderítő készülékkel. A készülékhez bővült a csőválaszték, idegmérgek nagy érzékenységű kimutatását szolgálókimutató csöveket is készleteztek. 1965-ig az MN képessé vált a terep és levegő vegyifelderítésével kapcsolatos feladatok ellátására. Megtanulták az új eszközök használatát, megszervezték javításukat, biztosították rendszerben tartásuk körülményeit. Bármilyen védekező célokat szolgáló eszközzel szembeni követelményeket a pusztító fegyverek fejlődése határozza meg. A „szupertoxikus” mérgező harcanyagok (tabun, szarin, V-anyagok) megjelenése, célbajuttató eszközök fejlődése ugrásszerűen növelte meg a tömegpusztító fegyverek alkalmazásának lehetőségeit. A szocialista országoktól átvett tapasztalatokra, a hazai ipari kapacitásokra alapozva az 1960-as évek első felében 10 éves cél volt a legveszélyesebb MHA nagyobb érzékenységű kimutatása, a felderítés rendszerének nagyobb fokú mobilizálása. A 60-a 70-es években rendszerben lévő vegyi és sugárfelderítő eszközök (gépjárművek) a kor műszaki színvonalának megfelelő szinten biztosították a szakfeladatok végrehajtásának technikai feltételeit. A fejlesztés a korábbiaknál bonyolultabb felépítésű eszközökhöz vezetett”. [3]

A MN-ben rendszeresített vegyi- és sugárfelderítő eszközök döntő többsége az 1960-80-es években hazai fejlesztésű és gyártású volt. A MN Vegyivédelmi Főnökség, a Haditechnikai Intézet (HTI, jelenleg HM FLÜ Technológiai Intézet), a fejlesztő vállalatok (pl. Gamma Művek, jelenleg Gamma Műszaki Zrt.) és kutatóhelyek (pl. KFKI, Budapesti Műszaki Egyetem) együttműködésével komoly erőfeszítések történtek az eszközrendszer magas színvonalon történő továbbfejlesztésére.

Sorsz.	Vállalat megnevezése	Vegyivédelmi eszköz
1.	Reanal Finomvegyszergyár (Budapest)	kimutató csövek, AVJ reagens készlet,
2.	Biogal Gyógyszergyár (Debrecen)	AVJ reagens készletek
3.	Gamma Művek (Gamma Zrt, Budapest)	vegyijelző műszerek (66M VFK, AVJ, GVJ, FVJ)
4.	Labor Műszeripari Művek	TVL-63

2. sz. táblázat

Fontosabb vegyivédelmi eszközöket gyártó és fejlesztő vállalatok (1954-1990) [4]

Az idegmérgek állandó figyelésére a szintén hazai fejlesztésű, gyors és érzékeny, biokémiai elven működő Automata Vegyi Jelző (a továbbiakban: AVJ) és a vegyszer nélkül működő, sugárforrást tartalmazó Gyorsműködésű Vegyijelzőt (a továbbiakban: GVJ) rendszeresítették. A GVJ-hez hasonló eszköz a 70-es években máshol nem volt alkalmazásban. A különféle védett objektumokban (budapesti metró, vezetési pontok) a mérgező anyagok detektálására használták.

Az AVJ-1 rendeltetése idegmérgek levegőből történő kimutatása, 24 V-os gépjármű akkumulátorról lehetett üzemeltetni, jelentős tömege (19 kg) miatt vegyifelderítő gépjárművekben és fixen telepítve használták. Biokémiai működési elvét tekintve a vizsgálandó levegőt egy reagenssel nedvesített indikátor szalagon szívatták át, amely idegmérgek jelenlétében elszíneződik, ezt egy fotoelektromos érzékelő méri és a készülék riaszt. Az AVJ-1 detektorának köszönhetően mintegy 2 nagyságrenddel meghaladja a GSZP-1 érzékenységét. Riasztási ideje koncentrációfüggő, a MHA megjelenésétől kb. 57 másodperctől max. 3,5 percig tart. [5]



2. Kép. AVJ-1 készülék

Az FVJ a nem idegméreg típusú MHA jelzésére szolgált, a „levegő mérgező harcgáz szennyezésének ellenőrzését végzi folyamatos üzemeléssel”. A levegő átszívatását előszűrést követően min. 6 órán keresztül max. 1,5 l/perc sebességgel villanymotoros szivattyú végezte (tápellátása 24 V-os és 12 V-os gépjármű akkumulátorról történt) és a kimutató csövek is fűthetőek voltak (beépített hőmérő). A szivattyú légszállító teljesítménye potenciométerrel volt szabályozható (az alkalmazott csövek számának függvényében 0,6, 0,9 és 1,2 l/perc) és rotaméteren lehetett beállítani. A készülék teljes súlya 6,5 kg volt, -40 °C -tól +45 °C

környezeti hőmérsékleten is működőképes és kezelőszemélyzete 1 fő volt. A műszer üzembe helyezése (egyszerre maximum 4 féle kimutató csövekkel történő feltöltése) maximum 10 percet vett igénybe. Az FVJ-hez rendszeresített kimutatócsövek az alábbi „F" típusok voltak: F-1 HCN és ClCN, F-2 foszgén, F-3 arzénhidrogén (arzin), az F-4 pedig kénmustár. A műszert az AVJ mellett (egyidejűleg) működtették és az AVJ kezelője kezelte.

Típus	Kimutatható MHA	Színjelzés	Érzékenység mg/l	Töltet alapszín	Színváltozás	Üzemeltethetőség óra
F-1	HCN-ClCN	1 kék gyűrű	0,02	v. sárga	Lilás rózsaszín	24
F-2	foszgén	2 kék gyűrű	0,02	drapp	téglapiros	24
F-3	Arzin	3 kék gyűrű	0,02	fehér	Lilás-kék	24
F-4	Kénmustár	3 piros gyűrű	0,02	c.sárga	Barnás-lila	1

3. sz. táblázat
Az FVJ kimutató csövei



3. Kép. A FVJ fényképe

Minden kimutatócső töltőanyaga fölé színminta gyűrű volt festve, ezzel hasonlították össze a MHA okozta színváltozást. A mennyiségi információt, a levegő mérgezőanyag szennyezettségének hozzávetőleges koncentrációját a színváltozás idő függvényében kialakuló színmélységéből lehetett következtetni (pl. F-1 csőnél enyhe elszíneződés = veszélyes 2-3 percen belül kb. 0,02 mg/l koncentrációt jelent, 0,5 percen belüli igen erős elszíneződés = „halálos" kb. 1 mg/l töménységet jelentett). A kimutató csövek tízesével papírtasakban voltak csomagolva, amelyek rövid kezelési utasítással voltak ellátva. Az FVJ-hez típusonként 6-6 csomag (60-60 db) cső volt készletezve. [6]

A GVJ-1 műszer rendeltetése a levegő folyamatos ellenőrzése és a MHA-k (idegmérgek, foszgén, cián, kénmustár) megjelenésének automatikus jelzése, riasztása volt.

A műszer idegmérgeket kimutató egységének működése fizikai elven (differenciál ionkamra) alapult, üzemeltethető gépjárműbe építve vagy azon kívül is. A mérgező anyag tartalmú levegő membrán szivattyú segítségével (1,5 l/perc légszívás nagysága) két

egybeépített ionkamrába került, amiben 1-1 alfa (Am-241, 4,5 MBq aktivitás) sugárzó izotóp ionizálta a levegőt. Egy ionkamrát vizsgálva az ionkamra elektródjai potenciáljának növelésével mind több ion éri el azokat (az elektródák fogják be az ionokat és az elektronokat), egy meghatározott feszültségnél pedig az összes keletkező ion eléri a gyűjtő elektródákat és az ionáram a telítettségi értéket veszi fel. Amennyiben valamilyen olyan anyag kerül a gáztérbe, amely az ionokkal vagy elektronokkal ionizációs kölcsönhatásba lép (MHA vagy akár cigaretta füst), a mérhető ionáram csökken. Az ionizációs kamrák 180-200 V egyenfeszültséggel, de ellentétes polaritással üzemelnek. Az első (munka) kamra ionizációs árama idegmérgekre és egyéb anyagokra megváltozik, míg az összehasonlító kamra csak zavaró anyagokra változtatja meg ionizációs áramát, idegmérgekre csak minimális változást ad. A két kamra ionizációs áramának különbsége adja az idegmérgekre jellemző különbségi áramot, lehetővé téve ezáltal az idegmérgek kimutatását.

Az ionkamrás berendezés hátránya a gyenge specifikussága, előnye gyors jelzése (kimutatás gyorsasága 10 s). A műszer tömege 10 kg, tápellátása 2 db 4,8 V-os beépített akkumulátorról (2 NKP 20-24 lúgos akkumulátor, üzemideje 6 óra -20 °C feletti hőmérsékleten) történt, gépjárműbe építve töltőberendezés biztosította a saját akkumulátorának töltését. A műszer riasztás esetén fény és hangjelzést adott, téli üzemeltetést automatikus fűtésrendszerrel tette lehetővé.

A foszgén, cián és kénmustár kimutatása indikátor csövekkel valósították meg, egyidejűleg 3 db cső üzemét biztosította, a csövek figyelése vizuálisan történt. [7]

Ebben a fejezetben célszerűnek látom megemlíteni a TVL-63 tábori vegyi laboratóriumot valamint a VLG-71 laboratóriumi gépkocsit is.

A TVL-63 hozzá készletezett tartalék vegyszerkészletével különböző anyagokból, haditechnikai eszközökről, fegyverzetről és felszerelésről vett minták MHA tartalmának kimutatására alkalmazták klasszikus kémiai analitikai módszerekkel. A kialakított, kihajtható fadobozban helyezték el a vizsgálatokhoz szükséges különféle laboratóriumi eszközöket és vegyszereket (kis üvegekben, ampullában), a teljes készletet bőröndben helyezték el. A készlet alkalmas volt MHA minőségi kimutatására, foszfor (P) és arzén (As) tartalmú MHA-k valamint nitrogénmustár és kénmustár mennyiségi meghatározására, ismeretlen anyagok elemanalízisére, vegyi mentesítés teljességének vizsgálatára és aktívklór tartalmú mentesítő anyagok klórtartalmának meghatározására.



4. Kép. A TVL-63 fényképe

A VLG-66, majd a VLG-71 vegyivédelmi laboratóriumi gépkocsi rendeltetése a különféle technikai eszközökről, anyagokról valamint fegyverzetről és felszerelésről vett minták, a levegő és talajminták MHA tartalmának és radiológiai szennyezettség vizsgálata volt. A Csepel D-344 zárt felépítményű gépkocsihoz utánfutón aggregátor és a munkatérül szolgáló, gépkocsihoz építhető pótsátor tartozott, a zárt felépítménybe építették a bútorzatot (laboratóriumi asztalok, fiókok) és itt kaptak helyet a kimutatáshoz szükséges felszerelések, a beépített tartozékok (olajkályha, csatornarendszer, vízvezeték rendszer, vegyifülke). A „nem beépített" (málházott) főbb tartozékok pedig a víztisztító rendszer, vákuumszivattyú, táramérleg, AVJ, FVJ, szárítószekrény, TRL-3, rétegkromatografáló készülék, PB gázfőző, mikroszkóp, üvegedényzet, laboratóriumi cikkek, vegyszerek stb. voltak. Kezelőszemélyzete 6 fő, a gépkocsiba épített és málházott eszközök segítségével, az analízisek leírása szerint végezték el a kimutatásokat [8].

Amint a fentiek is igazolják a vegyifelderítés, mint a mérgező harcanyagok elleni védekezés egyik alappillére a vegyivédelmi (ABV védelmi) szolgálat alapvető feladatai közé tartozik. Szakszerű végrehajtásának legfontosabb feltételei azok az eszközök, amelyek biztosítják a mérgező anyagok jelenlétére és az emberekre való hatásuk mértékére (koncentráció, expozíciós idő és toxicitás) vonatkozó információkat. A vegyifelderítés célja, hogy adatokat szolgáltasson az ellenség által alkalmazott vegyi fegyverek minőségéről, azok elhelyezkedéséről, terjedéséről, a veszélyes-szennyezett terület kiterjedéséről és határairól. A vegyi felderítésben alkalmazott eszközök működésének alapját a MHA kémiai vagy fizikai tulajdonságaiból fakadó hatások képezik, így a kémiai analitika és annak módszereire támaszkodik. Az elvi alapok mellett azonban az eszközök működéséhez figyelembe kell venni a harcászati cél elérése érdekében kialakított követelményeket. A vegyifelderítés olyan feladat (kimutatás, mérés), melyet háborús körülmények között, harctéren kell végrehajtani. Így az eszközökkel szembeni követelményeket is alapjaiban ez adja meg, hogy harci körülmények között, meghatározott mérési feladatokat kell megoldani.

Vegyifelderítő eszközzel szemben támasztott általános követelmények:

- specifikusság (adott MHA vagy anyagtípus jelenlétének megállapítása és megkülönböztetése);

- érzékenység (olyan koncentrációban/mennyiségben mutassa ki a MHA-t, amely az emberre nem jelent veszélyt);
- objektivitás (az eszköz eredményének kiértékelése során az egyéni megítélést, mérlegelést zárja ki és beavatkozás nélkül – automatizáltan – mutassa);
- gyorsaság (azonnal vagy rövid idő alatt jelezze a MHA jelenlétét);
- harci körülmények (a fenti követelményeket úgy teljesítsék, hogy a harci körülmények között il alkalmazható legyen – kis súly, ellenálló képesség időjárás és mechanikai hatásokkal szemben-, alacsony energiafelvétel, utánpótlás, javíthatóság stb.).

Ezek a követelmények tökéletesen és egyszerre nem teljesíthetőek, egy eszközön nem teljesülnek, hiszen némely elvárás ellentétes egymással (pl. gyorsaság-érzékenység). Az eszközök fejlődése/fejlesztése a fenti főbb mutatók (harcászati-műszaki követelmények, HMK) állandó javulását célozza, figyelembe véve a mindenkori műszaki színvonalat, az ellenség MHA arzenáljának, alkalmazási elveinek és lehetőségeinek fejlődését.

Általánosságban elmondhatjuk, hogy a vegyifelderítő eszközök fejlődése alapvetően a szubjektívtől az objektív felé, az általánostól a specifikus felé, az érzéketlentől az érzékeny felé, a lassútól a gyors felé és a szakaszos üzeműtől a folyamatos felé haladt és halad napjainkban is. A fejlődésnek sajnos általában ára, hogy elveszítjük a készülék egyszerűségét, könnyű használhatóságát, igénytelen kezelését és olcsóságát (bonyolult elektronika, „high-tech" megoldások). Például a szudánpor szóró dobozban vagy a későbbiekben ismertetett CALID-3 MHA kimutató papír nem specifikus (más vegyi anyagokra, pl. olajra is jelez), nem objektív (egyéni „leolvasás" sokat számít), nem érzékeny és „szakaszos" a kimutatás, de egyszerű, olcsó és nem igényel technikai kiszolgálást. A VFK-66 vegyifelderítő készlet rendszeresített kimutató cső választékával specifikussá tehető, kielégítő az érzékenysége, de csak egyszer használatos és viszonylag időigényes a kimutatási folyamat. Az AVJ objektív, gyorsan és folyamatosan működik, de nem jelez mindenfajta MHA-t, bonyolult felépítésű, nagyméretű (gépjármű akkumulátorához kötött és komoly feladat a rendszerben tartása. [9]

A fejezetet az alábbi, több szempontból is érdekes táblázattal zárom. A 4. számú táblázatban a Gamma Művek által gyártott vegyijelző készülékek-műszer típusok és darabszámok láthatóak.

Típus	Gyártási időszak	Gyártott darab
• PHR-54 Vegyi felderítő készlet	1961-70	24092 db
• 66M VFK Vegyi felderítő készlet	1972-91	9596 db
• GSZP-1 Automata vegyijelző	1963-68	2079 db
• FVJ-1 Folyamatos vegyijelző	1970-91	660 db
• AVJ-1 Automatikus vegyijelző	1970-91	359 db
• VJK (AVJ+FVJ) Vegyijelző készlet		565 db
• GVJ-1 Gyorsműködésű vegyijelző	1974-90	589 db

4. sz. táblázat

A Gamma Művekben gyártott eszközök és darabszámok (1961-1991) [10]

Vegyifelderítő eszközök a rendszerváltozás után és a NATO csatlakozást követően (1990-2009)

Az előző fejezetben tárgyalt eszközök és felszerelések az „1990-es évek elejére erkölcsileg és „fizikailag" is elavulttá váltak, a rendszerváltás után a hadsereg folyamatos létszámcsökkentésen, átszervezésen ment keresztül, melyek jelentősen érintették a vegyivédelmi szakcsapatokat, annak létszámát is. A Magyarországi szükségletek csökkenése, a szovjet piac összeomlása miatt az ABV eszközök gyártásában részt vevő vállalatok sora ment csődbe vagy felszámolásra került. Ezáltal jelentősen csökkent a hazai termelői kapacitás". [11] Az 1999-es NATO csatlakozásunkkal új szakasz vette kezdetét, megjelent az új Nemzeti Biztonsági és Nemzeti Katonai Stratégia, mely jelentősen kihatott az ABV eszközrendszerre is.

Az akkori (2007-ben megszüntetett) MH Vegyivédelmi Technikai Szolgálatfőnökségnek új kihívásokkal, fogalmakkal kellett szembesülniük (pl. interoperabilitás, STANAG) és a vegyivédelmi és vegyifelderítő szakanyagok cseréjét zökkenőmentesen, a szükségleteknek megfelelően tervezetten kellett végezniük (általában forráshiányos költségvetés mellett). Ebben az időszakban a hazai fejlesztés háttérbe szorult és a külföldről importált eszközök/berendezések vették át a korábbi eszközök helyét. Az MH vegyivédelmi szakmai felső vezetése törekedett a „kiváló minőségű, NATO kompatibilis", lehetőleg „hazai forrást is igénybe vevő" beszerzések lebonyolítására.

Az 1990-2002 évben kerültek rendszeresítésre az alábbiakban ismertetett eszközök. [12]

A CALID-3 kimutató papír az egyéni vegyivédelmi felszerelés fontos kiegészítője, levegőben, terepen, technikai eszközön vagy felszerelésen MHA cseppek és aeroszolok jelenlétét jelzi (G, H, V anyagok szerinti csoportosításban, eltérő színjelzéssel). A kimutatás elve, hogy a kimutató papírban lévő színezék (indikátor) anyag a cseppfolyós mérgező harcanyagban oldódik, miközben jellemző színváltozás jön létre. A mellékelt színetalonok segítségével következtetni lehet a mérgező harcanyag típusára. Az egyes mérgező harcanyagokra jellemző színelváltozás: G (idegméreg) - sárga, H (hólyaghúzó) - vörös, V (V-anyagok) - sötétzöld színetalonokat. A működési elvből következően egyes anyagok, így például az üzemanyagok, rovarirtó szerek, fagyálló folyadékok, valamint a nedvesség zavarják a kimutatást. Egyszerű, olcsó, de nem specifikus eszköz.

A *CAM* (Smiths Detection, Nagy-Britannia) típusú vegyijelző készüléket elterjedten használják a NATO tagországok hadseregeiben, az MH-ban is rendszeresítették. Hordozható (kézi) készülék, amely érzékeli és kijelzi az idegmérgek (G üzemmód) vagy a hólyaghúzó mérgező harcanyagok (H üzemmód) levegőben való jelenlétéből származó veszélyt. A készülék „plusz" üzemmódban klór, foszgén és HCN érzékelésére is alkalmas. A kimutatás fizikai elven, az un. ion mozgékonysági spektrometria elvén (IMS) alapul, vegyvédelmi öltözetben is könnyen kezelhető, nappal és éjszaka is egyaránt használható. A CAM-nek két üzemmódja van, amelyet a G/H üzemmód választó nyomógombbal lehet kiválasztani. G üzemmódban az ideggázokat érzékeli, H üzemmódban pedig a hólyaghúzókat.



5. Kép. CAM-2 hordozható vegyijelző

A GID-3 a CAM-2 járműfedélzeti változata, az idegmérgek és a hólyaghúzó mérgező harcanyagok jelenlétét már igen alacsony koncentráció esetén érzékeli. A szintén ionmozgékonyság tömegspektrometria elvén működő kétkamrás GID-3 már nem egy, hanem két béta radioaktív forrást tartalmaz.



6. Kép. GID-3 járműfedélzeti vegyijelző

A GTI-4 intelligens négycsatornás gáz-távadót elsősorban katasztrófavédelmi alkalmazásokra fejlesztette a Gamma Zrt. (Magyarország), de telepítve van az MH által üzemeltetett Automata Mérő és Adatgyűjtő Rendszer (AMAR) állomások egy részére is, az egyes telepítési helyek környezetében előforduló toxikus és robbanásveszélyes ipari gázok monitorozása céljából, jelenleg kísérleti üzemben működnek.



7. Kép. GTI-4 gáz-távadó

A cikkben az MH Havária laboratóriumánál meglévő, speciálisan „katasztrófavédelmi céljára beszerzett vegyifelderítő eszközöket nem tárgyalom. A 2002 év óta a vegyifelderítő eszközök tekintetében jelentős áttörés nem történt.

Összefoglalás

A cikkben röviden áttekintettem a MN-ben korábban és az MH-ban jelenleg is rendszeresített vegyivédelmi technikai eszközök közül a vegyifelderítő eszközök fejlődését, az elmúlt 60 év során végbement óriási eszköz (és érintőlegesen az eljárásbeli) változást.

A hidegháború időszakát vizsgálva megállapítható, hogy a vegyi csapatok és az összfegyvernemi, fegyvernemi, és szakcsapatok korszerű vegyi (és sugárfelderítő) eszközökkel illetve megfelelő védőképességet nyújtó védőeszközökkel, a korábbinál korszerűbb csapatmentesítő eszközökkel való ellátása lényegesen növelte a vegyi csapatok teljesítő képességét, hatékonyságát, védettségét, ezáltal harcképességük megóvásnak lehetőségeit. A fejlődés legszembetűnőbb példája a vegyifelderítő eszközök fejlődési üteme volt. Az 1950-es évek kezdetleges eszközeitől (a szudánpor szóró doboztól) eljutva a 60-as évek végéig a 66M VFK, az AVJ-1 és FVJ vegyijelző készülékekkel a MHA jelenléte a vegyi-sugárfelderítő gépjármű elhagyása nélkül, a műszerekről való közvetlen leolvasással megállapítható, ezáltal teljesen kiküszöbölték a vizuális (szubjektív) módszerek alkalmazását. A vegyivédelmi főnökök, törzsek és sorállomány az „új" technikával való ellátás folyamatával párhuzamosan megjelenő szabályzatok, segédanyagok (technikai utasítások, vegyi-sugárfelderítési utasítások, módszertani segédletek stb.) segítségével a kiképzéseken igyekeztek elsajátítani az új eszközök használatát, kezelését, alapvető műszaki-technikai kiszolgálási lépéseit. [13]

A NATO csatlakozás előtti és a napjainkig tartó időszakot vizsgálva (1990-2010) a (katona-) politikai-gazdasági és társadalmi elvárások a haderő folyamatos átalakítását, a haditechnikai eszközök fejlesztését és létszám folyamatos csökkentését jelentette, amely alapjaiban hatott a vegyivédelmi szolgálat eszközrendszerére is. Az 1990-2007 közötti létszámcsökkentés a vegyivédelmi szakcsapatokat is „mélyen" érintette, a csapat- és létszámcsökkentés a felderítő eszköz szükségletben is megmutatkozott, számos tapasztalt szakember „kiáramlott a rendszerből". A szükséglet csökkentése a hazai (önálló) gyártói kapacitás megszűnéséhez is vezetett.

Az eszközök műszaki-technikai szempontból vizsgálva megállapítható, hogy a jelenleg (hatályos vegyivédelmi „normában" szereplő) rendszeresített felderítő eszközeink korszerűek, a NATO más hadseregeiben is alkalmazzák („kompatibilisek"), többsége külföldi gyártótól származik, ezáltal szinte minimális a magyar gyártói és szerviz kapacitás és hozzájárulás. A „talpon maradt" és még meglévő szakcsapatokat, a HM Fejlesztési és Logisztikai Ügynökség Technológiai Igazgatóság (HM FLÜ TI) fejlesztési kapacitását és eszközgyártó-forgalmazó vállalkozásokat padig továbbra is fenn kell tartani, hogy az MH vegyivédelmi szakalegységei és a magyar hadiipar ne csak az íróasztalon, papíron létezzen.

A vegyivédelmi technika fejlődése – a felmerülő nehézségek ellenére- napjainkban lassuló ütemben folytatódik, de hatásai szerteágazóak. A vegyivédelmi technikai eszközök fejlesztésének üteme a biztosított költségvetési források szűkülése miatt csökkent ugyan, de szerencsére teljesen nem torpant meg. A NATO doktrínák, szabványok (STANAG), eljárások és új eszközök megjelenése rányomja bélyegét a kiképzésre, az eszközök bonyolultsága (és ára) pedig anyagi-technikai kiszolgálás felelősségét pedig megsokszorozza.

Köszönetnyilvánítás:
Köszönöm Baumler Ede (Gamma Műszaki Zrt. Műszaki igazgatója) részére a szakirodalmi segítséget és a rendelkezésünkre bocsátott szakmai anyagokat, fényképeket.

Felhasznált irodalom

[1] Ordasi István mk. őrgy.: A vegyivédelmi technikai eszközök fejlődésének rövid történeti áttekintése, Vegyivédelmi Évkönyv, MN Vegyivédelmi Főnökség kiadása, (1968), 204 - 212 pp.

[2] Schrönberger Károly őrgy.: A VX anyagok harci alkalmazása és az ellenük való védelem, Vegyivédelmi Évkönyv, MN Vegyivédelmi Főnökség kiadása, (1970), 48. p.

[3] Erdős József: Szudán portól az automata műszerekig, Vegyivédelmi Jubileumi Évkönyv, MN Vegyivédelmi Főnökség kiadása, 1975, 113-115. pp.

[4] Erdős József, Pintér István, Solymosi József (2003): Magyar ABV védelmi technikai almanach. In: Az ABV eszközök gyártói és fejlesztői, Zrínyi Miklós Nemzetvédelmi Egyetem Vezetés- és Szervezéstudományi Kar Vegyi és környezetbiztonsági tanszék, egyetemi jegyzet, 203-205. pp.

[5] Erdős József, Pintér István, Solymosi József (2003): Magyar ABV védelmi technikai almanach. In: A MN-ben rendszeresített ABV védelmi eszközök, Vegyi felderítő és időjárásjelző eszközök, Zrínyi Miklós Nemzetvédelmi Egyetem Vezetés- és Szervezéstudományi Kar Vegyi és környezetbiztonsági tanszék, egyetemi jegyzet, 135-143. pp.

[6] FVJ Műszer Műszaki Leírása, Kezelési Utasítása és Törzskönyve, A Műszaki kiszolgálás, tárolás és szállítás előírásai (kiadó és évszám nélkül)

[7] GVJ Technikai Törzskönyve Műszaki Leírása és Kezelési Utasítása (kiadó és évszám nélkül)

[8] VLG-71 Kezelési Utasítása I. és II. rész, (kiadó és évszám nélkül)

[9] Erdős József mk. alez.-Ordasi István őrgy.: A vegyi és sugárfelderítő eszközök fejlődését meghatározó tényezők, Vegyivédelmi Évkönyv, MN Vegyivédelmi Főnökség kiadása, (1968), 216-217. pp.

[10] Baumler Ede: Vegyivédelmi műszerek hazai fejlesztése, gyártása a múltban és a jelenben, Haditechnika, 2002/1 szám 19. p.

[11] Erdős József, Pintér István, Solymosi József (2003): Magyar ABV védelmi technikai almanach. In: Kitekintés-1990-es évek – NATO csatlakozás, Zrínyi Miklós Nemzetvédelmi Egyetem Vezetés- és Szervezéstudományi Kar Vegyi és környezetbiztonsági tanszék, 2003, Budapest, egyetemi jegyzet, 120-121. pp.

[12] Képes ismertető az ABV felszerelésekhez, az MH Vegyivédelmi Technikai Szolgálatfőnökség Kiadványa, 2002, Budapest (oldalszám nélküli kiadvány, CAM-2, CALID-3, Kimutatócső készlet leírása)

[13] Medvecz Sándor alez.: A tömegpusztító fegyverek elleni védelem és a vegyi biztosításkapcsolata, Vegyivédelmi Évkönyv, MN Vegyivédelmi Főnökség kiadása, (1972), 197.-198. pp.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Bugyjás József
bugyjas.jozsef@kvk.uni-obuda.hu

EFFECTS ON THE MODELING RESULTS OF INCREASING FINITE ELEMENT NUMBERS

Absztrakt/Abstract

Jelen tanulmány egy robbanás folyamatát vizsgálja. Egy olyan véges elem számítógépes modelljét mutatja be, amely a folyamat matematikai modelljére épül. A cél a modell és az elméleti eredmények összehasonlításával a lehetőségek tanulmányozása, valamint a korlátok javítása.

This study deals with the analysis of an explosion process. Model has been created by a Finite Element Model Software run on computer, according to the process of mathematical modeling. It studies the possibilities and limits for improvement of the model by comparing the theoretical and model results.

Kulcsszavak/Keywords: *véges elem, robbanás, modellezés ~ finite element numbers, explosion, modelling*

1. PROCESS OF MATHEMATICAL MODELING

In the methodes using FEM[1] a methode focusing on mathematics has been chosen for modeling the explosion process. This methode is the mathematical FEM. [1] Steps of the process are illustrated on Figure 1.

[1] FEM = Finite Element Methode

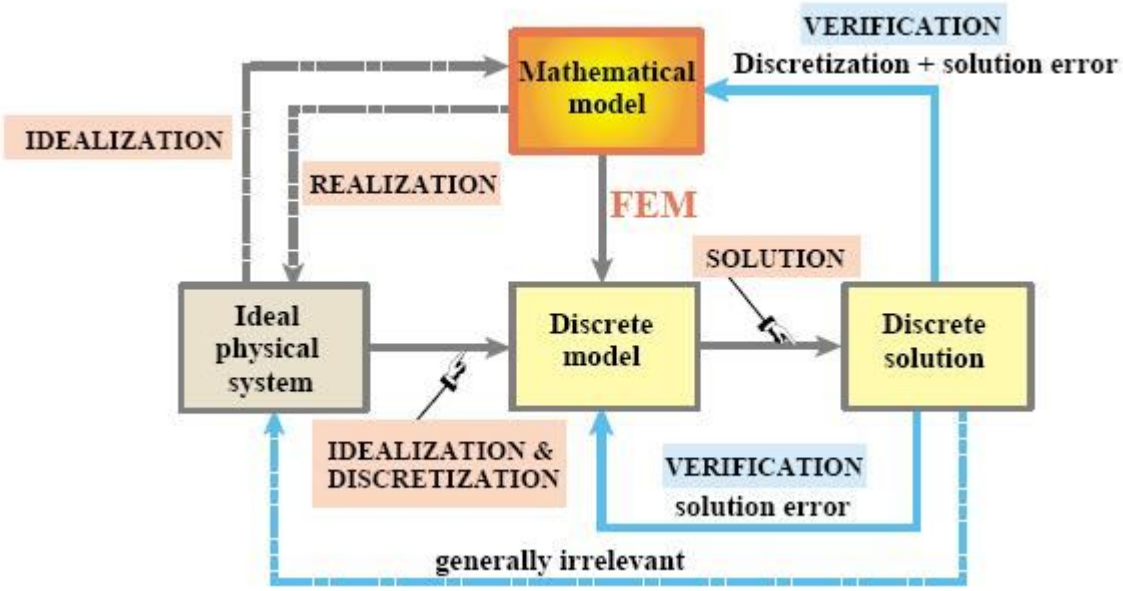


Figure 1. Mathematical FEM model [1]

Source of the proccess is mathematical model, which often is an ordinary – or partial differential equatation in space and time. A discrete finite element model is generated from a variational – or weak form of the mathematical model.

The concept of error arises when the discrete solution is substituted in the „model". This error is the amount by which the discrete solution fails to satisfy the discrete equations. This error is relatively unimportant, when using computers, and in particular direct linear equation solvers, for the solution steps.

More relevant is the discretization error, which is tha amount by which the discrete solution fails to satisfy the mathematical model.

Replacing into the ideal physical system would in principle quantify modeling errors, but this substitution in the mathematical FEM this is largely irrelevant, since the ideal physical system is merely a figment of the imagination.

2. THE MATHEMATICAL MODEL, THEORETICAL BACKGROUND

Detonation of high explosives is a mechanism when „high power" materials release their chemical energy. The chemical reaction, causing the release of energy, takes place in a narrow zone. This reaction zone propagates at high speed through the explosive that transforms the sloide explosive into hot compressed gases. This reaction zone has then a form of discontinouos wave similar to a shock wave, and has a pysical behavior which is determined solely by the properties of the unreached and completely reacted material on either side of the wave. This allows usage of the hydrodinamic approach of detonation .

Hydrodynamic Theory of Steady-state Plane Detonation [7]

The modell of the plane, steady-state reaction zone propagating at a constant speed D through the explosive is illustrated in Figure 2.

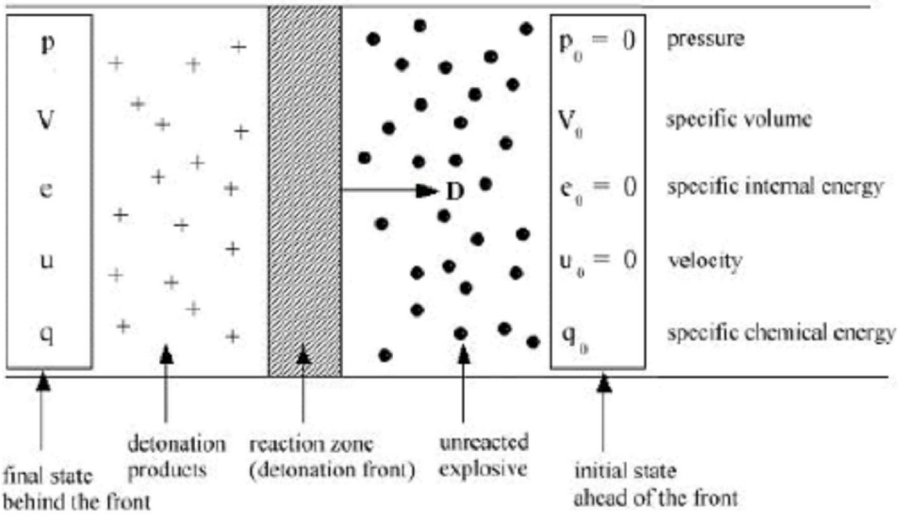


Figure 2. Plane Reaction Zone Propagating at Constant Speed

The Rankine-Hugoniot relations, which express the conservation of mass, momentum and energy in the material stream flowing through the reaction zone can be used to relate the hydrodynamic variable across the reaction zone.

Conservation of mass and momentum: $$p - p_0 = \frac{D^2}{V_0^2}(V_0 - V) \qquad (1)$$

Conservation of energy: $$e - e_0 = \frac{1}{2}(p + p_0)(V_0 - V) + q_0 \qquad (2)$$

Equation (1) describes a straight line (Rayleigt-line) determining the locus of all possible final states (p, V) , attainable by a continuous transition from the initial state (p_0, V_0) consistent with conservation of mass and momentum.

Equation (2) is merely thermodynamic, from which, with a given,equation of state p=p(V,e) relevant for the detonation products, the energy term can be eliminated , and results the Hugoniot curve of the explosive. The downward concave curve defines locus of all possible finals states (p, V) available by a discontinuous transition ffrom the initial state (p_0, V_0), consistent with conservation of energy. (Figure 3.)

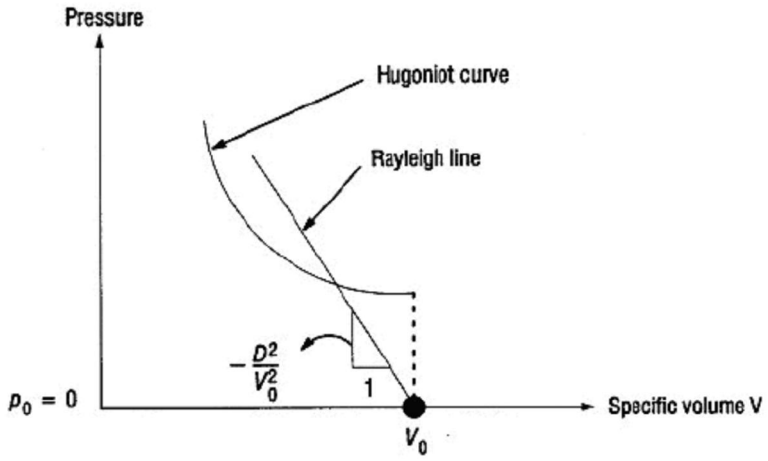


Figure 3. Hugoniot curve and Rayleigh straight

Forms of the Rayleigh straight and the Hugoniot curve are such that their interaction permits the existence of any detonation speed D above a „minimum value" and each value of D is consistent with two possible final states for the detonation products. There is one more condition required, which was supplied by Chapman and Jocquet, who added the following condition to conservation of mass, momentum and energy:

The detonation speed D is either such that the Rayleigh line is tangent to the Hugoniot curve of the explosive, or the detonation speed is the minimum velocity consistent with the Rankine-Hugoniot relations.
This process

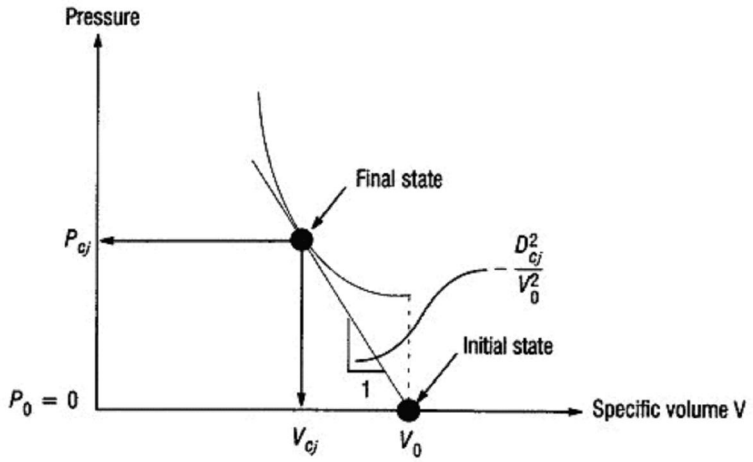


Figure 4. Hugoniot curve and Rayleigh straight in detonation process

According to the above considerations, when the ideal gas equation of state (with constant specific heat ratio γ) is to model the detonation products, the above formulas result:

$$P_{cj} = 2(\gamma - 1)q_0 p_0 \qquad (3)$$

$$V_{cj} = \frac{\gamma}{\gamma + 1} V_0 \qquad (4)$$

These relations can be applied also when using the JWL equation of state (with variable specific heat ratio) when measuring γ_{cj} at the Chapman-Joguet state (P_{cj}, V_{cj}) is behind the detonation front.

JWL Equation of State for Explosive Charges

The Jones-Wilkens-Lee (JWL) equation of state [2] is modeling the pressure, which is generated by the extension of chemical explosive material detonation. This formula is widely applied for engeenering calculations. It can be described by the bellow formula:

$$P = C_1\left(1-\frac{\omega}{R_1 v}\right)e^{-\eta v} + C_2\left(1-\frac{\omega}{R_2 v}\right)e^{-\eta v} + \frac{\omega e}{v} \qquad (5)$$

Where v is the specific volume, e is the specific energy, C_1, C_2, R_1, R_2, ω are dynamic coefficients of well-known explosive materials [3].

3. FEM PROGRAM APPLIED

MSC Dytran is a general-purpose, three-dimensional explicit finite element analysis sotware for simulating and analysing extreme short-duration events involving deformation of structural materials and the interaction of fluids and structures. For the easy modeling Dytran combine in a special way the finite element methode with mechanics of fluids.

The MSC Dytran Explicit FEA nonlinear solver technologies are used to analyse extreme, short duration, transient events within Lagrange and Euler domain. It can be used to examine modeling shocks, impacts, nonlinear lost of stability. It permits also simulation of interaction between stabile structures and fluids. MSC Dytran Models can be generated and analysed by MSC Dytran software .

The Patran is an open, user-friendly MCAE[2] application including a professional pre-and postprocessor.

4. MODELING OF CONSTANT DETONATION

For the simulation an average explosive, called Comp.B material has been chosen , which can be a reference in the future. Parameters of the detonation are included in the table 1.

	C_1 (10^{11}Pa)	C_2 (10^9 Pa)	R_1	R_2	ω	e_0 (MJ kg^{-1})	VOD (m s^{-1})	ρ_0 (kg m^{-3})
COMP.B	5.242	7.678	4.2	1.1	0.34	4.969	7980	1717

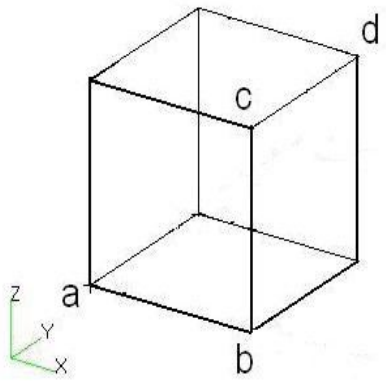
Table 1. JWl parameters of explosive used for modeling

e_0 specific chemical energy; VOD is C-J explosion speed

[2] Mechanical Computer-Aided Engineering

Target of the simulation consists in modeling the explosion of the material, verifying pressure behind the detonation front against theoretical Chapman-Jouguet value, and monitoring formation and expansion of shockwaves. [4]

The software applied uses the so-called „programmed burn" technology for the modeling of detonation of high-explosive materials. Basic condition of this technology consist in the fact, that reaction zone is constant in all directions, and it expands by the Dcj explosion speed of Chapman-Jouguet. As soon as it achieves and passes an element, the chemical energy develops proportionally on the element in the „burning time".
For the modeling of the detonation a cube of 15 mm edge was created. Nodes designed on Figure 5. are primary nodes for the tests since our further analysis will cover also the solids touching with explosive. We examined temporal procession of burning in the nodes, formation of pressure between nodes a-b, and also procession of pressure on „ab", „bc" and „cd" sections in certain moments.
The explosive charge was divided in four ways along the side edge of the cube.



Scaling:

Figure 5. Marks of explosive

1st. case 0.003 [mm] therefore 216 nodes and 125 Hex 8 elements set.
2nd. case 0.001 [mm] therefore 4096 nodes and 3375 Hex 8 elements set.
3rd. case 0.0005 [mm] therefore 29791 nodes and 27000 Hex 8 elements set.
4th. case 0.0003 [mm] therefore 132651 nodes and 12500 Hex 8 elements set.

Further reduction of the scale and therefore increase of number of elements was not possible due to limited memory capacity of the PC.

During program running following parameters and requirements wre used:
Duration of test: 5·10-6 [sec] (ENDTIME)
Data types to be displayed in 1·10-7 [sec] periods (TIMES)
Minimal and maximal intervals of analyse $1 \cdot 10^{-8}$ [sec] and $1 \cdot 10^{-7}$ [sec] (PARAM, MINSTEP; PARAM, MAXSTEP)
Hydrodynamic therories were assigned to the elements of the explosive charge (PEULER,1,1,Hydro)
Starting point of the detonation is point „a" with coordinates (0,0,0).

Geometric disposition, finite element network, material characteristics, starting conditions and requirements needed for the evaluation were given in the MSC Patran software, which generated a „.dat" extension file as a result for MSC Dytran.

Generated source file is the same in all four test cases. Discrepency was only in the „.bdf" extension file, where according to the scale other nodes and elements were used.

After running of the „.dat" extension file with MSC Dytran software, differeint type of files are generated, from which the following files can be processed further on:

.OUT MSC Dytran output file
.ARC MSC Dytran archive file, which permits MSC Patran postprocessing, that means evaluations and analysis of data.
_ERROR_SUMMARY.MSG Error messages during the FEM program running.

5. RESULTS, CONCLUSIONS

Results of the burning process

Analysis for all four cases were executed wih MSC Patran. Figures illustrating the burning process:

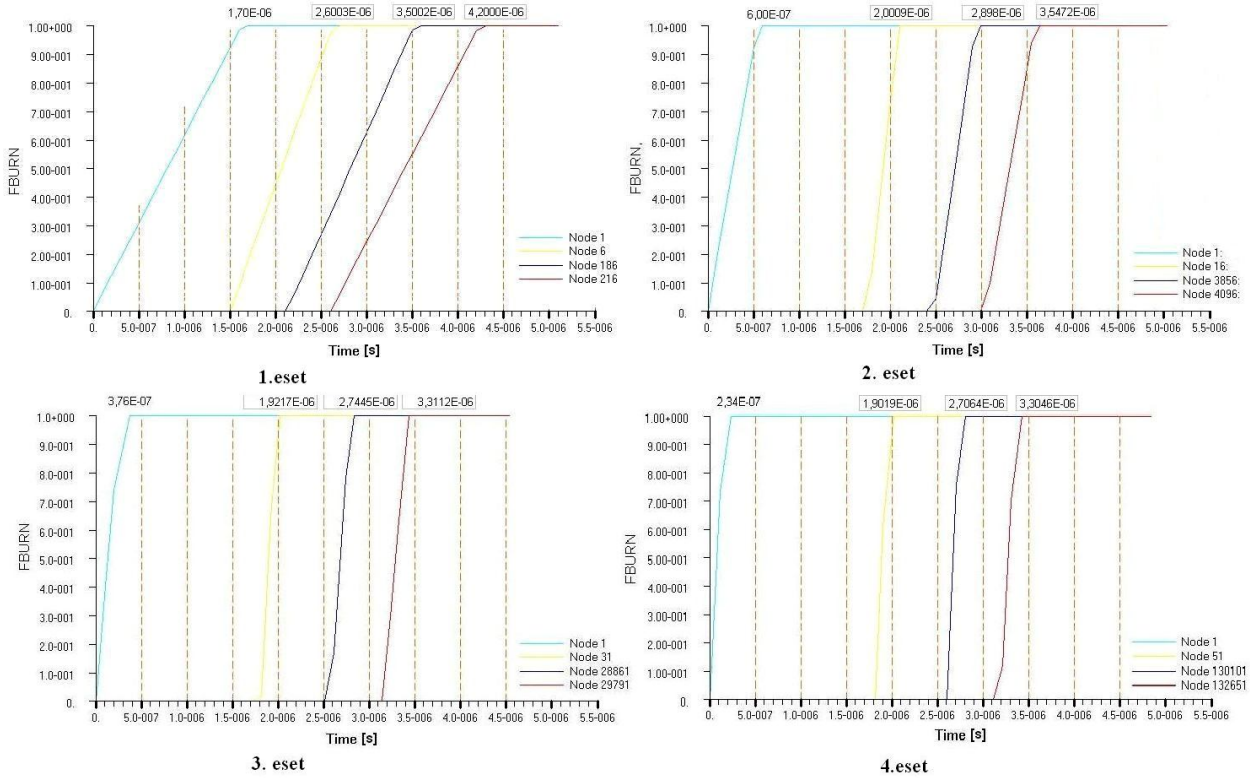


Figure 6. Burning processes of emphased nodes

Result data gave base for the examination of burning speeds,and they were compared with the theoretical 7980 [m/s] speed.
Data and results are included int he Table 2.

		a-b distance	a-c distance	a-d distance
		0.015[m]	0.0212132[m]	0.0259807[m]
1st case	Time needed for total burn[10^{-6} s]	2,600280	3,500219	4,200000
	Burning speed [m/s´]	5768,610359	6060,535819	6185,895594
	Compared to the reference [%]	**72,2884**	**75,9466**	**77,5175**
2nd case	Time needed for total burn [10^{-6} s]	2,000885	2,897841	3,547241

	Burning speed [m/s´]	7496,682397	7320,346986	7324,217622
	Compared to the reference [%]	**93,9434**	**91,7337**	**91,7822**
3rd case	Time needed for total burn [10^{-6} s]	1,921741	2,744498	3,311228
	Burning speed [m/s´]	7805,421096	7729,355126	7846,261034
	Compared to the reference [%]	**97,8123**	**96,8591**	**98,3241**
4th case	Time needed for total burn [10^{-6} s]	1,901888	2,706447	3,304630
	Burning speed [m/s´]	7886,898639	7838,026208	7861,927456
	Compared to the reference [%]	**98,8333**	**98,2209**	**98,5204**

Table 2. Comparison of burning speed with theoretical value

Analysis of results lead to the following conclusions:

1. The software chosen is suitable for the analysis and presentation of the process on PC.
2. Theroretical value can be accessed by the refinement of the finite element network . Comparison of the first and second case shows that trisection of the scale leads to a 20% improvement of the precision.
3. The needed precision fineness, which permits scientific tests can be defined and also can be applied on PC.

REFERENCES

[1] C. A. Felippa: Introduction of Advanced applications of FEM http://www.colorado.edu/engineering/cas/courses.d/IFEM.d/IFEM.Ch01.d/IFEM.Ch01.Slides.d/IFEM.Ch01.Slides.pdf

[2] Lee E.L., Hornig HC, Kury 3W. Adiabatic expansion of high expiosive detonation products, UCRL-50422.: Lawrence Radiation Laboratory, University of California; 1968.

[3] Lee, E.L. and Tarver, C.M., "Phenomenological Model of Shock Initiation in Heterogeneous Explosives," Physics of Fluids 23 (12), December 1980, pp. 2362-2372

[4] Cooper, Paul W., Explosives Engineering, New York: Wiley-VCH,1196. ISBN 0-471-18636-8

[5] Benson DJ. Computational methods in Lagrangian and Eulerian hydrocodes. Comput Methods Appi Mech. Eng 1992;99:235—394.

[6] Salas, M. D. "The Curious Events Leading to the Theory of Shock Waves, Invited lecture, *17th Shock Interaction Symposium*, Rome, 4-8 September 2006

[7] Mader Ch.L., Numerical modeling of explosives and propellants, 2nd edition,CRC Press ISBN 0-8493-3149-8

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Bunyitai Ákos
bunyitai.akos@gmail.com

TERAHERTZ-ES TECHNOLÓGIA ALKALMAZÁSA A BIZTONSÁGTECHNIKÁBAN

Absztrakt

Jelen tanulmány röviden összefoglalja azokat az ismereteket, amelyek napjainkban a világ számos fejlett országában elterjedőben lévő elektromágneses sugárzás TeraHertz spektrumának a biztonságtechnikában lévő alkalmazásának alapjai. Tudományos kutatások eredményeire támaszkodva objektíven vizsgálja a THz-es technológia előnyeit, hátrányait. Célja, hogy a felhasználók, érdeklődők, biztonságtechnikával foglalkozók alapvető kérdéseire – a találgatások és félreértések homályából kiemelkedve – választ adjon.

This article gives a breef summary of the basics of the utilization of TeraHertz spectrum of the electromagnetic radiation for security purposes spread in a number of developed countries in the world. The purpose is to give an objective survey highlighting the advantages and drawbacks of the THz technology based on the results of scientific research clarifying the risen guessings and the misapprehensions for the forthcoming users, inquirers and security officers.

***Kulcsszavak**: THz, TeraHertz, biztonságtechnika ~ THz, TeraHertz, security*

BEVEZETÉS

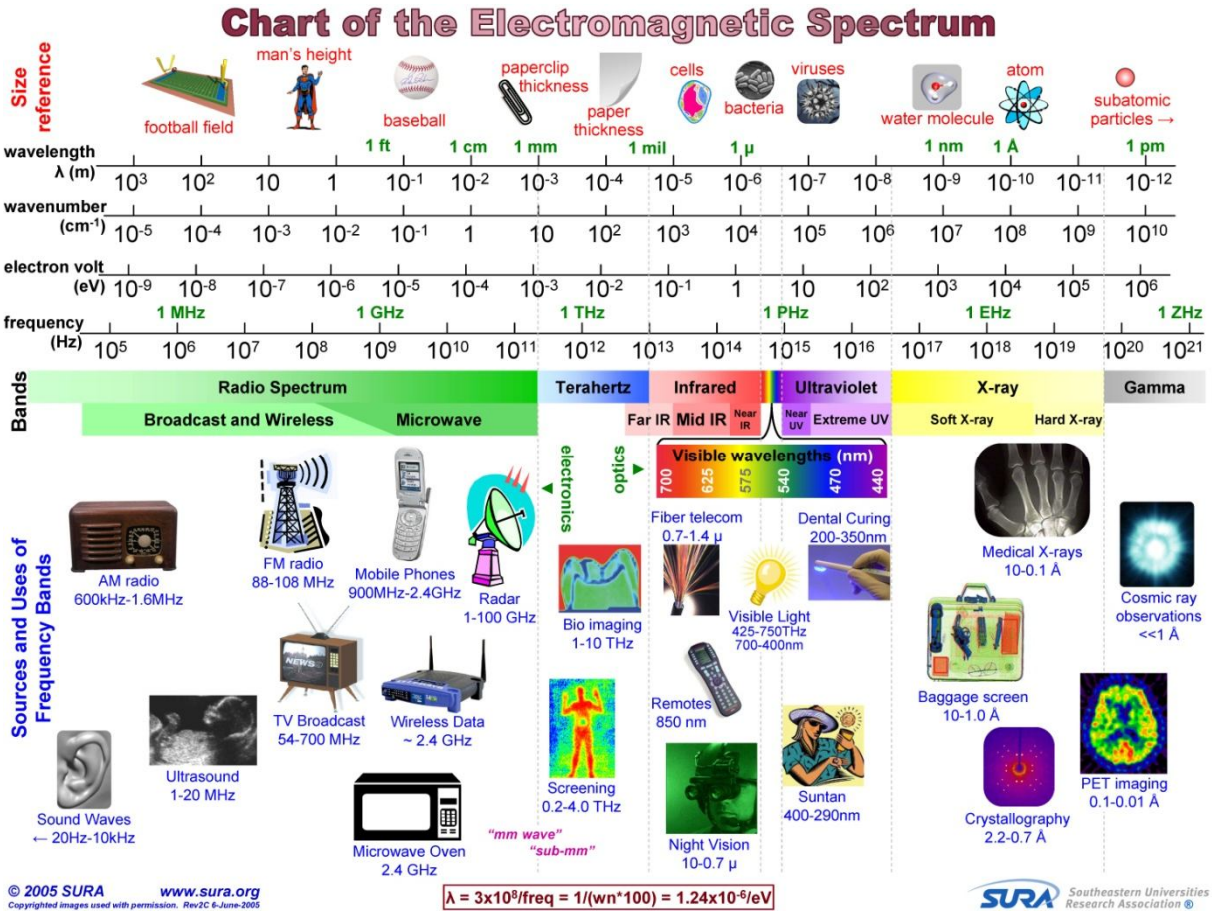
A 2001. szeptember 11-i terrortámadás óta egyre nagyobb nyomás nehezedik a biztonságtechnikával foglalkozókra. Az általános fenyegetettség éberségre szólítja fel az állampolgárokat éppúgy, mint az utcán járőröző rendőröket vagy a repülőtéri utasbiztonsági ellenőröket. A magas szintű elvárásoknak eleget téve a fegyveres testületek képzik a személyi állományt, tesztelik a szabályzatokat és természetesen folyamatosan fejlesztik eszközeiket.
A napjainkban egyre inkább elterjedő személyvizsgáló berendezések terén kiemelkedő újításnak tekinthető, hogy az elektromágneses sugárzás – a biztonságtechnikában ezidáig nem alkalmazott – TeraHertz spektrumában dolgoznak. Ezzel elérhető, az eddigi technológiákhoz képest magasabb biztonsági szint garantálása, használatuk pedig egyszerű és gyors. Az egészségre nézve minimális kockázattal járnak és nem sértik az emberi méltóságot. Típustól függően alkalmazhatók – többek közt – kiemelt objektumok, rendezvények beléptetésénél,

repülőtéri utasbiztonsági ellenőrzéseknél, vagy akár pályaudvarokon, az utazóközönség szúrópróba-szerű ellenőrzésére.

A cikk célja, hogy biztonságtechnikai oldalról közelítve röviden bemutassa a TeraHertz-es technológiát, illetve néhány tipikus eszközt, melyek alkalmazzák azt.

1. ÁLTALÁNOSSÁGBAN A T-HULLÁMOKRÓL

Prévost tételének kimondása óta tudjuk, hogy minden – 0 K feletti hőmérséklettel rendelkező – test környezetének hőfokától függetlenül elektromágneses sugárzást bocsát ki (és egyidejűleg el is nyel). Az elektromágneses sugárzás jellemzője a hullámtermészet, a terjedési sebesség (v), hullámhossz (λ), frekvencia (f), sugárzás erőssége. A TeraHertz-es hullám vagy T-hullám (T-ray) olyan elektromágneses sugárzás, mely hullámhosszát tekintve a mikrohullám felső határa és a távol-infravörös között helyezkedik el (1. ábra), vagyis 3 mm ($3*10^{11}$ Hz) és 300 mikrométer ($3*10^{12}$ Hz) közé tehető. /A THz tartományt sok esetben 100 GHz és 10 THz közé teszik./ Gyakorlatilag az elektronika és az optika határán foglal helyet, ezért tényleges alkalmazására évtizedeken keresztül nem volt technikai lehetőség (ld. 1.1. Rövid történeti áttekintés).



1. ábra. Az elektromágneses sugárzás spektrumai szemléletesen: a diagram – a könnyebb áttekinthetőség érdekében – kiegészül a hullámhossz nagyságát és az alkalmazást bemutató ábrákkal

A mai műszaki színvonal azonban lehetővé teszi, hogy alacsony energiájú TeraHertz sugárzást állítsunk elő és detektáljunk. Ez nem ionizáló hatású sugárzás, vagyis a tudomány

mai állása szerint nem roncsolja a vele kölcsönhatásba kerülő anyagokat. A semleges molekulákat, atomokat nem bontja pozitív ionokra és negatív elektronokra. Hullámhossztól és energiától függően áthatol(hat): füstön, ködön, papíron, kartonon, műanyagon, kerámián, fán, ruhaszöveten, vékonyabb falakon. A mikrohullámú technikából ismeretes skin effektus (örvényáramú veszteség) miatt az anyag vezetőképességével fordítottan arányos a behatolóképessége. Nem hatol át például a fémeken. Az ember testének kb. 70%-a víz, ezért a kültakaró alá ~1 cm mélységig lehet „belátni". Ennek oka, hogy a bennünk lévő nedvesség jelentős része izotóniás oldatként van jelen, ami erősen abszorbeálja a THz-es hullámokat. A szaru (haj, szőrzet, köröm) kisebb arányban tartalmaz elektrolitot.

Egy test abszorpcióképességén (elnyelőképesség, a) értjük a rá eső sugárzás energiájának azon tört részét, amelyet elnyel (nem ereszt át és nem ver vissza). Emisszióképességen (e) azt az elektromágneses energiát értjük, amelyet a test egységnyi felületen egységnyi idő alatt egységnyi térszögbe kibocsát. A test abszorpcióképessége és emisszióképessége anyagfüggő (ennek jelentőségét ld. 2. A THz-es technológia a biztonságtechnikában). Abszolút fekete testnek hívjuk azt a testet, amely a ráeső bármely hullámhosszúságú sugárzást teljesen elnyeli (tehát: a = A = 1, e = E). Kirchhoff törvénye kimondja, hogy az e/a hányados minden testre vonatkozóan azonos és csak a sugárzás hullámhosszának (λ) és a test hőmérsékletének (T) függvénye (nem függ az anyag minőségétől). Ez a függvény az abszolút fekete test emisszióképessége [3]:

$$\frac{e\,(\lambda, T)}{a\,(\lambda, T)} = E\,(\lambda, T)$$

1.1.Rövid történeti áttekintés

A TeraHertz-es spektrum kutatása hadászati célból kezdődött az 1950-es években. Széleskörű kihasználásának és elterjedésének az akkori technika fejlettségének hiánya szabott korlátokat, t.i. előállítása és detektálása nehézségekbe ütközött. Mintegy 10 évvel később, 1963-ban J. B. Gunn gallium-arzenid félvezető eszközt készített, az ú.n. Gunn-diódát, melynek jelentősége elsősorban a mikrohullámú-, a közelmúltban azonban a TeraHertz-es technológiában figyelhető meg (ld. 1.2. Előállítás és detektálás). A THz-es sugárzás iránti érdeklődés az 1980-as években nőtt meg ismét, amikor ultrarövid fényimpulzusok segítségével $3*10^{11}$ Hz feletti egy periódusból álló hullámot állítottak elő.

A THz előállításának, detektálásának és hasznosításának kutatásával foglalkozik többek között a NASA, az ENEA, a NICT, itthon pedig a Pécsi Tudományegyetem, valamint a Budapesti Műszaki és Gazdaságtudományi Egyetem.

1.2.Előállítás és detektálás

Előállítás félvezető-technológiával: a THz-es sugárzást Kaprowicz szerint [2] legegyszerűbben a korábban mikrohullámú technológiában alkalmazott gallium-arzenid (GaAs) vagy gallium-nitrid (GaN) Gunn diódával lehet előállítani. A Gunn dióda megfelelően előfeszítve és olyan környezetben, amely rezonátorként viselkedik (csőtápvonalban vagy koaxiális tápvonalban kialakított üreg, mikrosztrip kivitel esetén λ/2 tápvonalszakasz) hangolható frekvenciájú oszcillátorként funkcionál. A hangolás történhet mechanikusan (pl. fémcsavar) vagy elektronikusan (pl. varaktor). GaAs Gunn dióda segítségével 200 GHz (felharmonikusa már THz-es), GaN diódával 3 THz frekvenciájú rezgés állítható elő. A GaAs félvezető előremutató „továbbfejlesztése" az AlGaAs, mely 600 GHz frekvenciájú oszcillátor elkészítését teszi lehetővé [9].

Előállítás optikai úton: Hebling János a közelmúltban ultrarövid lézerimpulzusok optikai egyenirányítását alkalmazta újfajta sebességillesztési elrendezésben, mely nagy hatásfokú THz-es impulzus-sorozat előállítását tette lehetővé [5].

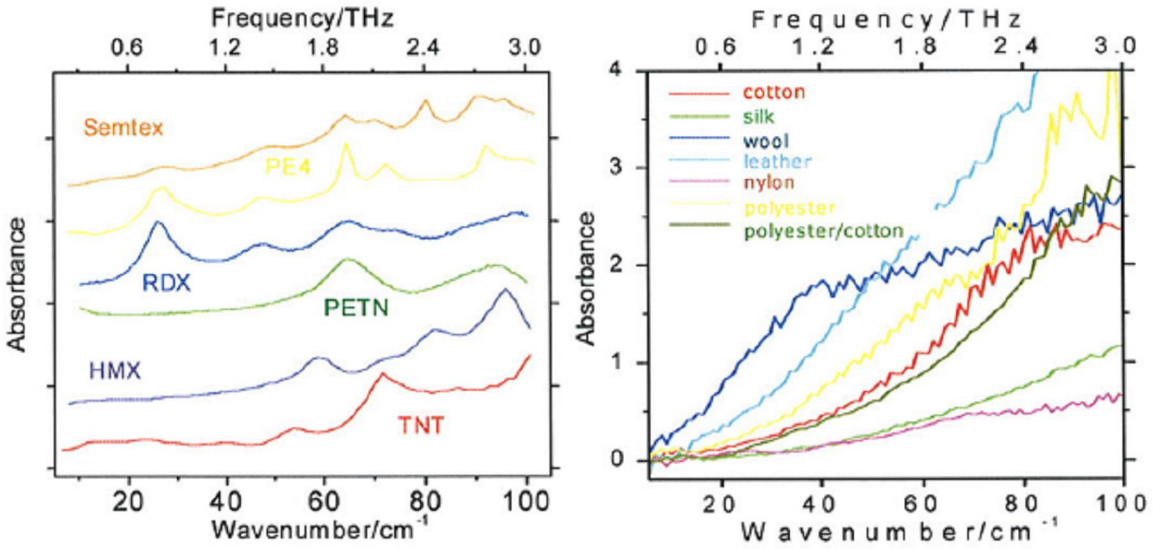
Detektálás: klasszikus eljárás alkalmazásával, a távoli infravörös sugárzásnál használt bolométerrel, valamint Golay-cellával. A bolométer működési elve röviden: a fémek hőmérséklet hatására történő elektromos ellenállásának megváltozásán alapszik. Egy nemvezető anyagra felvitt vékony germániumréteget 4 K hőmérsékletre hűtve a beeső elektromágneses sugárzás megváltoztatja hőmérsékletét és ezzel ellenállását. Hátránya a nehezen kezelhetőség. A Golay-detektor működése a gázok hőkiterjedésén alapszik. Mindkét megoldás a vizuális tartományban alkalmazott érzékelőkhöz képest meglehetősen hosszú időállandóval működik. Ismertek továbbá a THz-es sugárzás detektálására szolgáló félvezető alapú eszközök is.

1.3. Alkalmazási területei

A technológia alkalmazási területei közé tartozik az anyagvizsgálat (spektroszkópia), az orvostudomány, a rádiócsillagászat, a kommunikáció és a biztonságtechnika. Széleskörűen alkalmazható anyagok azonosítására is, kihasználva – a vizsgált anyagminőségtől függő – eltérő abszorpciós sávokat.
A továbbiakban a biztonságtechnikában történő alkalmazást vizsgáljuk.

2. A THZ-ES TECHNOLÓGIA A BIZTONSÁGTECHNIKÁBAN

A TeraHertz alkalmazása a biztonságtechnika területén nem tekint vissza nagy múltra, ám jövője megalapozottnak látszik. Felhasználható többek között levél-, csomag- és személyvizsgálatra. A különböző anyagok eltérő abszorpciós értéke „TeraHertz-es ujjlenyomatként" fogható fel. Az alábbi ábrán (2. ábra) jól látható, hogy a különböző anyagok (a bal oldali ábrán robbanóanyagok, a jobb oldali ábrán ruhaanyagok) különböző frekvencián eltérő abszorpciós értékkel rendelkeznek. /Mindkét ábránál: felső tengely: frekvencia [f] THz, alsó tengely: hullámok száma cm-enként, oldalsó tengely: abszorpció/



2. ábra. Robbanóanyagok (bal oldali ábra) és ruhaanyagok (jobb oldali ábra) eltérő abszorpciós értékeinek változása az elektromágneses hullám sűrűsége és frekvenciája függvényében

A 2. ábra rövid magyarázata: a bal oldali ábrán vizsgált Semtex, PE4, RDX, PETN, HMX és TNT robbanóanyagok eltérő (0,6-3,0 THz) frekvencián az adott anyagra jellemző, egymástól jól elkülöníthető elnyelőképességgel rendelkeznek. A jobb oldali ábrán látható cotton (pamut), silk (selyem), wool (gyapjú), leather (bőr), nylon (nylon), polyester (poliészter) és polyester/cotton (poliészer-pamut keverék) vizsgálata során kiderült, hogy a robbanóanyagoktól eltérő jellegű abszorpciós görbék miatt az anyagok automatikus detektálása lehetséges.

Jelentősége: a TeraHertz-es technológia alkalmazásával nem kell felbontanunk a levelet, hogy megvizsgáljuk: anthraxot tartalmaz vagy lisztet, hiszen a THz sugárzás a papíron áthatolva definiálhatja. Nem kell megsemmisíteni az összes őrizetlenül hagyott csomagot sem, ha – annak kinyitása nélkül „bele tudunk nézni". Természetesen nagy mértékben növelhető a közbiztonság azzal is, ha gyorsabb és alaposabb személyátvizsgálást alkalmazunk, méghozzá az emberi jogok csorbulása és egészségügyi kockázat nélkül. A THz sugárzást a biztonságtechnikában tehát anyagvizsgálatra és képalkotásra alkalmazhatjuk.

2.1. Képalkotás THz-es sugárzással

A gyakorlatban 1995-óta beszélhetünk olyan képalkotásról, mely a fent említett elektromágneses spektrumot alkalmazza erre a célra. Ennek fő oka, hogy ebben a tartományban korábban nem álltak rendelkezésre intenzív források és megfelelő érzékenységű, felbontású képérzékelők. Az eltelt 15 évben azonban sokat fejlődtek az előállításra és detektálásra szolgáló eszközök. A képfelbontást tekintve: a 10 mm-nél nagyobb tárgyak vizsgálata manapság nem jelent problémát.

A képalkotás kétféle elven jöhet létre: *passzív* és *aktív* módon.

- *Passzív* módszer, ha a testek azon tulajdonságát használjuk ki, hogy elektromágneses sugárzást bocsátanak ki. Ezt a sugárzást összegyűjtve és a THz-es tartományban vizsgálva elnagyolt képet kaphatunk (pl. ThruVision Systems T8000). A képalkotó eszköz tehát nem bocsát ki semmilyen, az élő vagy élettelen szervezetekre káros elektromágneses sugárzást.
  Ennél a módszernél – a detektálandó jel alacsony szintje miatt – kritikus a feldolgozó rendszer saját zaja, amely meghatározza a készülék és a vizsgálandó tárgy maximális távolságát a létrehozott kép elfogadható jel/zaj viszonya mellett. A képminőség pl. korellációs eljárással javítható.

- *Aktív* módszerről beszélhetünk, ha a képalkotó eszköz radar-elven működik, vagyis jól fókuszált elektromágneses hullámokkal pásztázza a vizsgálandó térrészt és a leképezni kívánt dolgokról visszaverődő hullámokat alkalmazza képalkotásra (pl. L3 communications ProVision).
  Ennél a módszernél a vizsgálandó test saját (háttér-) sugárzása hozzáadódik a megvilágításból adódó visszavert sugárzáshoz.

Egyik módszerrel sem detektálhatók testüregbe vagy bőrfelszín alá rejtett eszközök.

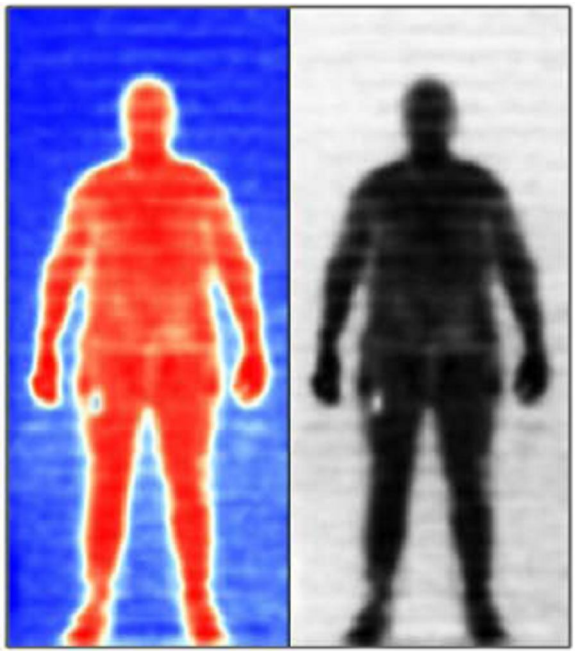
Példaként tekintsük az évek óta találgatások homályában és félreértések kereszttüzében lévő testszkennereket (ld. 2.2. és 2.3. alfejezetek)!

Fontos megjegyeznünk, hogy az Amerikai Egyesült Államok közlekedésbiztonsággal foglalkozó szervezete (TSA) jelenleg az ú.n. „backscatter" technológiát alkalmazó

berendezést is teszteli és alkalmazza (Rapiscan Secure 1000 Single Pose), melyet nem célszerű összekeverni a TeraHertz tartományban üzemelőkkel. Működése röviden: az eszköz kis energiájú röntgensugárzás segítségével a visszaverődő sugárzást detektálva krétarajz-szerű képet készít (tehát nem átvilágító, a detektor a sugárforrás felőli oldalon van) a testről elölről és hátulról [15]. Ellenőrzésenként 0,05μSv expozícióval kell számolni, ami az Amerikai Nemzeti Szabvány (ANSI 43.17) által megengedett érték 1/5-e; ez ekvivalensnek tekinthető 2 perc utazómagasságban eltöltött repülőút során minket ért kozmikus sugárzással. Az eszközből a TSA a 2010-es évben 150 db-ot tervez telepíteni az Amerikai Egyesült Államok repülőterein [16].

2.2. Egy passzív eszköz bemutatása: ThruVision Systems T8000 [17]

Működése: a vizsgálathoz semmi mást nem kell tennünk, mint a 230 kg-os szekrény méretű eszköz kamerájának látókörébe kerülni (a gyártónak természetesen létezik kisebb méretű szkennere is). Az eszköz a test által kibocsátott TeraHertz-es sugárzást összegyűjtve körvonalazott felvételt hoz létre. A szkennelés időtartama 3 és 30 s közötti. Az eszköz kb. 25 méterre „lát el", felbontása kisebb tárgyak detektálása esetén nem megfelelő a 100%-os azonosításhoz, ezért másodlagos vagy nagyobb tömeg feltűnésmentes vizsgálatához alkalmas (pl. pályaudvarokon, várótermekben, utcán lévők).
Az eredmény:



3. ábra. ThruVision Systems T8000 által készített képek, a személy jobb első nadrágzsebében 15 ml folyadék található

Az eszköznek semmilyen káros élettani hatása nem ismert, a létrehozott kép személyazonosításra alkalmatlan, illetve nem tartalmaz semmilyen részletet a vizsgált személy testéről [20].

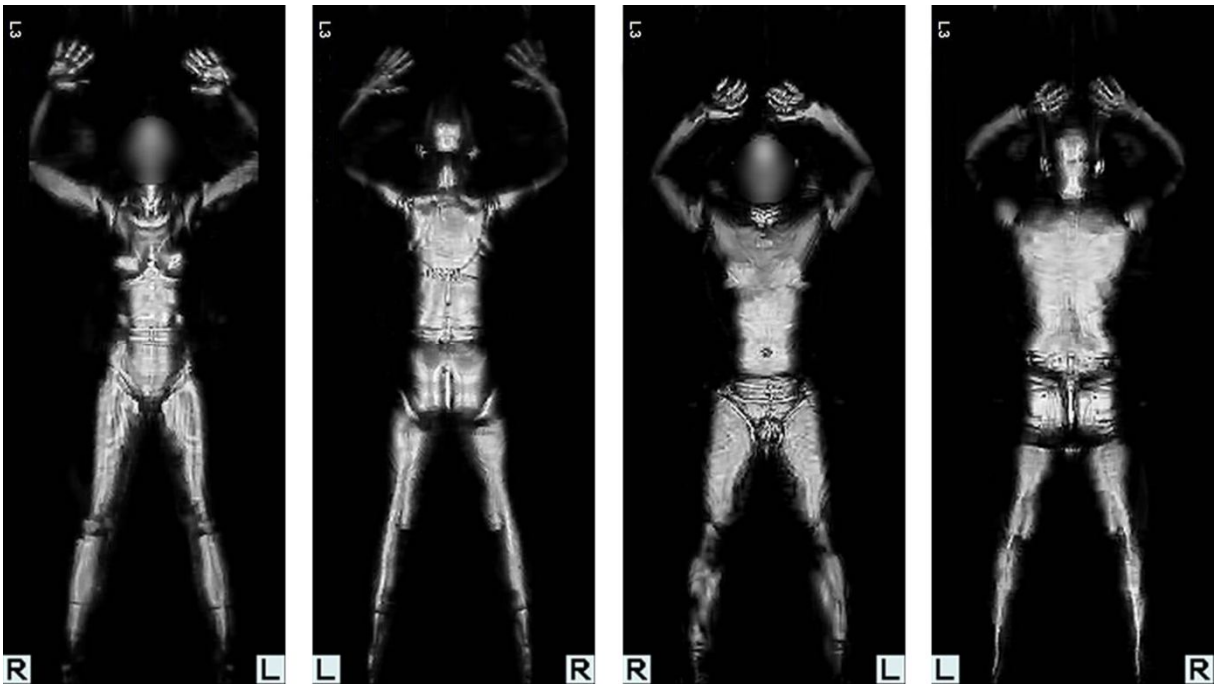
2.3. Egy aktív eszköz bemutatása: az L3 communications Security&Detection Systems fejlesztése, a ProVision nevű készülék [21]

A TSA által kiválasztott ProVision testszkennerből az USA 19 repülőterén jelenleg 40 db üzemel [16].



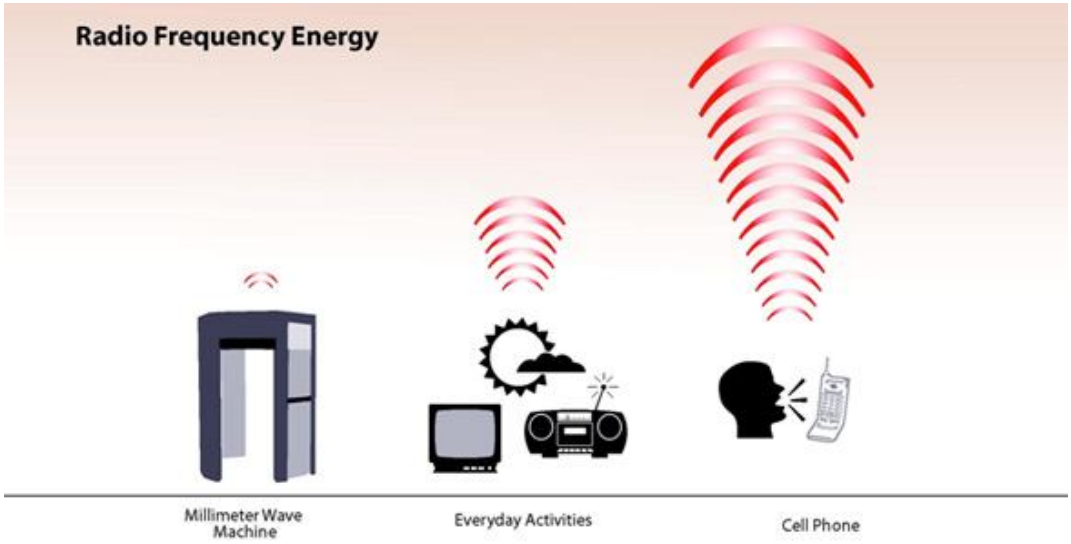
4. ábra. A ProVision szkenner

Működése: a vizsgálandó személy mindkét kézfejét fejmagasságba emelve beáll a kabinba (4. ábra) (semmilyen ruhadarabot nem kell levenni, a zsebeket nem kell kiüríteni), ahol 2 db teljes kabin magasságú adó-vevő milliméter hullámhosszúságú, nem ionizáló hullámokat (0,1-10 THz) bocsát ki. Az eszköz tehát aktív. A 2 db adó-vevő kb. 2-10 s alatt (vagyis óránként 200-400 személy vizsgálható) 1-1 félkört megtéve, teljes alapossággal „feltérképezi" a kabinban álló személyt, majd fekete-fehér 3D-s testfelszíni képet készít. Az Amerikai Egyesült Államok Kormányának hatástanulmánya megállapítja, hogy a létrehozott egészalakos képet (Whole Body Imaging: WBI) nem lehet egyenértékűnek tekinteni egy fotóval, illetve, hogy nem tartalmaz elegendő információt személy-azonosításhoz [20]. A képet egy – a vizsgált személlyel azonos nemű – utasbiztonsági ellenőr értékeli ki egy zárt, ablaktalan helyiségben, amelybe nem vihet magával semmilyen, a kép tárolására alkalmas eszközt (mobiltelefont sem). A képet a rendszer semmilyen formában nem rögzíti. A kiértékelő az ellenőrzött személy arcát (és a megrendelő igénye szerint a test egyéb részeit) maszkolva látja, sosem tudja kit vizsgált valójában, a kabinnál álló kollégájával csak annyit tud kommunikálni, hogy talált-e valamit, ami további vizsgálatot igényel vagy sem. Az eredmény:



5. ábra. ProVision által készített képek: egy hölgy és egy úr szkenner-képe elölről és hátulról

Élettani hatása: az USA kormányának 2009. júliusában kiadott hatástanulmánya szerint az eszköz által kibocsátott energia 0,00000597 mW/cm^2, vagyis 10.000-szer kisebb, mint egy adóüzemű mobiltelefoné (ld. 6. ábra) [20]. Ma Magyarországon a lakosságra vonatkozó egészségügyi határérték 300 GHz-en 1 mW/cm^2 [24].



6. ábra. A ProVision által kibocsátott energia nagysága szemléletesen, viszonyítva használati tárgyaink és mobiltelefonunk sugárzásához

A ProVision aktív testszkennerrel detektálhatóvá válnak a folyadékok, gélek, műanyagok, fémek, kerámiák, valamint a fegyverek, a robbanóanyagok, kábítószerek, pénz, stb. Az eszköz továbbfejlesztett változatán egy - a kabin külső oldalán - lévő kijelzőn megjelenő emberalak sárga téglalappal figyelmeztet a lehetséges idegen anyag jelenlétére.

3. ELŐNYÖK ÉS HÁTRÁNYOK, AGGÁLYOK

A biztonságtechnikában alkalmazott THz-es sugárzáson alapuló eszközök negatív biológiai hatásait; vallási, meggyőződésbeli, neveltetésből adódó aggályait; funkcionális előnyeit és hátrányait tárgyaljuk az alábbiakban. A fontossági sorrend természetesen egyénenként változik.

3.1 A nem ionizáló sugárzás biológiai hatásai

A rádiófrekvenciás sugárzás élettani hatásait több, mint 50 éve vizsgálják. Állatkísérletekből ismert, hogy a kis energiájú RF sugárzás direkt hatásaként DNS mutáció nem alakul ki. Energiája igen alacsony, ezért nem roncsolja a vele kölcsönhatásba kerülő anyagokat: áthatol rajtuk vagy valamilyen mértékben abszorbeálódik. Jelenleg nem áll rendelkezésünkre olyan kutatási eredmény, amely egyértelműen és meggyőzően párhuzamot vonna a rádiófrekvenciás expozíció és a hőre érzékeny szövetek károsodása (leukémia, szemlencse-károsodás, hererák, stb.) között. Azonban a mikrohullámú sugárzásnak különösen kitett személyek (pl. radarkezelők) esetében az összefüggés nem zárható ki. [26]

3.2. Vallási, meggyőződésbeli, neveltetésből adódó aggályok

Sokan nehezményezik, hogy egy számukra idegen ember látja testük körvonalát, vagyis ami a ruha alatt rejtőzik. Van, aki szégyenlősségből idegenkedik vagy megalázónak tartja az eljárást. Ez természetes és tiszteletben tartandó, hiszen eltérő kultúrák, különböző szokások, valamint egyéb behatások is változtatják hozzáállásunkat. XVI. Benedek pápa véleménye szerint az emberi méltóság és integritás tisztelete olyan alapvető érték, melyet még a biztonság fokozásának érdekében sem szabad csorbítani [27]. Egy amerikai muszlim csoport vallásjogi határozatban tiltja meg a vallás követőinek a testszkennerek használatát, érvelésük szerint azért, mert a Korán azt parancsolja a hívőknek, hogy takarják el nemi szervüket. Javasolják, hogy a repülőtéri biztonsági ellenőrzés során válasszák a régi fémdetektoros és felsőruházat-átvizsgálós módszert [28]. A fentieken túl számos szervezet kifogásolta, kifogásolja a testszkennerek bevezetését.

3.3. Funkcionális előnyök és hátrányok

Előnyök

- kényelmes, hiszen nem kell levenni az órát, kabátot, övet, cipőt
- gyorsabb utasbiztonsági átvizsgálás
- egyszerűbb utazás fém alapú orvosi implantátummal
- alaposabb vizsgálat: műanyag, kerámia, stb. anyagok felderítése
- várhatóan magasabb biztonsági szint, javuló közbiztonság

Hátrányok

- az utasbiztonsági ellenőrzést végző személy látja a test anatómiai részleteit -> nőt csak nő, férfit csak férfi ellenőrizhet, további kérdések merülnek fel
- a testüregbe rejtett eszköz vagy anyag nem észlelhető vele
- visszaélési lehetőség a test körvonalait mutató képpel

3.4. Egyéb kérdések

Egyértelműnek látszik, hogy aktív eszköz alkalmazása esetén az ellenőrzést végző személy azonos nemű kell, hogy legyen a vizsgált személlyel. Kérdéses azonban, hogy fiatalkorúak vagy transzszexuálisok esetén ki vizsgáljon. Lehet-e választani, hogy milyen nemű ellenőrizzen? Passzív eszköz alkalmazásakor – valószínűleg – nem merülnek fel ilyen jellegű kérdések, mivel csupán egy körvonalazott képet kapunk.
További kérdéseket vet fel az a hír, miszerint egy ismert színész az Egyesült Királyságbeli Heathrow repülőtéren „kiszivárgott" – az utasbiztonsági ellenőrzése során készült – kompromitáló kép [29]. A repülőtér biztonsági igazgatója cáfolta az eseményt.
Fontos megjegyeznünk, hogy Magyarország – a közeljövőben – nem tervezi ilyen eszközök tesztelését, beszerzését. A Budapest Airport jelenleg vizsgálja a testszkennerek bevezetésének lehetőségét. A repülőterek utasbiztonsági ellenőrzése továbbra is a fémdetektor kapun való áthaladásból és a csomagvizsgálatból áll [30]. Így az erre vonatkozó hazai jogszabály sem tesz említést a TeraHertz-es technológiáról, jelenleg csak a külföldön üzemelő eszközökkel kapcsolatosan merülhetnek fel kérdéseink. Amennyiben a Rendőrség indokoltnak tartaná ilyen eszköz bevezetését (pl. ha nagy mértékben megnőne az ország terrorfenyegetettsége vagy a közbiztonságra különösen veszélyes eszközökkel való visszaélések száma), a Szolgálati szabályzatban leírtak figyelembevételével alkalmazhatná [33].

ÖSSZEFOGLALÁS

A kutatási eredmények összefoglalásaként elmondható, hogy a TeraHertz-es technológia előtérbe kerülése új távlatokat nyitott a biztonságtechnikában. Ezt a célzott kutatások, a technika fejlődése és a magasabb biztonsági szintet garantáló személyvizsgáló-módszer iránti igény tette lehetővé. Megmutatta, hogy az embereknek mennyire fontos a biztonságérzet, amiért akár kellemetlenségeket is hajlandóak elviselni. A biztonságtechnikával foglalkozóknak olyan szabályok, berendezések bevezetésére és használatára kell törekedniük, amely nem káros az egészségre, gyors, megbízható valamint szem előtt tartja a vizsgált személy emberi mivoltát.

A tanulmányban bemutatott eszközök műszaki és egészségügyi szempontból megfelelőnek, biztonságtechnikai szempontból hasznosnak és előremutatónak bizonyultak. A rendelkezésre álló tapasztalatok alapján – a személyiségi jogi szervezetek támadása ellenére – megfelelnek azoknak a normáknak, amiket az emberek nagy többsége el tud fogadni a saját biztonsága érdekében.

Felhasznált irodalom

1. Wikipédia, a szabad enciklopédia *2010.02.28.*
   TeraHertz sugárzás

   http://en.wikipedia.org/wiki/Terahertz_radiation

   Ionizáló sugárzás

   http://hu.wikipedia.org/wiki/Ionizáló_sugárzás

   Gunn dióda

   http://en.wikipedia.org/wiki/Gunn_diode

   Gallium-nitrid

http://en.wikipedia.org/wiki/Gallium_nitride

2. Hebling János – Almási Gábor: Képalkotás és spektroszkópia THz-es sugárzással: a csillagászattól az orvosi alkalmazásokig, Magyar Tudomány: Szemtől szemben a lézerekkel, 2005/12, 1483. oldal

3. Budó Ágoston – Mátrai Tibor: Kísérleti fizika III. kötet (Optika és atomfizika), Tankönyvkiadó, Budapest, 1980. 267. oldal

4. Bánhegyi György: Érintésmentes elektromágneses mérési technológiák, Műanyagipari szemle 2008/06. *2010.03.05.*

   http://www.muanyagipariszemle.hu/2008/06/erintesmentes-elektromagneses-meresi-technologiak-05.pdf

5. Berkes József – Buzády Andrea – Pálfalvi László: Bemutatkozik a Pécsi Tudományegyetem Kísérleti Fizika Tanszéke, Fizika Szemle 2004/8. 264. oldal

6. Völgyi Ferenc – Nyúl László: Mérési segédlet a Gunn-oszcillátor vizsgálata, szinkronizálása című méréshez, Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar Mikrohullámú Híradástechnikai Tanszék, 1998. *2010.03.09.*
   http://www.mht.bme.hu/~lenart/Vill_4042/Gunn.pdf

7. Christian Wolff: Radar basics, 2005. *2010.03.05.*
   http://www.radartutorial.eu/21.semiconductors/hl15.en.html
   http://www.radartutorial.eu/17.bauteile/bt13.en.html

8. Taszner István: Telekommunikációs rendszerek Elméleti összefoglaló, Miskolci Egyetem Villamosmérnöki Intézet Automatizálási Tanszék, 2000.

9. Mohamed Missous – Faisal Amir – Colin Mitchell: Advenced step-graded Gunn diode for millimeter-wave imaging applications, SPIE Newsroom, 2009. *2010.03.05.*
   http://spie.org/x36521.xml?ArticleID=x36521

10. Hebling János – Almási Gábor – Kozma Ida Zsuzsanna – Pálfalvi László: Ultrarövid infravörös és távoli infravörös (THz-es) fényimpulzusok előállítása és alkalmazása, REAL – az MTA Könyvtárának Repozitóriuma, 2008. *2010.03.04.*
    http://real.mtak.hu/570/

11. Ludmány András: Asztrofizika űreszközökkel, 6. Infravörös csillagászat, Debreceni Egyetem, 2009. *2010.03.05.*
    http://fenyi.sci.klte.hu/oktatas/F2705jegyzet/ur-asztrofizika_6-10.pdf

12. Csibi Ádám: Fourier-transzformációs infravörös spektroszkópia, ELTE-TTK, 2006. *2010.03.05.*
    http://www.math.bme.hu/~jtoth/ELTE/CsibiA.pdf

13. TeraView, 2010.03.02.
    http://www.teraview.com/files/uploaded/File/TeraViewexplosivesdetectiontechnology.pdf

14. Pozsgai Imre: Mikroszkópia és lokális kémiai analízis, Magyar Mikroszkópos Konferencia, 2005.

15. Rapiscan Systems, *2010.03.02.*
http://www.rapiscansystems.com/

16. Transportation Security Administration: Imaging Technology, 2010. *2010.03.06.*
http://www.tsa.gov/approach/tech/imaging_technology.shtm

17. ThruVision Systems, *2010.03.05.*
http://www.thruvision.com/Our_Products/T8000_Sub_Pages/T8000_Specsheet_v5_%28lower_res%29.pdf

18. Camera 'looks' through clothing, BBC News, *2008.03.10.*
http://news.bbc.co.uk/2/hi/technology/7287135.stm

19. Transportation Security Administration: Response to: „Oops: Bascatter X-ray machines tear apart DNA", 2009. *2010.03.04.*
http://www.tsa.gov/blog/labels/Safety.html

20. U.S. Department of Homeland Security: Privacy Impact Assessment Update for TSA Whole Body Imaging, 2009. *2010.03.02.*

21. L3 communications Security&Detection Systems, *2010.03.05.*
http://www.dsxray.com

22. L3 communications Security&Detection Systems: How Millimeter Imaging Works, *2010.03.02.*
http://www.tsa.gov/assets/wmv/l3_mwave1.wmv

23. James Lin: New EMF Technologies – A Challenge for Radiation Protection?, International Commission on Non-Ionizing Radiation Protection (ICNIRP), 2008.

24. 63/2004. (VII. 26.) EszCsM rendelet a 0 Hz – 300 GHz közötti frekvenciatartományú elektromos, mágneses és elektormágneses terek lakosságra vonatkozó egészségügyi határértékeiről

25. Chung-Kwang Chou: New IEEE C95.1-2005 RF Safety Standard, IEEE International Committee on Electromagnetic Safety, Technical Committee 95, Subcommittee 4, Peru, 2006.

26. Fülöp Sándor: Tanulmány a nem ionizáló sugárzásról, Jövő Nemzedékek Országgyűlési Biztosa, 2009. *2010.03.06.*
http://jno.hu/hu/?&doc=tubes_b2

27. A pápa a testszkenner ellen megy, *2010.02.24.*
http://www.fn.hu/kulfold/20100224/papa_testszkenner_ellen/

28. Muszlim tiltakozás a testszkennerek ellen, *2010.02.13.*
http://www.honvedelem.hu/cikk/4/18376/fatva_testszkenner.html

29. Shah Rukh Khan sign off sexy body-scan printouts at Heathrow, *2010.02.05.* http://www.realbollywood.com/news/2010/02/shah-rukh-signs-sexy-bodyscan-printouts-heathrow.html

30. Budapest Airport Zrt. utasbiztonsági ellenőrzéssel kapcsolatos tudnivalók, *2010.03.06.* http://www.bud.hu/utasok/biztonsag

31. Testszkennert vezet be a Budapest Airport? *2010.01.11.* http://www.metropol.hu/cikk/510194

32. 1/2005. BM rendelet az utasbiztonsági ellenőrzést végző személyek e feladatra történő felkészítésének és vizsgáztatásának rendjéről

33. 62/2007. IRM rendelet a Rendőrség Szolgálati Szabályzatáról

Képek jegyzéke

1. ábra: http://www.sura.org/commercialization/terahertz.html *2010.02.23.*

2. ábra: felhasznált irodalom [13] *2010.03.02.*

3. ábra: felhasznált irodalom [17] *2010.03.05.*

4. ábra: http://www.dsxray.com/advancedimaging/PROV_PS_26.FEB.10_72dpi.jpg *2010.03.02.*

5. ábra: http://www.tsa.gov/graphics/images/approach/tech_mwave3.jpg *2010.03.02.*

6. ábra: http://www.dsxray.com/advancedimaging/L-3%20composite%20300dpi.jpg *2010.03.02.*

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Fialka György
gyorgy.fialka@ge.com

A PÉNZINTÉZETEK TECHNIKAI BIZTONSÁGÁNAK TÖRTÉNETI FEJLŐDÉSE ÉS JÖVŐJE

Absztrakt

A pénzintézetek biztonságának megteremtése, védelmük lehetőségei, a nagy mennyiségű pénz közelsége okán kiemelt feladatként jelentkezik a megalakulásuk kezdete óta. A cikk végig kíséri a kezdetektől napjainkig az alkalmazott mechanikai és elektronikai biztonságtechnikai eszközöket, alkalmazási korlátaikat és működésük lehetőségeit. A támadás-védekezés egyensúlyának állomásait és a jövő jelenleg látható új útjait.

The high amount of valuables which can be found in every bank, require special arrangements to provide adequate security, since the beginning of their existence. This article is telling the history of the mechanical and electronic security systems, from the beginning till the present day, showing the operational conditions and the limits of their use. It is presenting the balance between the threats and protection, and future possibilities.

Kulcsszavak: *érzékelés, beavatkozás, mechanikus, elektronikus, paradigmaváltás ~ detection, intervention, mechanical, electronic, paradigm shift*

Bevezető

Magyarországon 1841 októberében nyílt meg az első kereskedelmi bank. Így országunkban a pénzintézeti biztonság fogalma ez időtől számítható.

Kezdetekben a biztonság a fizikai értelmében, a szilárdság és az áthatolhatatlanság fogalmával volt egyenértékű, a bankfiókok tekintetében. A pénz szállítása tekintetében pedig, a megvasalt járművek és a nagyszámú fegyveres kíséret volt az elfogadott védekezési forma.

Ez időben az úgynevezett kasszafúrás volt a jellemző bűnelkövetési forma, amely az intelligens bűncselekmények csúcskategóriájába tartozott. Ezeket a bűncselekményeket jellemzően zárás után, minél csendesebben fondorlatosan kitervelt módon bejutva a bankfiók belsejébe kényelmesen, kihasználva a jelzőrendszerek hiányát, hajtottak végre. A méregdrága

speciális páncélszekrények megfúrása jelentős műszaki ismereteket követelt meg elkövetőjétől. Volt idő mikor a nyomozók, az elkövetés módszeréből nagy magabiztossággal, a végrehajtó személyét is meg tudták állapítani, az egyedi páncélszekrény nyitási módszerek ismeretében.

A másik jellemző pénzintézet elleni elkövetési forma a primitívebb, erőszakosabb változat, a bankrablás fegyveres „hagyományos" végrehajtási kategóriája. Ekkor a nyitvatartási időben rontottak a rablók a bankfiókra és erőszakkal jutottak a bankban található pénzhez. Ezen módszerek megakadályozására legfeljebb az élőerős őrzési formát alkalmazhatták a bankárok melynek eredményessége nagy reménnyel nem kecsegtetett, hiszen a támadás bekövetkezéséről, értesíteni, vagy segítséget kérni valakitől informatikai rendszerek nélkül szó sem lehetett.

A technikai eszközök és módszerek fejlődése a pénzintézeti védekezésben is változásokat hozott. Különféle jelzőrendszerek kialakításával próbálták a banki biztonság fokozását elérni. Itt a jelző csengők mechanikus táv- „drótok" kötelek, csőtelefon, leeső jelzők mechanikus, később elektromos változatain keresztül alakultak ki napjaink behatolás jelző berendezései.

Ez az eszközcsalád minden lehetséges behatolási módszer ismeretében tagozódott a behatolási mód érzékelésére kifejlesztett eszközökre (nyitás, mozgás, rezgés, törés). Az érzékelést kezelő intelligens központi egységek pedig felkészítve az elkövetési cselekmény lehetséges módozataira, ezekre kifejlesztett intézkedési, védelmi programcsomagokat tartalmaznak. Ezek a berendezések az idők során egyre magasabb technikai, technológiai, és programozási szinten valósulnak meg.

A behatolás jelző eszközök kialakulása után felmerült a kültéri vész jelzés igénye, a külvilág figyelmének felhívása a támadás eseményére. Kialakultak a külső hang és fényjelző eszközcsoportok. Ezek elsődleges feladata megbízható módon a környezet figyelmének ráirányítása a bekövetkezett támadásra valós időben, a segítségkérés e módon történő realizálása, valamint a támadók elriasztása. A jól működő berendezés csoportok kialakítása megszülte a következő problémakört, a szabotázs védelem létrehozásának feladatát. A bűnözők a védelmi eszközök szabotálásával próbálták helyreállítani a kommunikációs rendszerek hiányából fakadó előnyöket. Elvágták az elektromos kábeleket (villany, távközlés), megrongálták, működésképtelenné tették a hang és fényjelző berendezéseket. Ezért kialakultak a második védelmi kört képviselő szabotázsvédelmi rendszerek, melyek feladata a behatolás jelző eszközök hiteles működésének védelme, támadásuk esetén riasztás jelzés kezdeményezése. A riasztó rendszerek eredményességük révén olyan sikeressé váltak, hogy nagy számban elszaporodtak egyéb felhasználási területeken is (lakások, gépjárművek, boltok). Ennek eredményeképpen a sok jól és kevésbé jól kivitelezett és felszerelt eszközöktől zengett nap mint nap környezetünk, a 120 dB-s hangerővel. Gyakorlatilag, ennek hatására elvesztette a külső riasztás módszere hitelességét. De más veszélyhelyzet is kialakult a hangos riasztás miatt. Az agresszív hangjelzés, a rablás során elindulva a támadót is stresszelte, és ez több esetben értelmetlen erőszakos bűncselekmények bekövetkezéséhez vezetett.

Felvetődött ezért a támadáskori hiteles átjelzés igénye, amikor is a behatolás, vagy támadásjelző rendszer közvetlenül az intézkedésre alkalmas, és jogosult helyre küldi el valós időben a támadás tényét, helyét, és módját leíró jelcsomagot, úgy hogy a támadó ezt nem érzékeli. Az átjelzések intelligenciája a leeső jelzőtől napjaink szabotázs védett, több utas, IP alapú valós idejű kép, hang tartalommal bíró csomagjáig jutott el. Az átjelző rendszerekkel szemben támasztott igények napról napra formálódnak, szabványosodtak. A támadási cselekmények változatai, valamint a technika fejlődéséből adódó lehetőségeink, még koránt sem kimerítettek.

A felügyeleti és együttműködő hatóságok részéről felvetődött igényként a napi és a rendkívüli események dokumentálási igénye, mely megoldására a pénzintézetekben megjelentek a különféle képrögzítő eszközök. A kezdeti robot fényképező gépektől napjaink digitális technikájáig

elérkezve gyorsan elszaladt az idő. Az események meghatározott időtartamonként történő hiteles rögzítésére, tárolására, visszajátszására vagy, támadás esetén megfelelő végpontra történő továbbítására alkalmasak ezek az eszközök. A technika és az informatika szolgáltatásainak hihetetlen fejlődési sebessége határtalan lehetőséget szab még e téren részünkre.

A pénzintézetek területén zajló belső mozgások szabályozására, ellenőrzésére a beléptető rendszerek korlátlan választéka ad lehetőséget. Ezek az eszközök alkalmasak a belépő személy azonosítására, jogosultsági szintjének megállapítására, és az belépési, benntartózkodási idő megmásíthatatlan tárolására.

Még szintén a biztonsági eszközök csoportjába tartoznak a tűzjelző eszközök is, melyek e rendkívül veszélyes elemi kár bekövetkeztének megbízható jelzését, elterjedésének gátlását hivatottak végezni. Integrált biztonsági rendszerekben a védelem és a menekülési útvonalak biztosítása, a tűzút zárása, a menekülési útvonal megnyitása, valamint speciális kármegelőző oltórendszerek üzemeltetése is e tárgykörbe tartozhat.

Egyéb, az elemi károk bekövetkeztét gátló érzékelő eszközöket is alkalmazhatunk még biztonsági rendszereinkben. Pl. CO, víz-, gáz-érzékelőket, valamint szeizmikus rezgésérzékelőket, melyek növelik a működésbiztonságot.

Megemlíthetjük még a terror elhárítási feladatok végrehajtásakor alkalmazható érzékelő eszközpark néhány elemét is:

- speciális gázok, méreganyagok, kábítószerek, vegyi és biológiai, valamint robbanó anyagok érzékelő eszközeit
- fémérzékelő és csomagvizsgáló eszközöket

1. Biztonságtechnikai, műszaki védelem alapvető szabályai

A biztonságtechnikai, műszaki védelem magába foglalja az épületek és egyéb építmények mechanikai, valamint elektronikai eszközökkel való védelmét, továbbá az ezek alkalmazásához meghatározott módszereket és eljárásokat. A biztonságtechnikai, műszaki követelmények meghatározása és egyes ehhez kapcsolódó feltételek biztosítása kizárólagosan a Bankbiztonsági Szolgálat feladatköréhez tartozik. A Bankbiztonsági szakértők előzetes véleményét kell kérni a bankcsoport céljára szánt ingatlanok vételét, az új iroda - és fiókberuházások, illetve bővítések építészeti tervpályázatának kiírását, vagy építészeti tervezését megelőzően. A tervek építésügyi hatósági engedélyezésre való benyújtása, a kivitelezési tervek elfogadása csak a Bankbiztonsági Szolgálat előzetes egyetértésével történhet, amit a terveken minden esetben rögzíteni kell

Az elektronikai védelem megtervezéséről, kivitelezéséről, műszaki átvételéről és rendszeres karbantartásáról, valamint a tárgyi tevékenységhez tartozó kötelezettségvállalási jog gyakorlásáról - a jóváhagyott beruházási terv szerint - a Bankbiztonsági Szolgálat gondoskodik. A biztonságtechnikai védelmi rendszer jóváhagyott tervétől eltérni csak a Bankbiztonsági vezető hozzájárulásával lehet.

Ezek azok az általános szabályok, amelyek mentén a biztonságtechnikai védelem fogalomrendszerét feldolgozhatjuk.

2. A pénzintézetek mechanikai védelmének eszközei

A mechanikai védelemi tevékenység az építményi héjszerkezet határvonalán kezdődik. (Ebbe természetesen beleértendő a födém és a padozat is!) Tudvalevő, hogy egy létesítmény biztonsági egyenszilárdsági mutatója a szerkezet leggyengébb pontjának szilárdsági mutatójával egyenértékű, ezért a tervezésnél a szilárdsági elvárásokat e szerint kell meghatározni. Tehát az

épített szerkezetek, és a nyílászárók megválasztásánál a MABISZ szabályzat mellékletében meghatározott, értékhatárhoz kötött minőségű elemek alkalmazását, beépítését szükséges előírni és alkalmazni. (Persze a biztonsági minősítési rendszerben egyenértékű eszközök is alkalmazhatóak.) Az áthatolás gátlásának egyszerűbb elemei a vastagítás és a nagyobb szilárdságú eszközök alkalmazásával növelik az áttörés, áthatolás elleni védelmet. A koronafúrás ellen már speciális alakú és változó keménységű fémelemek beépítésével, az oxigénlándzsás támadások ellen pedig áramkorlátozással, valamint erős, szerves füstöt termelő úgynevezett „kompozit" anyagok alkalmazásával növelik a védekezés szintjét.

Az épület héjszerkezetén belüli további mechanikai biztonságnövelő eszközök a következők:

- a belső pénzforgalmi terek markáns elválasztására szolgáló épített megerősítések, biztonsági ajtók
- a pénz átadás- átvételt biztonságossá tevő átadó zsilip, a kiépített szeparált pénzszállítási útvonallal
- a megbízható pénztároló eszközök trezor, páncélszekrény, nyitási idő programozható többrekeszes multisafe és az időzárak

Ezen eszközök persze csak akkor teljesítik a tervezett elvárásokat, ha az előírt, üzemeltetési szabályokat leíró biztonsági utasításokat maradéktalanul betartják az alkalmazottak.

De ne feledjük! A mechanikai biztonsági eszközök önmagukban nem alkalmasak a támadás megakadályozására. Feladatuk az elrettentés és az áthatolás időtartamának megfelelő, előírt időtartamú késleltetése. A védelem fokozását a biztonságtechnikai rendszerek integrációjával érjük el.

3. Elektronikai biztonságtechnikai jelzőeszközök

Az elektronikai biztonságtechnikai jelzőeszközök telepítése előtt a MABISZ szabályzat vagy a már elfogadott szabványok idevonatkozó előírásainak figyelembevételével kell elkészítenünk a **biztonságtechnikai tervet**. Elkészítéséhez a mechanikai biztonság meglétének ellenőrzésén kívül, a létesítményben folyó funkcionális tevékenységek teljes körét is meg kell ismernünk, csak ennek ismeretében tervezhetünk megfelelően.

A biztonságtechnikai terv teljes részletességgel foglalkozik funkciónként és helység fajtánként az előírások szerinti a részleges és teljes elektronikai biztonsági rendszerek típusainak meghatározásával.

Meghatározó e csoportban a **behatolás jelző** eszközök családja.

E rendszerek három fő részre tagozódnak:

Az **érzékelő eszközök** a behatolással járó változásokat jellemző fizikai paraméterek detektálásán alapuló jelérzékelő berendezések. Képesek a rezgés, a mozgás, a hőmérséklet változás, sugárzás, különféle gázjelenlét érzékelésére és megbízható, valós idejű kijelzésére. A megbízható változás érzékelés érdekében többféle jelformáló fizikai módszer közös alkalmazását kombinálják egy érzékelő fejben, amely így a téves riasztás lehetőségét kizárja félrevezethetetlen módon.

Az érzékelők által kibocsátott jeleket a **jelzővonalak** feladata a központi egységbe vezetni. Velük szemben, az érzékelők által kibocsátott jel keletkezés pontos helyének, típusának megbízható, szabotázsvédett átvitele az elvárás.

A **központi egység** a beérkezett jelek kezelésére, értékelésére szolgáló vezérlő software programja szerinti előírások végrehajtását, a teljes rendszer felügyeletét, tápellátását, és

szabotázsvédelmét végzi. Vezérli a hang és fényjelző berendezéseket, valamint indítja a távátjelző egységet riasztási esemény kialakulásakor.

E rendszer szerves részeként, de önálló funkcióval működik a **támadásjelző hálózat**. Feladata, hogy rablótámadás esetén azonnal csendes riasztást kezdeményezzen. A támadásjelző rendszer jeladóit rejtett módon kell elhelyezni, hogy működtetésük észrevehetetlen legyen a támadó számára, mivel csak így várható el azok működtetése az alkalmazottaktól. A támadásjelző jeladó létezik mobil változatban is.

Következő nagy eszközcsoport a beléptető rendszerek csoportja.

Az érzékelés módja szerint megkülönböztetünk kódvezérléses, mágneskártyás (kártyaolvasós) közelítéses, proximity, valamint biometrikus típusú rendszereket. A proximity rendszerek intelligensebb több feladatra alkalmassá tehető, de természetesen jóval költségesebb berendezés-családok. A rendszercsalád csúcsán áll a biometrikus érzékelésen alapuló beléptető rendszer, bár funkcionalitását tekintve működése hasonló az előzőekhez. Eltérés az azonosítás kizárólagosságában rejlik, mivel ujjlenyomat, hang, írisz, arckép, a személyazonosítás alapja. A rendszerek a biztonság fokozása érdekében egymással kombinálhatóak.

Feladatuk a beléptetés és az épületen belüli mozgások automatikus, programozás szerinti vezérlése, belépési jogosultság-csoportok kezelése, a cselekmények folyamatos dokumentálása, a rendkívüli események azonnali jelzése. Összehangoltan működik, és ha kell, együttműködik az épület egyéb biztonsági berendezéseivel (pl. tűzjelző rendszer). Kellő intelligencia szint esetén alkalmassá tehető tartózkodási hely megállapításra, telefonvonal automatikus tovább-irányítására, munkaidő nyilvántartás adatainak gyűjtésére, rendszer hozzáférési adatok tárolására, helyi egyéb jogosultságok tárolására pl. kávéautomata használat.

A következő csoport a **képrögzítő, esemény dokumentáló** rendszerek csoportja. Csak a történeti hűség kedvéért még megemlítem az álló képeket, képsorozatokat rögzítő robotfényképező gépeket, bár feltételezésem szerint már nem használják Magyarországon sehol sem. Gyakorlatilag az analóg videó képrögzítő berendezések is a végüket járják. A jelenlegi technikai színvonal már a digitális képalkotás, rögzítés, és továbbítás szintjén tart. E rendszerekkel szembeni főbb követelmények és előírások a következők:

- Szélsőséges fény és hőmérsékleti viszonyok közötti minőségi képalkotás
- Megváltoztathatatlan idő és esemény dokumentálás
- Megfelelő időtartamú tárolás
- A hozzáférést csak a regisztrált személyek részére esemény- dokumentáltan engedélyezzen
- A távátviteli igényeket kielégítse megfelelő engedélyezett irányokba
- Folyamatos 24 órás üzembiztonság.

A kamerák tekintetében jelentős készletválaszték áll rendelkezésünkre, a normáltól az infra sugaras képfeldolgozásig, a közepes és nagyfelbontású érzékeléstől, a vezérelhető optikai zoom-ig, a csőházban futó kameráktól a mennyezeti 360 fokosig sorolhatnám a lehetőségeket, amelyek kiválasztását döntően a feladatokból fakadó igények határozzák meg.

A rögzítés, tárolás és a továbbítás feladataihoz is, az igények mentén léteznek szintén megfelelő eszközcsaládok nagy választékban.

Felhívom a figyelmet arra a rendkívül lényeges tényre, hogy a képrögzítési tevékenység, a személyes adatok kezelése kategóriába tartozik, ezért kezelésére a személyes adatok kezelésére vonatkozó tőrvények és rendeletek **minden tekintetben vonatkoznak**.

Az **átjelző rendszerek**-kel kapcsolatos elvárások:

Elsődlegesen a behatolás és a tűzjelző rendszeren keletkezett jelzésekből, az előzetesen meghatározott rendezési és sorrendi elvek alapján kiválasztottakat megfelelő biztonsággal, és tartalmi sorrendben, azonnal továbbítsa a diszpécser központba. Itt az intézkedési jogosultsággal rendelkező személyek az utasítások értelmében eljárnak.

Ez a gondolatsor négy fontos logikai tevékenységet takar:

- Először az átjelző központ és a helyi rendszerek összeillesztését, megfelelő programozását és 24 órás folyamatos üzemképességét.
- Másodszor az átviteli csatornák szabotázsvédett működőképességét (lehetőleg legalább kétirányú).
- Harmadszor a fogadóközpont értelmezési szoftverének megfelelő programozását, ügyeletesének gyors reagálását, kontroll és értesítési rendszerének helyes működését, a reagáló egységek megfelelő valós idejű informálását a folyó cselekményekről.
- Negyedszer egy szakszerű beavatkozó tevékenységet, amely a cselekmény megakadályozását, felszámolását jelenti.

Egy bankrablási szituáció helytelen kezelésének következményei beláthatatlanok. Bár jelzem e téren jelentős fejlődés várható. A Magyar Rendőrség a nappali támadásjelzések fogadására IP felületű felügyeleti rendszert fejlesztett, mely alkalmas a valós idejű jelfogadásra, felügyelt intézkedésre, folyamatos képfogadásra és kommunikációra. Ez a rendszer lehetővé teszi a bankrablási helyzetek megoldásának újraértékelését.

A **tűzjelző rendszerek** a biztonság katasztrófavédelmi ágát képviselik.

Feladatuk a létesítményben keletkezett tűzesemények azonnali jelzése, speciális esetben, intelligens rendszer telepítése esetén, oltásának megkezdése (spinklerek, speciális oltógázok) valamint a tűzterületek menekülési útvonalainak megnyitása, és egyéb épület felügyelettel kapcsolatos programozott intézkedések megtétele.

A tűzjelző rendszer központja a tűzjelzést a területileg illetékes Tűzhatóságnak közvetlenül is jelzi az érvényes utasítás alapján, párhuzamosan az átjelző rendszer központjával. E rendszerek nagy intelligenciával rendelkező érzékelőkkel és szoftverrel készülnek, működésük megfelelőségét rendszeres ellenőrzéssel szükséges kontrollálni.

A rabláselhárítás egyik újabb elemeként megemlíteném még az **elektronikus időzárakat**, melyek megakadályozzák:

- az üzemidőn kívüli páncélszekrény vagy páncélajtó nyitást
- üzemidőn belül nagyobb összegek azonnali felvételét
- riasztás bekövetkezése után bármilyen értéktároló kinyitását,
- és egyéb programozási trükkök alkalmazását helyi igény szerint

Új eszköze a bankrablások elleni küzdelemnek az un. **robbanó pénz** vagy eredeti nevén a „dye-pack”. Az eszköz aktív részét a pénztári pénzjegykötegek közé telepítik. Rablás esetén ez az eszköz az elrabolt pénz közé kerül. Mikor a rabló elhagyja a bankfiókot, akkor az eszköz működésbe lép. A teljes bankjegy készletet, valamint a rablót is erős sárga festékfüsttel beszínezi eltávolíthatatlanul. A pénz értéktelenné válik és a menekülő elkövető elfogási esélye jelentősen megnő.

A fentiekben felsorolt rendszerek, eszközök, és módszerek valamint a mechanikai védelem eszközei és módszerei alkotják közösen a pénzintézeti védelem tárgyi eszközcsoportját. A fizikai védelem további feladatait a **biztonsági élőerős őrzés** tevékenysége foglalja magába. A technika és az élőerő együttes alkalmazása, tevékenységük egymáshoz illesztése, fokozza a biztonsági, védelmi tevékenység hatékonyságát.

A múlt és a jelen pénzintézeti biztonságának fejlődési sebességét döntően az elkövetésekből levont konzekvenciák és azok gyakorisága vezérelte. Érzékelhető, hogy az alkalmazott eszközpark technikailag még fejleszthető, finomítható, de igazi áttörést csak valami paradigma váltás okozhat a védelemben. A kérdést érdemes egy kicsit tudományosan elemeznünk, ahhoz hogy a lehetséges irányokat megfogalmazzuk.

4. A probléma tudományos megfogalmazása

A pénzintézetek biztonsága több, egymásba épülő és egymást kölcsönösen feltételező tényező hatása mentén, éppen ezért állandóan változó képet mutatva formálódik. A technikai fejlődés mechanikai, elektronikai és vegyi eredményei és a humán kutatások idevonatkozó következtetései egyaránt megjelennek e folyamat fejlődési ágában. A fejlődés hajtómotorja persze, a bekövetkezett támadásokból leszűrt konzekvenciák alapján megfogalmazódott prevenciós igény, amely a védelem különféle szükségleteit formázza meg a pénzintézetek részére.

Ezek, függően a támadás irányától, az intelligens csalási folyamatoktól a legdurvább erőszakos rablási cselekményekig terjedő spektrumban mozognak. Talán az erőszak természete és eredménye miatt, nagyobb hangsúlyt kap az ezek elhárítására fordított energia. A bankrablások, mint e csoport kiemelkedő cselekményei, külön fejtörést okoznak a szakembereknek, hiszen e cselekmény ellen technikai, a szabályzási és a pszichikai eszközök kölcsönös alkalmazása mentén érhetünk el csak jobb eredményeket.

A végrehajtott bankrablások folyamatát, bekövetkezésük okait, valamint a védekezésben alkalmazható lehetséges prevenciós folyamatokat tudományos alapossággal elemezték, értékelték nagy tudású rendőrségi és civil biztonsági szakértő csoportok. A feldolgozott eseményekből több, jellemzőnek tekinthető tevékenységcsoportot állapíthattak meg.

1. Az ismertté vált, letartóztatott elkövetők meghallgatásakor végrehajtott vizsgálatok bizonyították, hogy a támadók szinte minden esetben felderítették a pénzintézetet, valamint környezetét és ez alapján megtervezték az elkövetést. Ezeket a felderítéseket a biztonsági szolgálat nem mindig észlelte, így megelőző intézkedéseket sem tudtak tenni. A támadás megkezdésekor is a személyzet csak vizuálisan tudta érzékelni a vészhelyzetet, különféle biztonságtechnikai szenzorok nem jelezték előre a támadást, így a végrehajtott intézkedések is csak követő jellegűek, ezért zömükben korlátok között végrehajthatóak voltak.

2. A kiválasztáskor a magas technikai színvonalú integrált biztonságú fiókokat a rablók elkerülték, az alacsony nyereség, és a nagy lebukási veszély okán.

3. A megtámadott bankfiókok alkalmazottai körében kialakult egy új jelenség, amelyet „**Móri szindróma**” néven említünk, amikor a dolgozók a lemészárolástól félnek a rablást követően. A banki dolgozók biztonságérzete ezért a fiókokban jelentősen csökkent, ami kihatással van az ügyfelek kiszolgálására, valamint a rabláskor végzendő prevenciós feladatokra is.

A tudományos elemzéseket követő feltételezések egyik lehetséges iránya az **érzékelés, előjelzés** fejlesztésében látja a megoldás útját.

A kialakult biztonságtechnikai termékcsaládok fejlesztése termékei, melyeket a pénzintézetek is teljességükben alkalmaznak, jelenlegi fejlettségük csúcsát elérték. A további fejlesztések zöme ezen eszközök gyártásának automatizálásával, paramétereik javításával, megbízhatóságuk fokozásával, valamint méreteik csökkentésének témájával foglalkoznak. Paradigmaváltás szükséges e tekintetben. Új, pszichés humán jellegű érzékelők bevezetése tudja csak ezt a cserét elősegíteni.

A bankrablás megelőzési szakaszában, valamint közvetlenül a bűncselekmény kísérleti szakaszában olyan komplex logikai, fizikai és humán biztonsági funkciókat ellátó intelligens rendszer kifejlesztése a cél, amely biztonsági riasztások fokozatait indítja be. A biztonsági riasztások hatására az intelligens rendszer döntéseket hoz, amely a bankrablás megelőzését, megakadályozását is eredményezhetik.

A bank biztonság területén már alkalmaznak logikai és fizikai biztonsági rendszereket, de kevésbé élünk azonban a humán biztonsági lehetőségekkel.

A humán biztonság tudományos területein már vannak működő nemzetközi kezdeményezések az elkövetői magatartások elemzésére. Más területek kutatási eredményei azt bizonyították, hogy az elkövetői magatartások technikai eszközök felhasználásával szoftveres úton is nyomon követhetők és a megelőzés szolgálatába állíthatók.

Elméletileg megalapozott az a cél, hogy létrehozhatóak olyan intelligens szenzorok, amelyek a fenyegetést előjelző humán paramétereket értékelik-elemzik és a keletkezett információkat továbbítják egy döntés végrehajtó központba.

A pszichológusok feltételezik, hogy minden elkövetőre érvényes az a szabály miszerint: A bankrablás tervezésekor és az elkövetést közvetlenül megelőző szakaszban az elkövető egy jól felismerhető magatartási mintázatot hordoz, idegrendszeri és pszichés ismertetőjegyeket közvetít.

Az említett magatartási és ismertető jegyeket az e célból fejlesztett logikai és a humán biztonsági eszközök felismerni képesek, azt egy intelligens rendszernek továbbítják, amelyek döntéseket hoznak a szükséges riasztási fokozatok bevezetésére. Eredményeként riasztás érkezik a banki és biztonsági személyzethez, valamint a fizikai biztonságot működtető döntés végrehajtó központhoz.

A riasztások több fokozatúak lehetnek, vannak olyan riasztások, amelyek ellenőrzést igényelnek, ennek végrehajtásából az ügyfél semmit nem észlel, a banki forgalmat nem zavarják.

A pénzintézeti biztonságtechnika területén a paradigmaváltás lehetséges irányai közül az egyik út tehát az intelligens szoftverek és az érzékelés új típusainak, illetve a másik a **reagálás** eszközeinek és módszereinek fejlesztésében rejlik. A prevencióban talán a legfontosabb szenzitív kérdéscsoport a rendkívüli események bekövetkezése esetén történő válaszadás eszközrendszerének, és módszereinek fejlesztésében rejlik. A pénzintézeti biztonság, elsődleges védelmi feladata, az emberélet védelme. Az értékvédelem erre épülve és ennek érdekében működik.

A reagálási eszközök ilyen lehetséges fejlesztési iránya a füstágyú például, ami a bankrablás esetén az ügyféltér elárasztására alkalmas semleges kémhatású, magas levegőtartalommal rendelkező, de sűrű, átláthatatlan, nagy sebességgel terjedő füst előállítására alkalmas eszköz. A füstfejlesztő fejek megfelelő elhelyezésével az elkövetőt, a pénztártól a kijárat felé ki lehet szorítani. A füst átláthatatlansága mellett pszichés hatást is gyakorol a támadóra, amely automatikusan menekülésre készteti. A bankfiókok ügyfélterében, eredményesen alkalmazhatónak látszik ez az eszköz, de nyilvánvaló, hogy az alkalmazás fizikai, pszichikai és egészségügyi feltételeit alaposan ki kell vizsgálni.

Ezek a kutatási irányok látszanak jelen pillanatban a pénzintézeti védelem jelenlegi új irányvonalainak. Persze a tudományok egymásba ágyazottsága folytán bármi más területen felbukkanó újítás is lehet hatással e biztonsági területre.

Felhasznált irodalom

1. Magyar Biztosítók Szövetsége: Biztonságtechnikai útmutató a betöréses lopás-rablásbiztosítási kockázatok kezelésére (ajánlás)
2. Dr. Kiss Sándor: Biztonságtechnika alapjai, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2004.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Lasz György
georgelasz@gmail.com

GONDOLATOK A KÖZTERÜLETI BIZTONSÁG, TÖMEGRENDEZVÉNYEK BIZTOSÍTÁSA ÉS A MAGÁNBIZTONSÁGI SZOLGÁLATOK KAPCSÁN - DE FACTO

Absztrakt

A végrehajtó hatalom közbiztonság fenntartására létrejött, kényszerítő monopólium birtokosaként a rendőrség mind létszám, mind technikai eszközök hiányában, de leginkább az általa biztosított szolgáltatás magasabb foka miatt nem képes a tömegrendezvények biztosítását önállóan ellátni sőt, szolgáltatásának és rendeltetésének specifikumai miatt számos feladatot a közterületen más nem láthat el. A cikk szerzője publikációban a magánbiztonsági szolgálatok térnyeréséről, felértékelődéséről is értekezik, s arról, hogy a jövőben szerepük növekedésével kell számolni. Fontos kérdés a „mass private property" problematikája, vagyis a magántulajdon sajátos formája, amit sokan fél-magántulajdonként ismernek el, mint a bevásárlóközpontok, vagy épp tömegrendezvények központjai. A biztonsági feladatok országonként eltérő minőségben, mennyiségben jelennek meg, megosztva az állami és civil biztonsági szolgálatok terheit. Ezért is az egyes nemzeti magán biztonsági szolgálatok feladatait egyenként kell elemezni ha a kulturális vagy/és politikai hátteret szeretnénk megérteni – vallja a cikk szerzője egyetértésben egy nemrégiben készült francia kutatással.

As the single owner of the executive power to maintain community safety, the police has neither the necessary staff, nor the technical equipment to secure large scale events on their own. Because of the police's special function and high- value service, many tasks and duties in the public space cannot be outsourced. The author of the study argues that the role and value of private security companies is more and more recognized, and there is an increasing tendency to outsource some of the policing duties. The question of the mass private property - a special form of the private ownership of the public space, as the shopping malls or leisure centers- is an important one. The partnership approach to the policing duties differs from country to country, sharing the burdens of the public and private security sector in different way in each country. The study concludes that in order to understand the cultural or/ and political background in each country, the tasks and duties of the private security services have to be analyzed on a national basis- as it has been done in a recent French study.

Kulcsszavak: *közbiztonság, rendezvénybiztosítás, tömegrendezvények, magánbiztonság, „mass private property” ~ community safety, event securing, large scale gatherings, private security, mass private propety*

Mea culpa

Nemrégiben került a kezembe egy, az Országos Rendőr-főkapitányság által jegyzett tanulmány, amely nagyon helyesen, a tárgyban legfontosabb alapnormára hivatkozva közterületen ellátott feladatnak tekinti a magánbiztonsági szolgáltató által ellátott rendezvénybiztosítást, a pénz- és értékszállítást, a szállítmánykísérést, továbbá részben az értékőrzést is. „Az említett közterületinek minősíthető szolgáltatások közös jellemzője, hogy minden, a törvényben meghatározott esetben szerződésben rögzített konkrét személy- vagy vagyonvédelmi feladatokhoz kapcsolódik, illetve rendezvénybiztosítás esetében a rendező és a résztvevők jogos érdekeit, biztonságát veszélyeztető magatartások elleni védelemben realizálódik. Kétségtelen, hogy e vonatkozásban a magánbiztonság védelmét szolgáló vállalkozói tevékenység szorosan kapcsolódik a közbiztonság fenntartása érdekében foganatosítható rendészeti feladatokhoz, azonban azokkal nem azonosítható és nem is mosható össze. A magánbiztonsági szolgáltató a VSzVMt. hatályos szabályai szerint nem vállalhat általános közbiztonság védelmi feladatot. Erre anyagi jogi felhatalmazottsággal és hatáskörrel sem rendelkezik.”[1]

Jelen alkalommal kerülni szeretném (annál is inkább mert erre korábban több kísérletet tettem) a magán-közbiztonság fogalmi elemeinek elhatárolását, vagy a közbiztonsági feladatok pozícionálását. Amivel azonban semmiképpen nem érthetek egyet, a tanulmányban, az pedig a következő: „A tömegrendezvények biztosítása alapvetően rendőri feladat, amelyben más rendészeti szervek vagy magánbiztonsági szolgáltatók nem vehetnek részt.”[2]

Ha jelen mondat igaz lenne, akkor az elmúlt esztendők megszámlálhatatlan tömegrendezvénye maradt volna tényleges biztosítás nélkül, teremtve ezzel óriási biztonsági kockázatot.

A végrehajtó hatalom közbiztonság fenntartására létrejött, kényszerítő monopólium birtokosaként a rendőrség mind létszám, mind technikai eszközök hiányában, de leginkább az általa biztosított szolgáltatás magasabb foka miatt nem képes a tömegrendezvények biztosítását önállóan ellátni sőt, szolgáltatásának és rendeltetésének specifikumai miatt számos feladatot a közterületen más nem láthat el. Így tehát - mea culpa! – meggyőződéssel vallom, hogy mind a jogalkotó szándéka szerint, mind a helyesen és következetesen kialakult szakmai gyakorlat szerint magánbiztonsági szolgálatok biztosították a legnagyobb tömegrendezvényeket az elmúlt években és szerepük a jövőben sem nélkülözhető, sokkal inkább feladataik kiszélesítésére kerül majd sor. Az, hogy ez mennyire így van, az alábbiakban minden bizonnyal igazolást nyer majd.

A (köz)biztonság szereplői

Az állam, a *végrehajtó hatalom, ám különösen a politika* szereplőinek igazán fontos lenne a közbiztonság kérdései okán kompromisszumot kötni, s az egyes racionalizálási, vagy rendészeti-szakmai kérdések megítélését a szakértőkre, nem pedig lobbycsoportokra vagy az

[1] Kacziba Antal: Lehetséges jövőkép… Rendőrség Tudományos, Technológiai és Innovációs Tanácsa, Kézirat, Budapest, 2010.

[2] Kacziba Antal: Lehetséges jövőkép… Rendőrség Tudományos, Technológiai és Innovációs Tanácsa, Kézirat, Budapest, 2010. 60 p.

ellenzéki vagy épp kormányzati szerepből fakadó rituális szokásokra bízni. Amikor nyilvánvalóvá vált, hogy az állam nem képes polgárai számára a biztonságot, mint alkotmányos jogot garantálni, felvetődik a kérdés: ki pótolja az ekként keletkezett űrt?
Tény, hogy nincs következetes, jól elkülönülő vonalvezetése a közbiztonság alakításának, (talán épp ezért) lehetne érdemi kompromisszumot kötni e kérdésekben.
Murphy törvénye igaz mindenütt, a bűnözésben is, tehát ahol alkalom kínálkozik, ott az állam *polgárai* közül biztosan lesznek, akik megragadják a lehetőségeket. Az állampolgárok szabadságfoka jelentősen megnőtt a korábbi politikai rendszer elvetésével, ám a szabadsággal járó negatív társadalmi deficiteket, különösen a szegénységet, a bűnözés növekedését erős frusztrációként élték meg. Mindig könnyebb elfogadni a jót, az előnyöket, mint megérteni az ezzel járó hátrányokat, s Magyarországon is ez történt. A nagyon gazdag és nagyon szegény rétegek közötti óriási ellentétek feszítik a társadalmat, ami azt is jelenti, hogy a nagyon gazdagok „megvehetik" szinte teljes, saját biztonságukat, a depriváltabb rétegeknek azonban valamilyen másodlagos biztonság jut. Épp ezért e rétegek alkalom esetén könnyen térnek a bűn útjára, vagy használják ki a szabályozatlan területeket. Mindig lesznek akik kihasználják e lehetőségeket, s lesznek olyan marginális csoportok, akik számára ez jelenthet fő megélhetési forrást.
A megváltozott helyzetben a polgárok célpontjaivá válnak a külföldiek, a „tehetetlen" rendőrök, az „erélytelen" politikusok, később pedig a biztonságot megfizetni képes polgárok is. Ennek kiegyenlítésére szükséges az államnak olyan intézkedéseket hoznia, amelyek legalább a bűnözés elfogadható szintű megjelenéséig csökkentik az áldozatok személyi és anyagi terheit.
Mindezeken túl aggasztó módon csökkent a társadalom önvédelmi képessége, amit talán csak az utóbbi időben néhány civil szervezet próbál ellensúlyozni. A közgondolkodás még mindig nem látja tisztán, hogy a bűnözés magában a társadalomban keletkezik, ezért ellene küzdeni is legeredményesebben magában a társadalom alapjaiban, jó és időbeni felismeréssel lehet.
A *rendőrségre* mindig nehéz jogalkalmazói szerepkör jut, amelynek tagjai a hierarchiából fakadóan még csak nem is kritizálhatják az őket érintő folyamatokat. Vagy ha mégis megteszik, karrierjük gyors véget érhet. Emellett a szervezet nem is igazán befogadással tekint az újra, a változásokra, önmegőrző képessége bár sokat veszített az elmúlt években, mégis értékes tulajdonságai között tartandó számon. A rendszerváltással nagyon jelentős súly nehezedett rá[3]. Egyrészt saját múltja mellett fel kellett dolgoznia egy legitimizációs válságot is, amelyeket morális válság kísért. Harmadsorban pedig – s ez a legnehezebb – a szakmai válság megoldása jelent igazán nagy terhet számára, hiszen a személycserékkel új koncepciók mindig, igazi áttörés ritkán érkezik. A rendőrök éppúgy reagálnák a változásokra, mint minden hasonló, mamut állami szervezet, s ráadásul szigorúbb konformitás kényszer terhe alatt.
A *magánbiztonsági szolgálatok* pedig igen, nyugodtan mondhatjuk, hogy immáron a megváltozott közbiztonság legújabb szereplői és segítői.
Nem vitathatjuk, hogy a biztonság itt kiemelt (fő)szereplőin túl minden szereplő helyzete – már ami a bűnözés elviselését illeti – nehezebbé vált. Éppen ezért fontos lenne, hogy a társadalom valamennyi meghatározó szereplője a biztonságot célzó törekvéseket szakmaiságukba ágyazva, nem pedig más, jelentéktelen determinánsokra alapozva ítélje meg.

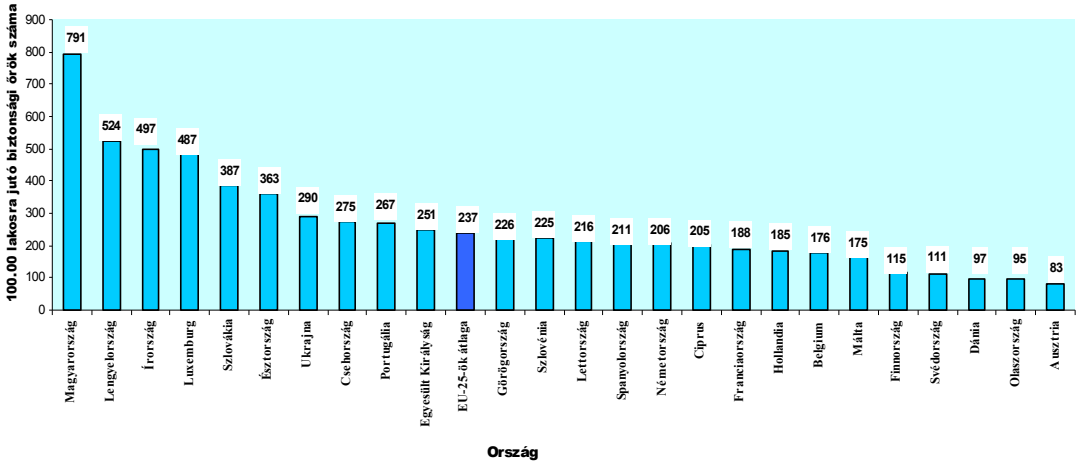
Magánbiztonság Európában

A biztonsági feladatok országonként eltérő minőségben, mennyiségben jelennek meg, megosztva az állami és civil biztonsági szolgálatok terheit. Ezért is az egyes nemzeti magán

[3] Korinek László: A társadalom emésztési zavara avagy a közbiztonság és bűnügyi helyzet Magyarországon. Magyarország politikai évkönyve, Budapest 1998.

biztonsági szolgálatok feladatait egyenként kell elemezni, ha a kulturális vagy/és politikai hátteret szeretnénk megérteni.
A magánbiztonsági szolgálatok megjelenése és elterjedése Európában nemzetközi jelenség, amely három okra vezethető vissza: a fogyasztói társadalom és új tulajdoni formák kialakulására, a rendőri feladatok növekedésére és az Amerikából induló válságra.[4]
A magánbiztonsági őrök száma országonként változik, amint az alábbi táblázat mutatja:

1 Ábra- A magán biztonsági szolgálata létszáma Európában



Forrás: CoESS

Míg az EU átlag 237 biztonsági őr 100.000 lakosra, nagy eltérések tapasztalhatók mind az átlag fölött, mind pedig alatta. Hat ország átlagértéke 350 fölött van, öté pedig 120 alatt.

A legmagasabb értéket Magyarország adja a táblázat szerint. A lakossághoz viszonyított biztonsági őrök száma háromszor nagyobb az EU átlagnál. Ez az egyetlen ország, amelynél ilyen kimagasló az eltérés az EU átlagtól. Három ország átlaga kétszer nagyobb az EU átlagnál: Lengyelország, Írország, Luxemburg. Két EU tagállam átlaga 350- 400 között található: Szlovákia és Észtország. A legkisebb értékkel rendelkező ország Ausztria. A lakossághoz viszonyított biztonsági őrök száma háromszor kisebb az EU átlagnál. Négy ország átlaga kétszer kisebb az EU átlagnál: Finnország, Svédország, Dánia és Olaszország.

Így az EU átlag 14 országra tekintve lényeges, országok melyeknél a 100.000 lakoshoz viszonyított biztonsági őrök száma 175 és 290 között van. Négy ország átlaga kissé magasabb az EU átlagnál: Csehország, Portugália, Egyesült Királyság. A maradék tíz ország átlaga kissé alacsonyabb az EU-snál: Görögország, Szlovénia, Lettország, Spanyolország, Németország, Ciprus, Franciaország, Hollandia, Belgium és Málta.

Amint látható, az eltérések nem magyarázhatók a kulturális különbségekkel. Hogyan lehetséges, hogy Ausztria és Olaszország ugyanabba a kategóriába tartozik mind a skandináv EU tagállamok – teszi fel a kérdést a CoESS[5]? Vagy Írország, Luxemburg miért mutat hasonlóságokat inkább a volt szovjet blokk országaival – Lengyelország, Szlovákia- és miért nem inkább az Egyesült Királysággal vagy Hollandiával? A hagyományos földrajzi- kulturális

[4] La participation de la sécurité privée á la sécurité génerale en Europe. CoESS – Confederation of European Security Services.Livre Blanc, Décembre 2008. Institut National des Hautes Etudes de Securite, France.”Vhite paper Private Security”
[5] La participation de la sécurité privée á la sécurité génerale en Europe. CoESS – Confederation of European Security Services.Livre Blanc, Décembre 2008. Institut National des Hautes Etudes de Securite, France.”Vhite paper Private Security”

térképet átrendezi ez a függvény. Azt mutatja, hogy a magán biztonsági szolgálatok elterjedése sokkal inkább a piaci igényekhez[6] alkalmazkodik, mint a politikai szabályozáshoz. E szabály alól csak Skandinávia kivétel.

A „mass private property" megjelenése

„A magánterület védelme ezzel szemben magánbiztonsági kérdés, fő szabályként magánbiztonsági védelmi aktivitást feltételez. Azzal a már érintett kivétellel, amikor a magánterület védelmét valamely nyomós közérdekből rendészeti eszközökkel szükséges megoldani" – fogalmaz a bevezetőben hivatkozott magyar rendőrségi tanulmány.[7] Az egyik legérdekesebb kérdés azon magánterületek kérdése, amelyeket tömegesen vesznek igénybe használóik. Ezek a bevásárlóközpontok, de sportcsarnokok is, leginkább a tömegrendezvények helyszínei. Jellemzően ezek közrendjét általában szinte kizárólag magánbiztonsági szolgálatok biztosítják.

A köz- és magánszféra közelítése a közbiztonság és a tömegrendezvények okán

A közbiztonsági szervekkel ellentétben, a magán biztonsági szolgálatok feladatait szerződésben rögzítik. Magánterületeken (bevásárlóközpontok, irodaházak, stb) és közterületeken (repülőterek, metróállomások, középülete, stb) feladataikat sokszor a hatóságok mellett, azok kiegészítéseként végzik. A köz- és magán biztonsági szolgálatok együttműködése nagyon sokszínű és sokrétű, ezt a CoESS tanulmánya is megerősíti. Ez a kutatási metódus nem új keletű. 1998-ban, egy London környékén végzett felmérés során brit kutatók[8] már rendszerezték a közszféra és a magánszféra együttműködését a rendfenntartás terén. Három kategóriát állítottak fel: együttműködés, versengés és párhuzamos működés. Ezek a kategóriák bármely feladat elemzésére használhatók bármely adott időszak vizsgálatakor. Nem államonkénti sajátosságokat és nem irányzatokat foglalnak magukba, hanem a közszféra és a magánszektor adatainak összehasonlítására használhatók. Az együttműködés szempontjából vizsgálva, kijelenthetjük, hogy a magán biztonsági szolgálatok átveszik a rendőrségtől azok feladatainak egy részét, hogy a közbiztonsági szerveknek nagyobb erőforrásuk legyen központi feladataik ellátására.[9]
A kooperáció területei az alábbiak lehetnek:

- általános együttműködés
- integrált együttműködés
- stratégiai együttműködés
- helyi együttműködés
- opportunista együttműködés és
- ad-hoc együttműködés.

A felsoroltak közül az opportunista együttműködés igényel magyarázatot, amely Romániai példával világítható meg: itt az együttműködés a bűnmegelőzésre is kiterjed. Mivel a rendőrség gépkocsiparkja nem számottevő, ezért 1998-ban megállapodást kötöttek a magán biztonsági szolgálatokkal gépjárművek kölcsönzésére. Sőt, megállapodást kötöttek néhány magán biztonsági szolgálattal, melyben felhatalmazzák őket a közrend fenntartásával és az

[6] Az őrző védő feladatok nagy száma kereskedelmi létesítmények őrzését és a bolti lopások megakadályozását szolgálja.
[7] Kacziba Antal: Lehetséges jövőkép… Rendőrség Tudományos, Technológiai és Innovációs Tanácsa, Kézirat, Budapest, 2010.
[8] Trevor Jones & tim Newburn, Private security and public policing, Clarendon Press, Oxford, 1998
[9] La participation de la sécurité privée á la sécurité génerale en Europe. CoESS – Confederation of European Security Services.Livre Blanc, Décembre 2008. Institut National des Hautes Etudes de Securite, France."Vhite paper Private Security"

antiszociális viselkedés visszaszorításával. Így a rendőr és a biztonsági őr ugyanazon időben, ugyanabban a gépjárműben járőrözik.

Összegzés

Fentiekből kitűnik, hogy a de jure szabályozás kialakítását a tömegrendezvények biztosításában a gyakorlat alakítja. Ebben a magánbiztonsági szolgálatok jelentős feladatokat vállalnak magukra, ezért helyes majd, ha véleményük megjelenik a jogi szabályozásban is. Nem szabad elfelejteni, hogy a rendőrséggel közösen jelentős tapasztalati kincs birtokában, magas felkészültséggel és tapasztalattal sokat segítenek a közterületi és rendezvényi biztonság megalapozásában.

Felhasznált irodalom

1. Kacziba Antal: Lehetséges jövőkép… Rendőrség Tudományos, Technológiai és Innovációs Tanácsa, Kézirat, Budapest, 2010.
2. Korinek László: A társadalom emésztési zavara avagy a közbiztonság és bűnügyi helyzet Magyarországon. Magyarország politikai évkönyve, Budapest 1998.
3. La participation de la sécurité privée á la sécurité génerale en Europe. CoESS – Confederation of European Security Services.Livre Blanc, Décembre 2008. Institut National des Hautes Etudes de Securite, France.”Vhite paper Private Security”
4. Trevor Jones & tim Newburn, Private security and public policing, Clarendon Press, Oxford, 1998

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Bárdos Zoltán
zoltan.bardos@katved.hu

A VESZÉLYES ANYAGOK SZÁLLÍTÁSÁNAK SZABÁLYOZÁSA ÉS A KÖZÚTI SZÁLLÍTÁSOK ELLENŐRZÉSÉNEK FEJÉR MEGYEI TAPASZTALATAI

Absztrakt

Mai világunk egyik legdinamikusabban fejlődő iparága a vegyipar. Sokhelyütt gyártanak, tárolnak és alkalmaznak alapanyagként vagy késztermékként olyan veszélyes anyagokat, amelyek potenciálisan veszélyeztethetik az emberi életet és környezetet. Ezeket a kockázatot jelentő anyagokat közúton, vasúton, földi vízi vagy légi úton belföldre és külföldre egyaránt szállítják, mely önmagában is egy veszélyes művelet. A tevékenység veszélyes jellege magából a szállított anyagból és a szállítás tulajdonságaiból tevődik össze. Köztudott, hogy a világon az egyik legveszélyesebb üzem, - ahol a legtöbb baleset és elhalálozás történik -, a közúti szállítás. Igaz, a közúti veszélyesáru-szállításra vonatkozó nemzetközi előírás (ADR) folyamatosan követi a technológiai fejlesztéseket és szabályozza a szállításokat, de a végrehajtás terén hiányosságok mutatkoznak. Gondot nemcsak a rakomány nem megfelelő előkészítése, a szállítmányok rögzítésének hiányosságai vagy a szállító fegyelmezetlensége okozza, hanem sok esetben a fuvarokmányok pontatlansága, a szállítmány tartalmára vonatkozó megtévesztés, a közlekedési és szállítmányozási fegyelem megsértése. A veszélyes anyagok közúti szállításának veszélyei nemcsak Magyarországon, hanem az egész világon súlyos problémát jelentenek a lakosság és az esetleges balesetek felszámolásában résztvevő szervezetek számára. A balesetek során, a szabadba kijutó anyagok szennyezhetik a talajt, az atmoszférát, az élelem, az ivóvíz és takarmány készleteket, pusztulást okozhatnak az állat- és növényvilágban. Jelen írásban vizsgálom a veszélyes áruk szállításának szabályozását, valamint a Fejér megyében végrehajtott közúti szállítások ellenőrzésének tapasztalatait.

One of the most rapidly growing area of the world's economics is the chemical industry. Dangerous substances as raw materials or end-products are produced, stored or used in many places, this way potentially endangering human health and the environment. These hazardous materials are transported by road, railway, on ground, river or in the air, both inland and abroad, which means dangerous activity even on its own. The danger comes both from the transported material and the way of transportation. It is well known, that one of the most dangerous activities in the world - where most of the accidents and human deaths happen – is the road transportation. However, the international regulation

concerning road transportation of dangerous goods (ADR) is developing continuously to follows technological improvements in order to control deliveries, but there are deficiencies with the enforcement. There are problems not only with improper preparation of the cargo, fixation defects of shipments or misconduct of transporters, but in many cases inaccuracies in transportation documents, intended deceptions concerning cargo content or breach of traffic and transport regulations. Dangers emanating from road transportation of dangerous goods mean a massive problem to the population and the disaster response organizations not only in Hungary but all over the world. During an accident, dangerous materials coming out to the environment can pollute the soil, the atmosphere, food, drinking water and stover reserves, can damage the fauna and the flora. The author in paper investigates the regulations concerning transportation of dangerous goods and experiences of road transportation controls in Fejér County.

Kulcsszavak: *veszélyes áruk szállítása, ADR, veszélyes anyagok, közúti szállítás ellenőrzése ~ transportation of dangerous goods, ADR, dangerous materials, road transportation control*

Bevezető

A hétköznapi ember számára nem biztos, hogy egyértelmű és világos a veszélyes anyag fogalma. Mit tekintünk veszélyes anyagnak, mitől veszélyesek ezek az anyagok, milyen veszélyeztető tényezők vannak és ezek milyen hatással, lehetnek az emberre és a környezetre? Azt hiszem ezeket az alapfeltevéseket célszerű először röviden tisztázni mielőtt a veszélyes anyagok szállításával kapcsolatosan felmerülő kérdések vizsgálatára rátérnék. Magyarországon a kémiai biztonságról szóló törvény[1] biztosítja, „az ember legmagasabb szintű testi és lelki egészségéhez, valamint az egészséges környezethez fűződő alapvető alkotmányos jogait" ez a jogszabály fogalmazza meg a veszélyes anyagok és veszélyes keverékek káros hatásainak megfelelő módon történő azonosítását, a megelőzése, az elhárítás feladatait. A veszélyes anyagok fogalmát több jogszabály és szakmai útmutató is tartalmazza, amelyekről elmondható, hogy egyik részük tudományos, míg másik részük az alkalmazás szempontjait veszi figyelembe. A különböző szakmai anyagok (publikációk) a tudományos megközelítést választják, és olyan anyagként tekintenek rá, amely az emberi életre és a környezetre azok elemeire káros hatással vannak. A szakirodalomban elmélyedve azt tanulmányozva az anyagok veszélyes, vagy veszélytelen minősítése igen bonyolult, szinte definiálhatatlan a veszélytelenség. A veszélyes és veszélytelen megítélése a kritérium rendszertől függ, mely kritériumot ki és hogyan fogadja el, így feltételek sorozata dönti el a veszélyesség mértékét. A jogszabályok más utat választva taxatív módon felsorolják az anyagokat és az alkalmazás célját figyelembe véve, mennyiségekhez is kötik. A veszélyes anyag meghatározása több jogszabályban is megtalálható a katasztrófavédelmi törvény[2] végrehajtási rendeletének[3] mellékletében meghatározott küszöbérték mennyiségek (kritikus tömeg) alapján kerültek az üzemek alsó vagy felső küszöbérték szerint veszélyességi besorolásba.[1] A kémiai biztonságról szóló törvény 3. § (1) bekezdése és a végrehajtási

[1] 2000. évi XXV. törvény a kémiai biztonságról
[2] 1999. évi LXXIV. törvény a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről
[3] 18/2006. (I. 26.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről

rendelete[4] 1. számú melléklete szerint a veszélyesnek minősülő anyagokat csoportosítják, és sajátosságaik szerint történik az anyagok veszélyesség szerinti osztályozása az alábbiak szerint.

Általános követelmények a veszélyes anyagok és készítmények osztályozására és feliratozására (címkézésére)[2]:

1. Osztályozás fizikai-kémiai alaptulajdonságok alapján
2. Osztályozás toxikológiai tulajdonságok alapján
3. Osztályozás a környezeti hatások alapján

1. Fizikai-kémiai tulajdonságok

1.1. Robbanásveszélyes

1.2. Égést tápláló, oxidáló

1.3. Fokozottan tűzveszélyes

1.4. Tűzveszélyes

1.5. Kevésbé tűzveszélyes

1.6. Egyéb tényezők

2. Toxikológiai sajátosságok

2.1. Nagyon mérgező

2.2. Mérgező

2.3. Ártalmas

2.4. Maró

2.5. Irritatív

2.6. Túlérzékenységet okozó (allergizáló, szenzibilizáló)

2.7. Specifikus egészségkárosító sajátosságok: szerv vagy szervrendszer specifikus hatások heveny, félheveny vagy idült mérgezésben vagy azt követően, amelyek súlyosak és nem súlyosak, reverzíbilisek vagy irreverzíbilisek lehetnek

2.8. Rákkeltő

2.9. Mutagén

2.10. Reprodukció-károsító (szaporodást károsító)

2.11. Egyéb jellemző tulajdonságok (bőrön át felszívódik, kumulálódik stb.)

3. Ökotoxikológiai, környezetkárosító, környezetszennyező sajátosságok

3.1. Nagyon mérgező

3.2. Mérgező

3.3. Ártalmas

[4] 44/2000. (XII. 27.) EüM rendelet a veszélyes anyagokkal és a veszélyes készítményekkel kapcsolatos egyes eljárások, illetve tevékenységek részletes szabályairól

A veszélyes anyagokkal kapcsolatos problémakör a XX. század elejétől a vegyipar ugrásszerű fejlődésétől kezdve létezik. A bekövetkezett balesetek elleni védekezés helye, gyakorisága és módszerei alapján a kérdéskört kétfelé kell választani: a gyártás, tárolás, feldolgozás, raktározás helyhez kötött tevékenység, amelyekre a beavatkozási és lakosságvédelmi tervek elkészíthetőek, a mennyiségek viszonylag könnyen ellenőrizhetőek a gazdálkodóknál, a hatósági munka tervezhető. Ezzel ellentétben a másik terület: a szállítás területe nehezen tervezhető, a változó helyszín, mennyiség miatt a beavatkozások és a lakosság védelme sokkal nehezebben előkészíthető így lehetséges ad hoc jellegű beavatkozás is.
A katasztrófavédelmi törvény IV. fejezetében a súlyos ipari balesetek megelőzésének és elhárításának átfogó jogi szabályozásával foglalkozik, azonban hatálya nem terjed ki a veszélyes anyagoknak a létesítményeken kívüli közúti, vasúti, légi és vízi szállítására.[1] A publikációban a veszélyes anyagok közúti szállításának szabályozásával és a szállítás szabályainak betartásának az ellenőrzésével foglalkozom.

A veszélyes áruk[5] szállítási szabályainak történeti áttekintése

A veszélyes áruk közúti szállításának szabályozása egészen a 18. századra nyúlik vissza. Először 1799-ben a lőpor lófogattal való szállítására készült szabályozás. Ez tíz évvel az első speditőrökre vonatkozó münsteri rakományrögzítési előírás után készült a biztonságos közlekedés elősegítése érdekében. A vízi szállítás szabályozásának kezdete 1831-re datálható, és a „Mannheimi Akta" 1868-től szabályozza a veszélyes áruk szállítását a Rajnán. A Németországból származó előírások értelmében a Rajnán behajózott veszélyes szállítmányokra fekete olajfestékkel rá kellett írni a „Méreg!" feliratot.
A vasúti veszélyes áru fuvarozás szabályozásának kezdete 1890-re tehető, majd az első nemzetközi egyezmény 1893-ban született meg, melyben Svájc és Németország szabályozta a veszélyes áruk vasúti szállítását egymás országai között. A RID 1894-ben került megalkotásra. A veszélyességi bárcák 1928-ban jelentek meg először, amelyeket robbanóanyagok esetén vörös felrobbant bomba, maró anyagok esetén vörös vesszőfonatos üvegballon, a gyúlékony anyagok esetén pedig vörös alapon fekete fáklya szimbólumokkal jelképeztek.
A második világháborút követően az ENSZ 1945 óta világviszonylatban foglalkozik a veszélyes áruk biztonságos szállításának kérdéseivel. Az illetékes szerve az ECOSOC, amelynek egyik albizottsága a „Veszélyes Áruk Szállításának Szakértői Csoportja" végzi az operatív munkát.
Az ECOSOC feladatának tekinti minden szállítási mód tudományos, műszaki és adminisztratív alapjainak kidolgozását. Az ENSZ ajánlások -Veszélyes áruk szállítása- címmel 1956-ban jelent meg először előírás a szállításokra vonatkozóan. Az IRU (International Road Transport Union) 1948-ban alakult és aktívan közreműködött az ADR 1957-es születésében. Az ADR-t (European **A**greement concerning the international carriage of **d**angerous goods by **r**oad) az európai országok kötötték 1957. szeptember 30-án Genfben és 1968. január 29-től hatályos. AZ ADR-hez mostanáig 43 tagállam csatlakozott. A magyarországi csatlakozás 1979-ben volt, miután Aszódon 1976-ban súlyos etilén baleset történt. Az ADR ugrásszerű fejlődése az 1978. július 11-én a spanyolországi Tarragona közelében, Los Alfaques-ben történt propilénkatasztrófa után kezdődött.
Jelenleg már kétévenként rendszeresen módosítják az ADR- t, egyrészt a vegyipari és műszaki-technikai fejlődéshez való igazítás, másrészt pedig a világszintű előírásokhoz való

[5] **Veszélyes áru**nak nevezzük azokat a áruféleségeket (anyagokat és tárgyakat), amelyek a szállításuk során tűz- és robbanásveszélyt, egészségkárosító (főként maró, mérgező) hatást vagy környezetkárosító tulajdonságokat hordoznak, s amelyeket ilyenként azonosít valamely közlekedési ágazat veszélyes áru szállítási szabályzata. http://hu.wikipedia.org/wiki/Vesz%C3%A9lyes_%C3%A1ruk_sz%C3%A1ll%C3%ADt%C3%A1sa

illesztés céljából. A spanyolországi katasztrófa következtében indult el intézményesített formában a veszélyes árut szállító gépjárművezetők képzése is, először Németországban. A veszélyes áru szállítási biztonsági tanácsadók képzése - az 1987-es németországi herborni súlyos baleset - következtében kezdődött meg 1989-től szintén Németországban.
Magyarországon először 1977-től a Hungarocamionnál képezték az etilént szállító tartányjárművek vezetőit, majd 1980-tól a nemzetközi fuvarozásban résztvevő gépkocsivezetők is kaptak ADR képzést. Nemzetközi szinten 1980-ban az IRU javaslatot készített az ADR képzés egységesítésére és összehangolására. Ezek után az ADR-ben először 1983. január 01-től írták elő a tartányos gépkocsivezetők kötelező ADR képzését, majd 1985-től a vizsgakötelezettséget is. A vizsgáztatási jogot Magyarországon az 1983-ban létrehozott Közlekedési Főfelügyelet (jelenleg Nemzeti Közlekedési Hatóság) kapta. Az ADR-ben sokáig csak a tartányos gépjárművezetők képzése volt szabályozva. A robbanóanyagok és tárgyak – 1 osztály – szállítását végző gépjárművezetők képzését 1990-től írja elő az ADR. A nem tartányos képzés (2-9 osztály küldeménydarabok és ömlesztett áru) 1995-től jelent meg az ADR-ben, ha 3,5 t legnagyobb megengedett össztömeg feletti járművel történik a szállítás. Ezt 2005. január 01-től terjesztették ki a 3,5 t-nál kisebb járművekkel végzett szállításokra (az átmeneti idő 2 év). Rómában 1994-ben a WP. 15 határozata szerint informális ülésen tanácskoztak az országok az ADR képzés egységesítése tárgyában. Az ADR-ben ezután erősen a német képzési gyakorlat felépítését követő képzési rendszer jelenik meg. Ugyanakkor a mai napig jelentős eltérések mutatkoznak a különböző országok ADR képzésében és feltételrendszerében. Ezért is fontos az IRU törekvése az ADR képzés akkreditációs rendszerére vonatkozóan, hogy a vizsgakövetelmények, a tematika, képzési idő, gyakorlati képzés egységesíthető legyen.

Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Európai Megállapodás (ADR)[3]

A veszélyes anyagok közúti szállítására az **ADR** nemzetközi veszélyes áru szállítási szabályzat előírásai vonatkoznak. Ez magában hordozza azokat a biztonsági előírásokat, melyek betartása mellett az előre nem látható (külső) behatásokat leszámítva a szállítás alapvetően biztonságosan végezhető. Az ADR „A” és „B” mellékletének kihirdetéséről és belföldi alkalmazásáról szól a 20/1979. (IX.18) KPM rendelet, amely 1979. augusztus 18. óta hatályos és kötelezővé teszi a nemzetközi előírások hazai alkalmazását. Az ADR azon járművekre értelmezhető, amelyek legalább négy kerékkel rendelkeznek és nem számítanak lassú járműnek,vagy mezőgazdasági vontatónak. Utóbbiakkal való mezőgazdasági vegyszer- illetve üzemanyag-szállítást a 113/2004.(IX.23.)GKM rendelet belföldön az általános (értsd ADR) előírásoktól kissé eltérő módon szabályozza.

A Megállapodás szövege rövid és egyszerű. A lényege a második cikkben van, mely kimondja:

1. Azok a veszélyes áruk, amelyeknek szállítását az „A” Melléklet megtiltja, nemzetközi szállítás tárgyát nem képezhetik.
2. Egyéb veszélyes áruk szállítása megengedett, ha:
   a) a szóban forgó árura, különösképpen annak csomagolására és bárcázására vonatkozóan az „A” Mellékletben előírt feltételeket, és
   b) a szóban forgó árut szállító jármű szerkezetére, felszerelésére és közlekedésére a „B” Mellékletben előírt feltételeket teljesítették.

Az „A” és a „B” Melléklet követelményrendszerét az ADR hatálybalépése óta rendszeresen kiegészítik, illetve korszerűsítik. A Mellékletek teljes átstrukturálására legutóbb 1992 és 2000 között került sor, amelynek első verziója, vagyis az *ADR 2001* 2001. július 1-től, 2003. június

30-ig volt használatban. Ezt váltotta a második, a harmadik és negyedik verzió (*ADR 2003*, *ADR 2005 ill. ADR 2007*), amelyek közül utóbbi 2007. július 1-től, 2009. június 30-ig volt hatályos. Az ADR 2007 előírásai 2009. július 1-jétől nem használhatók; a legfrissebb kiadást ADR 2009 néven ismerjük (kihirdetve a 2009. évi LVIII. törvénnyel[6]). Az ADR Európai Uniós hatálybalépését a veszélyes áruk szárazföldi szállításáról szóló, 2008. szeptember 24-i 2008/68/EK európai parlamenti és tanácsi irányelv rendelte el. Ez az irányelv mellékletében tartalmazza, hogy az egyes uniós tagállamok milyen belföldi eltéréseket írhatnak elő. Az ADR belföldi alkalmazására a 38/2009.(VIII.7.) KHEM rendelet 2. Melléklete tartalmaz könnyítéseket.

A veszélyes árúk szállításának kockázatát sokan hajlamosak alábecsülni, pedig nincs olyan veszélyes árú, amely az élő anyagra és a környezetre nézve minden tekintetben teljesen veszélytelen volna. Minden ismeretlen, nem tisztázott eredetű vagy egyértelműen nem azonosítható veszélyes árút erősen mérgezőnek, tűz- és robbanásveszélyesnek kell tekinteni mindaddig, amíg arra illetékes szakértő nem azonosítja.

A szállító jármű megjelölését a rakodás megkezdése előtt kell elvégezni. Az árudarabokat az ADR által meghatározott jelöléssel, egyes csomagolások minősítési jellel ellátva rakhatók fel a szállító járműre. A veszélyes árúk szállítása esetén alapvető jelentősége van a rakomány megfelelő elhelyezésének, rögzítésének a gépjárművön, tekintettel arra, hogy a járműről esetleg lehulló árudarabok, amelyek veszélyes anyagot tartalmaznak sérülésük révén súlyos károkat okozhatnak. Az a személy, aki a ráháruló feladatokat a szállítás során (szállításnak része a szállítás során történő ideiglenes tárolás az árú becsomagolása, továbbá be- és kirakodása, beleértve a töltést és ürítést is) nem a jogszabálynak megfelelően végzi, szabálysértést követ el.

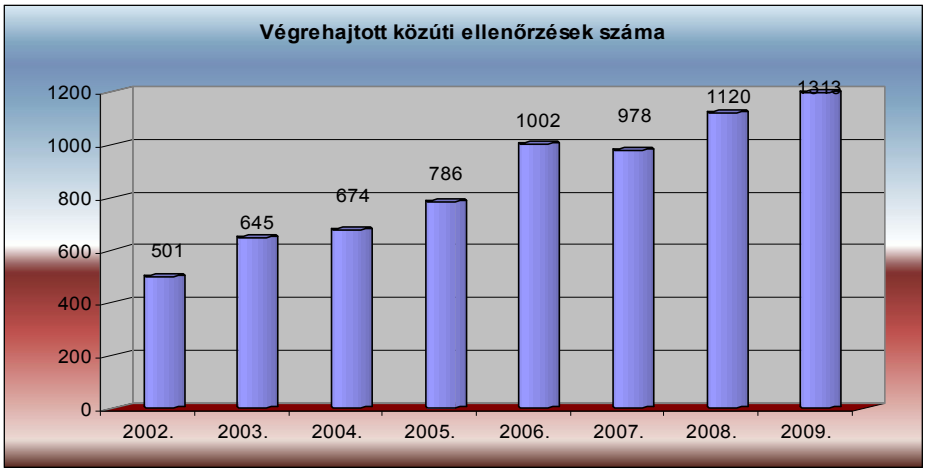
Az utolsó „hagyományos" – un. szélzetszámos rendszerű ADR 1999-ben jelent meg. Az ADR „átszerkesztési munkái"-nak befejezésével, az európai hagyományokkal – tradicionális RID rendszer – való szakítás is megtörtént egyben és az átszerkesztett ADR már a globalizáció jegyében született 2001-ben. Az új ADR-rel egyrészt az előírások is közeledtek egymáshoz, másrészt a számítógépes feldolgozás is könnyebbé vált ezért is nevezik „felhasználó barátabb" szabályozásnak. A veszélyes áruk Európai Unión belüli szállításáról a többször módosított 94/55 EGK Tanácsi Irányelv az ún. „ADR keretirányelv" rendelkezik. Ennek az irányelvnek az értelmében 1997. január 01-től a mindenkori hatályos ADR „A" és „B" Mellékletével egyező előírásokat kell alkalmazni az EU-n belüli veszélyes áruk belföldi szállítására is.

A katasztrófavédelmi igazgatóság ellenőrzési tapasztalatai

A katasztrófavédelem együttműködőként 2001-től vesz részt a veszélyes áruk közúti szállításának ellenőrzésében. A célkitűzés az ellenőrzések megkezdése óta az volt, hogy a lakosság egészsége és a környezet védelme érdekében minél magasabb szinten felkészült szakemberek végezzék az ellenőrzéseket. Ezért a katasztrófavédelem szervezetéből legalább OKJ-s ADR/Veszélyes áru ügyintézői bizonyítvánnyal rendelkező munkatársak végezhették az ellenőrzéseket. Az évek során több mint kétszázan szerezték meg ezt a végzettséget, és néhányan – magukat továbbképezve – biztonsági tanácsadói képzettséggel is rendelkeznek. Az ellenőrzések 2007-ig csak a rendőrséggel, közlekedési hatósággal együtt voltak lehetségesek, tekintve, hogy a katasztrófavédelemnek önálló megállítási jogköre nem volt. Ebben az időszakban jellemző volt, hogy a társ hatóságok a veszélyes árut szállító járművek ellenőrzését (a veszélyes árura vonatkozó előírások betartása vonatkozásában) teljes

[6] 2009. évi LVIII. törvény a Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Európai Megállapodás (ADR) „A" és „B" Melléklete 2009. évi módosításaival és kiegészítéseivel egységes szerkezetbe foglalt szövegének kihirdetéséről

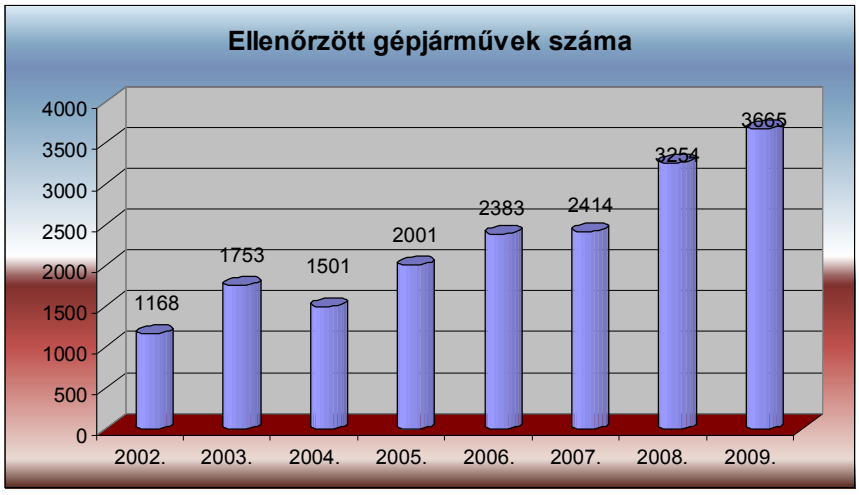
egészében átengedték a katasztrófavédelem szakemberi részére, tekintettel arra, hogy a kollégáink alaposabb képzésben részesültek, így az ellenőrzések részletesebbek, a hiányosságok feltárása alaposabb volt. A megfelelő bírságrendelet hiányában azonban egy-egy hiányosság feltárása komolyabb szankcióval nem járt a szállításban résztvevők részére. Ebből kifolyólag sokan az ADR előírásainak „laza" betartása mellett szállították a veszélyes árut, komoly kockázatot jelentve a közlekedésben részt vevőkre és a lakosság egészségére, valamint a környezetre.
2007. május 1-től a közúti közlekedésről szóló törvény[7] módosítása a katasztrófavédelmet önálló hatóságként beemelte az ADR ellenőrzést végzők közé, így önálló jogkörrel tudtuk az ellenőrzéseket folytatni. Ezzel párhuzamosan sor került az ADR-ben foglaltak megsértése miatt kiszabandó bírságokat tartalmazó külön rendelet kiadására, mely a bírságtételeket olyan szintre emelte, amely a veszélyes árut szállítókat az ADR-ben foglalt előírások alaposabb betartására sarkallta. Mivel a közigazgatási bírságok a kiszabó szervezetet illették meg 2010. január 1-ig, - és a befolyt bírságokat kizárólag az ADR ellenőrzéssel kapcsolatos tevékenység fenntartására és fejlesztésére lehetett fordítani -, így igazgatóságunknak lehetősége nyílt a megfelelő felszerelések beszerzésére a tevékenység folytatásához.



1. ábra. Országosan végrehajtott ellenőrzések száma 2002-2009, Forrás[8]

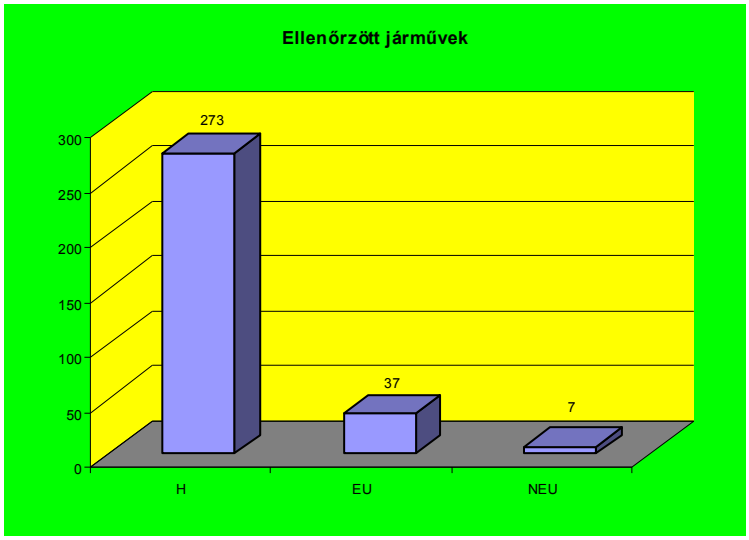
Az 1. ábrán látszik, hogy az ellenőrzések száma (országosan) a szakemberek képzésének számával együtt az évek folyamán növekszik. A katasztrófavédelem területi szervei különböző mértékben ugyan, de jelentős erőfeszítéseket tettek az ellenőrzések rendszeresebbé tételére, az ellenőrzések számának növelésére.

[7] 1988. évi I. TÖRVÉNY a közúti közlekedésről
[8] Országos Katasztrófavédelmi Főigazgatóság 2009. évi ADR összefoglaló jelentés



2. ábra. Az ellenőrzött gépjárművek száma országosan 2002-2009, Forrás[9]

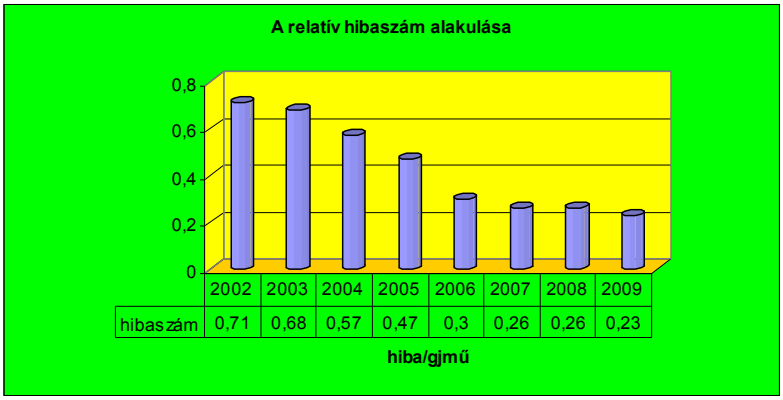
A 2. ábrán az ellenőrzött gépjárművek száma látszik, mely szintén folyamatos növekedést mutat. 2009-ben a katasztrófavédelem szervezetében országosan összesen 159 képzett (OKJ-s végzettséggel rendelkező) ADR ellenőr hajtott végre ellenőrzéseket. A legtöbb ellenőr (11-11 fő) Békés és Tolna megyékben, valamint a Fővárosban tevékenykedett, a legkevesebb (4 fő) pedig Fejér megyében. Az ellenőrzött járművek száma Fejér megyében 317 db, Békés megyében 330 db, Tolna megyében 239 db, és a Fővárosban 187 db volt.
Az ellenőrzések nem csak a narancssárga táblával megjelölt gépjárművekre terjednek ki, hiszen az ADR 1.1.3.6 bekezdésében foglalt mentességi határ alatti szállításoknál a gépjárművet nem szükséges megjelölni. 2009-ben országosan 7305 db olyan gépjármű ellenőrzésére került sor, amely nem volt narancssárga táblával megjelölve, és nem is szállítottak veszélyes árut. Ilyenkor az ellenőrzés csak a fuvarokmány és a rakomány megtekintésére terjed ki. A nem jelölt járművek vizsgálata során az ellenőrök több esetben tártak fel veszélyes áruszállítást, melyek közül többnél a vonatkozó előírásokat betartották, de sajnos több olyan szállítás is történt ahol a szabályok betartásának még a szándéka sem volt meg.



3. ábra. Fejér Megyében 2009-ben ellenőrzött gépjárművek száma, Forrás[10]

[9] Országos Katasztrófavédelmi Főigazgatóság 2009. évi ADR összefoglaló jelentés
[10] Fejér Megyei Katasztrófavédelmi Igazgatóság 2009. évi beszámoló jelentése

Az igazgatóság hatósági jogkörével élve a 2009-es évben 61 ellenőrzési alkalommal 317 gépjármű, továbbá 16 telephely ellenőrzése történt meg. A 3. számú ábrán az ellenőrzött gépjárművek számszaki adatai láthatóak hazai, EU és nem EU bontásban. Az ellenőrzések következtében 96 esetben került sor bírság kiszabására veszélyes áruszállítással kapcsolatos szabálytalanságok megsértése miatt. Általánosságban elmondható, hogy hiányosságok feltárására legtöbb esetben a belföldi fuvarozást vállaló kisebb hazai vállalkozásoknál, illetve az Európai Unióból származó külföldi cégek gépjárműveinél kerül sor.
Számos hiányosság volt az ADR 1.1.3.6 bekezdésében szereplő bizonyos mentességi határ alatti mennyiséggel szállítók körében. Ezekben az esetekben a szállítók rendszeresen úgy végezték a szállítást, mintha egyáltalán nem vonatkozna rájuk semmilyen ADR szabály, ami viszont nem felel meg a hatályos jogszabályoknak, így az ilyen esetek jelentős számában a súlyos mulasztások miatt nagy összegű bírság kiszabására került sor.
Az egyes területi szervek között jelentős eltérés mutatkozik a hiányosságok feltárásában, az ellenőrzések hatékonyságában. Az igazgatóságok statisztikáit tekintve a felderítés adatai még mindig nagy szórást mutatnak (0–34%).



4. ábra. A relatív hibaszám alakulása 2002-2009, Forrás[11]

A 4. ábra a relatív hibaszám alakulását mutatja, melyből látható, hogy a szállítók egyre jobban odafigyelnek a szállításokra. Ez egyértelműen a megnövekedett bírságtételekkel magyarázható, azonban a szabálytalan szállítások száma stagnál. Ez arra vezethető vissza, hogy a közlekedési morál, a szállítói fegyelem ugyan mutat pozitív változást, viszont a növekvő jelenlét a közutakon, a hatékonyság növelő intézkedések, valamint a nem jelölt járművek fokozottabb ellenőrzése előhozza azokat a látens hibákat, hiányosságokat is, amelyek eddig nem kerültek az ellenőrök látókörébe.
Ezek az adatok is jelzik annak a létjogosultságát, hogy a hivatásos katasztrófavédelmi szervek a továbbiakban is önálló hatóságként lépjenek fel a veszélyes áruk szállításának ellenőrzése során. Az ellenőrzések szükségességét és hatékonyságát igazolja, hogy a tárgyidőszakban szakembereink több, a korábbiakban már ellenőrzött gépjárművel találkoztak, amelyek üzembentartói a feltárt hiányosságokat időközben pótolták.
A hiányosságok területén a legtöbb hiba a fuvarokmányok nem megfelelő vezetése mellett a tűzoltó készülékekkel, valamint a rakományrögzítéssel kapcsolatosan fordult elő. Kiemelten kezelendő az írásbeli utasítás hiánya, a járművek, illetve a küldeménydarabok nem szabályos jelölése, bárcázása, valamint jelentős mértékű a védőfelszerelések és a figyelmeztető jelzőeszközök hiánya, érvényességi idejének lejárta, vagy működésképtelensége.
Sajnálatos módon még mindig jelentős azon szállítmányok száma, melyeknél a szabálytalanságok halmozottan jelentkeztek. Több esetben találkoztak ellenőreink olyan

[11] Országos Katasztrófavédelmi Főigazgatóság 2009. évi ADR összefoglaló jelentés

veszélyes árut szállító gépjárművel, mely az ADR egyetlen előírását sem tartotta be. Ezek között egyaránt találhatók voltak hazai és külföldi gépjárművek is.
Az 1/2002. (I. 22.) Kormányrendeletben[12] foglaltak szerint az I. kategóriájú hiányosságok feltárásakor a veszély elhárítására azonnali intézkedéseket szükséges megtenni, így a legtöbb esetben a gépjármű nem közlekedhet tovább a hiányosság kijavításáig. Ezek az ún. kényszervárakoztatások amellyel igazgatóságunk ellenőrei is többször éltek az elmúlt évben.
A katasztrófavédelem a veszélyes áruk közúti szállításához kapcsolódó feladatokat telephelyen is ellenőrzi. Ezen ellenőrzések kiemelt fontosságúak, hiszen a szabálytalanságok nagy része már a telephelyen, a szállítás megkezdése előtt megelőzhető, így növekedhet a lakosság és a környezet biztonsága. A telephelyi ellenőrzéseket az is indokolja, hogy feltehetően a Seveso II. szabályozás hatálya alóli mentesség érdekében, a gazdálkodók egy része veszélyes anyagaikat rendezetlen helyzetű ipari parkokban és kisebb telephelyeken igyekeznek elhelyezni. Igazgatóságunk ADR ellenőrzései tervezése során folyamatosan törekszik a közúti és telephelyi ellenőrzések arányosságára, ami eddig sikerült.

Az ellenőrzések tervezése és végrehajtása

Az ellenőrzések tervezésére vonatkozóan az Országos Katasztrófavédelmi Főigazgatóság (OKF) által kiadott – ADR ellenőrzések végrehajtására vonatkozó – hatályos Utasítása tartalmaz iránymutatásokat. Igazgatóságunk az Utasításban lefektetett elvek mentén havi ellenőrzési tervet készít, amely napi bontásban tartalmazza a tárgyhónapra vonatkozó ellenőrzéseket, ezek között közúti és telephelyiek is szerepelnek. Az ellenőrzések hatékonyságának növelése érdekében negyedévenként tartunk régiós ellenőrzéseket is, amikor három-négy megye egyszerre hajt végre ellenőrzést és kifejezetten az ellenőrzés alól kibújni szándékozó és kerülő utakat igénybevevő gépjárművek ellenőrzés alá vonása a célunk.

Ezen túlmenően az ellenőrzések komplexebbé tétele érdekében – melynek fontosságát és hazai szükségességét már 2004-ben tartalmazta egy publikáció[13] – részt veszünk a társszervezetek által tartott autópálya kiterelések, nemzetközi akciókban, ahol a Vám- és Pénzügyőrség, Nemzeti Közlekedési Hatóság, Megyei Rendőr-főkapitányság munkatársaival közösen hajtunk végre ellenőrzést. Az OKF vonatkozó Utasítása értelmében az ellenőrzést minimum kettő fő hajtja végre, melyből az egyik személynek rendelkeznie kell OKJ-s ADR ügyintézői végzettséggel. Az ellenőrzések végrehajtásához igazgatóságunkon – az országban elsőként – 2009-ben rendszerbe állítottunk egy Peugeot Boxer típusú gépjárművet (1. sz. kép), melyet „mozgó irodának” alakítottunk ki és minden olyan eszközzel felszereltük, mely az ellenőrzés szakszerű és komfortos végrehajtásához szükséges. Felszereltük: önálló áramforrással, lap toppal, multifunkciós színes nyomtatóval, fényképezőgéppel, a gépjárművek szabályos megállításához szükséges felszerelésekkel, láthatósági jelzésekkel ellátott ruházattal, mintavevő készlettel, hogy csak a legfontosabbakat emeljem ki.

[12] 1/2002. (I. 11.) Korm. rendelet a veszélyes áruk közúti szállításának ellenőrzésére vonatkozó egységes eljárásról
[13] Norbert Körmendy, László Földi: Current issues of the transportation of dangerous goods by road, from the aspect of disaster management, with special emphasis to the accession of Hungary to the European Union, AARMS Academic and Applied Research in Military Science Vol.3 Issue 3. (2004) Budapest p. 427-436. ISSN 1588 8789 (peerreviewed) URL cím: http://www.zmne.hu/aarms/index.htm



1. sz. kép. ADR ellenőrzésre használt gépjármű, Készítette Bárdos Zoltán 2010. Forrás[14]

A különböző veszélyes áruk közúti szállítása során balesetek is bekövetkezhetnek (2. sz. kép), melyek következményeinek a felszámolása az elsődleges beavatkozók – hivatásos és önkéntes tűzoltóságok – feladata. A veszélyes anyagot szállító járművek káreseteinek felszámolásához szükséges speciális felszerelések nem minden tűzoltóságon találhatóak meg. A kárfelszámolások biztonságos és hatékony végrehajtásának céljából, az országban hét műszaki mentőbázis került kialakításra, ahol vegyi és műszaki mentőkonténerek találhatóak. A veszélyes árut szállító gépjárművek baleseténél a kiérkező tűzoltók egyik legfontosabb feladata, a szállított veszélyes anyag beazonosítása. Sajnos ez nem minden esetben könnyű feladat, hiszen a veszélyességi bárcák sérülhetnek, az UN számok és veszélyt jelző számok leeshetnek, a fuvarokmányok megsemmisülhetnek. Ezekben az esetekben a beavatkozások megkezdése előtt szükséges a baleset során sérült rakományra, szállított anyag tulajdonságaira vonatkozó információkat szerezni. Ez megvalósulhat, egyrészt a Veszélyhelyzeti Felderítő Csoportok (VFCS, Budapesten VFSZ) helyszínre rendelésével, a VFCS személyzete kéziműszerekkel, vagy akciós szettel tudja beazonosítani a szabadba került anyagokat. Az EU-ban már 1991-ben létrehoztak a veszélyes anyagok baleseteinek egységes kezelésére egy veszélyhelyzet kezelő rendszert (ICE). A rendszerben a vegyipari cégek önként segítséget nyújtanak a hatóságoknak a veszélyes anyagok szállítási baleseteinél.[8] Hazánkban a Magyar Vegyipari Szövetség (MAVESZ) 1998. március 4-től működteti a Vegyipari Riasztási és Információs Központot (VERIK). Az információs és segítségnyújtó rendszer része az európai elhárító (ICE) szervezetnek, fõ feladatuk segítséget nyújtani veszélyes anyagok szállítási baleseteinél. A VERIK rendszer működésének 3 fokozata van:

1. fokozat: azonnali tanácsadás telefonon vagy faxon,
2. fokozat: tanácsadás a baleset helyszínén,
3. fokozat: műszaki segítségnyújtás a helyszínen.

A központ szolgáltatása a nap 24 órájában elérhető, hazánkban hét VERIK központ található, melyek bázisai nagy vegyipari cégek, ez a szolgáltatás szervesen kielégíti az elemi katasztrófa-megelõzés és elhárítás rendszerét, valamint nagyban segíti az elsődleges beavatkozókat a veszélyes anyagok azonosításában.

[14] Fejér Megyei Katasztrófavédelmi Igazgatóság



2. sz. kép. Festéket és segédanyagokat szállító gépjármű balesete az M1-es autópályán
Készítette: Bárdos Zoltán, Forrás[15]

Jelentős előrelépést jelentene a veszélyes áruk szállításának biztonságosabbá tételében, ha hazánkban is megvalósulna a veszélyes anyagot szállító járművek nyomon követésére a – más országokban már működő és bevált – **GPS** nyomkövető jelzőrendszer. Ezen rendszer segítségével folyamatosan ellenőrizhetővé válna az útvonal betartás fegyelme, az előírt pihenők és ellenőrzések megtartása. Folyamatos naprakész információ állna rendelkezésre az ország területén lévő veszélyes anyagok mennyiségéről, és területi eloszlásáról. Könnyebben megtervezhetővé és szervezhetővé válna a kárelhárítás és kárfelszámolás, tervezhetőbbé válna az ellenőrzés. [5]

Összegzés

A veszélyes anyagokkal kapcsolatos tevékenység speciális területét jelenti a veszélyes áruk fuvarozása. Ez a veszélyforrás mobilitása miatt a fuvarozókat, a hatóságokat, valamint a mentőerőket is nehéz feladat elé állítja. A megelőzés szabályai adottak, az ADR betartására vonatkozó ellenőrzési rendszert a katasztrófavédelem szervezete az elmúlt években kialakította, melynek tökéletesítése folyamatos. A jogszabályok adta lehetőségek keretein belül a szabálytalanságoktól való visszatartáshoz a szükséges szankcionálási lehetőségek adottak[16]. Az elkövetkező tíz évben a hazai szénhidrogén kitermelés mennyisége folyamatosan csökkeni fog, ugyanakkor a vegyipari termelés mértéke folyamatosan növekszik. A vegyipar nyersanyag igényét veszélyes anyagok közúti szállításával lehet csak biztosítani az országon belül és külföldről hazánkba, valamint tranzitként az országon keresztül (Nyugat-és Kelet Európa között) történő szállítással. Az úthálózat szerkezete, átbocsátó képessége és minősége várhatóan csak lassan változik, így sajnos növekszik a közutak veszélyes anyaggal történő terhelése, ami több baleset és katasztrófa bekövetkezésének lehetőségét jelenti. [6]

Jövőbeni feladata a katasztrófavédelem szervezetének – ezen belül katasztrófavédelmi igazgatóságunknak –, hogy az ADR ellenőrzések hatékonyságának fenntartásával – a közlekedésben résztvevők és a településeken lakók biztonságának érdekében – a veszélyes áruk szállításával foglalkozó gazdálkodók szállítási fegyelmét növeljük. Ebbe beletartozik az áruk szállításra történő előkészítésének, a berakásnak, a szállítási szabályoknak, az előírt

[15] Fejér Megyei Katasztrófavédelmi Igazgatóság

[16] 156/2009. (VII. 29.) Korm. rendelet a közúti árufuvarozáshoz, személyszállításhoz és a közúti közlekedéshez kapcsolódó egyes rendelkezések megsértése esetén kiszabható bírságok összegéről, valamint a bírságolással összefüggő hatósági feladatokról

felszereléseknek, a fuvarokmányoknak az ellenőrzése. Célunk természetesen nem a büntetések miden, áron való kiszabása, hanem a biztonságos szállítási feltételek jogszabályokban foglaltak szerinti megvalósulásának biztosítása. Igazgatóságunkon 2009. januárjától az országban elsőként került létrehozásra, egy hatósági alosztály melynek fő feladata az ADR ellenőrzések végrehajtása és a kapcsolódó hatósági feladatok végzése. Az elmúlt közel másfél év tapasztalata alapján elmondhatjuk, hogy a feladatrendszer ilyen módon való kialakítása beváltotta a hozzá fűzött reményeket, az ADR feladatot végrehajtása országos szinten is elismerést váltott ki. A jövőben a várhatóan növekvő számú veszélyes áru szállítás az elkövetkező években folyamatos feladatot fog adni a katasztrófavédelem szervezete számára, úgy látom, hogy munkatársaink szakmai felkészültsége és hozzáértése alapján a kihívásoknak meg tudunk felelni. Az ellenőrzések szakszerű végrehajtásával kívánjuk elérni, hogy a veszélyes áru szállítmányok számának emelkedésével nem növekedjen a közlekedők és a lakosság veszélyeztetése.

Felhasznált irodalom

[1] Dr. Hesz József: Veszélyes anyag fogalma és a velük kapcsolatos rendkívüli események elhárítása http://www.vedelem.hu/letoltes/tanulmany/tan244.pdf letöltés ideje: 2010. 05. 22.

[2] 44/2000. (XII. 27.) EüM rendelet a veszélyes anyagokkal és a veszélyes készítményekkel kapcsolatos egyes eljárások, illetve tevékenységek részletes szabályairól

[3] Sárosi György Hungária Veszélyesáru Mérnöki Iroda Kft: Veszélyes anyagot szállító járművek www.minipolice.hu/kiserlet/panel/nyomtat/ny_veszely.htm letöltés ideje: 2010. 05. 22.

[4] Veszélyes áruk szállítása: Wikipedia http://hu.wikipedia.org/wiki/Vesz%C3%A9lyes_%C3%A1ruk_sz%C3%A1ll%C3%ADt%C3%A1sa letöltés ideje: 2010. 05. 20

[5] Nagy Lajos tűo. ezredes, Nagy Károly mk. őrnagy, Földi László mk. százados Veszélyes anyagok szállítása www.zmne.hu/tanszekek/vegyi/docs/fiatkut/veszagsz.htm letöltés ideje: 2010. 05. 20.

[6] Török Bálint Zoltán nyá. tű. alezredes: Veszélyes anyagok közúti szállítási balesetei során a tűzoltóság beavatkozásának taktikai és technikai fejlesztési lehetőségei Doktori (PhD) értekezés 2009. http://portal.zmne.hu/portal/page?_pageid=34,57843,34_59615&_dad=portal&_schema=PORTAL

[7] Norbert Körmendy, László Földi: Current issues of the transportation of dangerous goods by road, from the aspect of disaster management, with special emphasis to the accession of Hungary to the European Union, AARMS Academic and Applied Research in Military Science Vol.3 Issue 3. (2004) Budapest p. 427-436. ISSN 1588 8789 (peerreviewed) http://www.zmne.hu/aarms/index.htm letöltés ideje: 2010. 05. 24.

[8] Bálint Török, László Földi: Possible use of the *VERIK* system in disaster relief of road accidents during transportation of dangerous goods, AARMS Academic and Applied Research in Military Science Vol.6. Issue 4. (2007) Budapest p. 647-658. ISSN 1588 8789 (peer reviewed) http://www.zmne.hu/aarms/index.htm letöltés ideje: 2010. 05. 24.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Cimer Zsolt
zsolt.cimer@katasztrofavedelem.hu

Szakál Béla
Szakal.Bela@ymmfk.szie.hu

A VESZÉLYES ÁRU KÖZÚTI SZÁLLÍTÁSÁBÓL SZÁRMAZÓ KOCKÁZATOK MEGHATÁROZÁSÁNAK LEHETŐSÉGE

Absztrakt

A veszélyes áru közúti szállítás nagyon szigorú szabályokhoz kötött tevékenység, amelyek betartása nagymértékben hozzájárul az ebből származó kockázatok csökkentéséhez. Ugyanakkor egy hipotetikus, veszélyes áru baleset következményeinek elemzésével a szerző felhívja a figyelmet arra, hogy pusztán a vonatkozó jogszabály, az ADR betartása nem feltétlenül elégséges a veszélyes áru közúti szállításából származó kockázatok lakossági tolerálásához. Magyarországon jelenleg a veszélyes áru közúti szállításából származó kockázatok meghatározására nincs jogszabályi előírás, vagy belső nemzeti útmutató. A szerzők bemutatnak egy, a veszélyes áru közúti szállítására Hollandiában kidolgozott mennyiségi kockázatelemzési eljárást, és megvizsgálják annak hazai adaptálási feltételeit, lehetőségeit.

The road transport of dangerous goods is an activity bounded by severe regulations. Observing these regulations contributes to the reduction of risks. The author will analyse the consequences of a hipothetical accident of a transport of dangerous goods in order to call the attention to the fact, that only observing the legal and ADR regulations is not always enough to tolerate the risks of these operations. Currently in Hungary there are neither a legal regulation nor a national guide exist for the determination of these risks. The author presents a methode of quantitative risk analysis of the transport of dangerous goods originated from the Netherlands and examines the conditions and possibilities of its adaptation.

Kulcsszavak: *veszélyes áru szállítás, kockázatelemzés ~ road transport of dangerous goods, risk analysis*

BEVEZETÉS

Köztudott, hogy a világon az egyik legveszélyesebb üzem a közúti közlekedés, itt történik a legtöbb baleset és elhalálozás. A közúti közlekedés kockázata tovább növekszik, ha ehhez hozzászámítjuk a veszélyes áruk közúti szállítását is. A veszélyes áruk közúti szállításának veszélyei nemcsak Magyarországon, hanem az egész világon súlyos problémát jelentenek a lakosság és az esetleges balesetek felszámolásában résztvevő szervek számára. A gondot nemcsak a rakomány nem megfelelő előkészítése, a szállítmányok rögzítésének hiányosságai vagy a szállító fegyelmezetlensége okozza, hanem sok esetben a rakomány nem megfelelő okmányolása, a szállítmány tartalmára vonatkozó szándékos megtévesztés és a közúti közlekedési és szállítmányozási fegyelem megsértése. Természetesen ezen okokon kívül még számos létezik. [1] Éppen ezért a veszélyes áru közúti szállítást, mint tevékenységet az illetékes hatóságok szigorú jogi normához kötik. Ez a jogi norma az „European Agreement concerning the international carriage of dangerous goods by road" nemzetközi egyezmény, közismert néven az ADR, amely honosításával hazai jogszabállyá is vált.

Hazánkban az ADR betartásán túlmenően, korábban az illetékes hatóságokkal engedélyeztetni kellett az egyes, „nagyobb kockázatot" jelentő veszélyes áru tervezett közúti szállítási útvonalát „az egyes veszélyes árukat szállító közúti járművek útvonalának kijelöléséről" szóló 122/1989 (XII.5.) MT rendelet" előírásainak megfelelően. Amennyiben a szállítás egy település közigazgatási határán belül történt, akkor ezt a jegyző engedélyezte. Amennyiben a szállítás a fővárosban, illetőleg az egy megyén belüli települések között történt, akkor a területileg illetékes megyei, fővárosi közlekedési felügyelet volt az engedélyező. A több megyén keresztüli szállítás során, az országhatáron belépő forgalomban, illetve a pótlólagos útvonal kijelölésnél az Útgazdálkodási és Koordinációs Igazgatóság volt az engedélyező hatóság. A kockázatcsökkentés szempontjából a jogszabály rendkívül lényeges eleme volt, hogy a veszélyes szállítmányról és a tervezett útvonalról a beavatkozó szervek – tűzoltóság, polgári védelem – tájékoztatást kaptak, ugyanis az engedélyezési folyamatban a katasztrófavédelem szakhatóságként működött közre. A jogszabályt 2007-ban hatályon kívül helyezték.

A „kisebb kockázatot" jelentő veszélyes áru közúti szállítási útvonalát illetően a beavatkozó szervek korábban sem rendelkeztek semmilyen információval. A nyomon követés hiányára – mint a prevenció lehetséges eszközére – már a 2000. évben megjelent szakirodalom is felhívta a figyelmet: „Magyarország területén a veszélyes anyag szállítmányok útvonalának nyomon követésére a más országokban már működő és bevált GPS nyomkövető jelzőrendszer még nincs kiépítve, így közvetlen információval egy szállítmány be- vagy kilépéséről, a lefutott nyomvonalról, annak esetleges szándékos megváltoztatásáról nem rendelkezünk." [2] E területen napjainkig nem történt változás.

Időközben más megközelítésből ugyan, de hasonló céllal az ADR-ben is új elemként került megfogalmazásra, miszerint az ADR Szerződő Feleinek (így hazánknak is) az alagutakon való áthaladás tiltását és az alternatív útvonalakat jelzésekkel és táblákkal kell jelölni. Az alkalmazott jelek nemzetközi megértésének elősegítését a Bécsi Egyezményben szabályozták. A veszélyes árut szállító járművek közúti alagúton való áthaladását tiltó jeleket és jelzéseket olyan helyen kell kitenni, ahol még lehetőség van az alternatív útvonal választásának. [3] Tekintettel arra, hogy hazánkban a nemzetközi jogszabály hatályba lépésekor nem voltak a közúti közlekedésben alagutak, az előírást az illetékes hatóságoknak nem kellett érvényesíteniük. Hasonló, az ADR-ben rögzített szabály autópályákra, főútvonalakra, lakott területre nincs érvényben, ugyanakkor a Szerződő Feleknek azonban lehetősége van belső, nemzeti szabályzók kidolgozására és érvényesítésére.

Megítélésem szerint az ADR szerinti nagyon szigorú preventív előírások betartása a veszélyes áruk közúti szállításából származó kockázatokat jelentős mértékben csökkentik. Ugyanakkor e jogszabályi előírások betartása nem jelent egyértelműen elégséges feltételt a veszélyes áruk szállításából származó kockázatok lakossági szintű elfogadásához. A kockázatok tolerálhatóságának megítélésében a legnagyobb problémát az jelenti, hogy jelenleg Magyarországon nincs olyan jogi norma, amely kötelezné az illetékes hatóságokat a veszélyes áruk szállításából származó kockázatok felmérésére, és azoknak az előre deklarált elfogadhatósági kritériumokkal való összevetésére. Hiányzik továbbá a kockázatelemzés eredményeit alkalmazó belső nemzeti szabályzó, amely a hatósági szervek számára határozná meg, hogy a lakosság védelme érdekében mely területeken, és milyen feltételekkel szükséges korlátozni a veszélyes áru közúti szállítását.

1. A VESZÉLYES ÁRU SZÁLLÍTÁS ELLENŐRZÉSÉNEK TAPASZTALATAI

Ahhoz, hogy a megelőző intézkedések kockázatcsökkentő szerepüket be tudják tölteni, azaz jelen esetben az ADR egyre szigorúbb előírásai elérjék céljukat, azokat pontosan be kell tartani a tevékenységben résztvevőknek.

Az ADR előírásainak betartásáról célellenőrzésekkel lehet meggyőződni, amelyre a jelenlegi jogi szabályozás keretei között a rendőrség, a közlekedési hatóság, vám és pénzügyőrség, illetve a katasztrófavédelem kiképzett szakembereinek van hatásköre.

2007-ben az Országos Katasztrófavédelmi Főigazgatóság és területi szervei által ellenőrzött 2414 gépjármű közül 300-nál tártak fel a szakemberek hiányosságot. A magyar szállítók 13%-a, a külföldi szállítók 12%-a nem felelt meg valamilyen szempontból az előírásoknak. Az ellenőrzést végzők többféle problémából eredően, 585 hibát állapítottak meg, ami azt jelenti, hogy a hibák halmozottan jelentkeztek.

2008-ban katasztrófavédelem szakemberei 1120 alkalommal vettek részt közúti ellenőrzésen és 3254 veszélyes árut szállító gépjárművet ellenőriztek, 35%-kal többet, mint 2007-ben. A szakemberek az ellenőrzött 3254 gépjármű közül 367-nél tártak fel hiányosságot, a magyar szállítók 10%-a, a külföldi szállítók 1,2%-a nem felelt meg valamilyen szempontból az előírásoknak.

2009-ben a katasztrófavédelem szakemberei 1313 alkalommal vettek részt közúti ellenőrzésen, és 3665 veszélyes árut szállító gépjárművet ellenőriztek. Az ellenőrzött 3665 gépjármű közül 370-nél tártak fel a szakemberek hiányosságot, a magyar szállítók 9%-a, a külföldi szállítók 1,1%-a nem felelt meg valamilyen szempontból az előírásoknak.

A fenti adatokból egyértelműen látszik, hogy az elmúlt évekhez képest valamelyest csökkent a tapasztalt hiányosságok száma mind a belföldi, mind a külföldi szállítók körében. A 2009. évben tapasztaltak alapján – hasonlóan az előző évekhez – a legtöbb hiányosság a belföldi fuvarozást vállaló kisebb hazai vállalatok, illetve az Európai Unióból származó külföldi cégek gépjárműveinél fordult elő. Az előző évek tapasztalatához képest némileg változott a hibás szállítások aránya az EU-s és nem EU-s járművek között. Ez részben annak is köszönhető, hogy bővült az EU tagállamok száma, viszont ezzel együtt nem javult számottevően a szabálykövetés hajlandóság, a szállítói morál. A legtöbb hiba a fuvarokmányok nem megfelelő vezetése mellett, a tűzoltó készülékekkel, valamint a rakományrögzítéssel kapcsolatosan fordult elő. Kiemelten kezelendő az írásbeli utasítás hiánya, a járművek, illetve a küldeménydarabok nem szabályos jelölése, bárcázása, valamint

jelentős mértékű a személyi védőfelszerelések hiánya, érvényességi idejének lejárta, vagy a figyelmeztető jelzőeszközök működésképtelensége. [4, 5]

Az elmúlt évek célellenőrzései alapján megállapítható – részben az egyre növekvő bírságoknak köszönhetően -, hogy a veszélyes áru közúti szállítás szereplői egyre inkább betartják a vonatkozó előírásokat.

2. A VESZÉLYES ÁRU KÖZÚTI SZÁLLÍTÁSA SORÁN BEKÖVETKEZŐ BALESET LEHETSÉGES KÖVETKEZMÉNYEINEK ELEMZÉSE

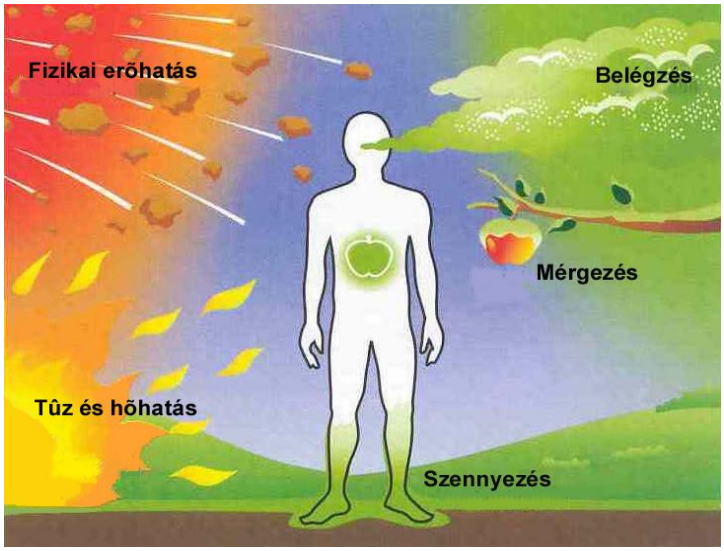
2.1 A veszélyes áru közúti szállítása során bekövetkező baleset lehetséges következményei általánosságban

A veszélyes árut szállító közúti jármű balesetének következményeit elemezve a hatások igen változatosak lehetnek: szerencsés esetben kizárólag a jármű sérül, a veszélyes áru csomagolása nem, így veszélyes anyag nem kerül a szabadba. Kevésbé szerencsés körülmények között a veszélyes áru csomagolása is megsérül, és veszélyes anyag kerül a szabadba.

A veszélyes anyagok szabadba kerüléséből származó következmények egyértelműen levezethetők a veszélyes áru tulajdonságaiból, miszerint az tűz- és robbanásveszélyes, maró, toxikus, ökotoxikus, karcinogén, radioaktív tulajdonságokkal rendelkezhet. Ezek alapján a veszélyes anyag szabadba kerülése során leggyakrabban az alábbi táblázatban bemutatott hatások következhetnek be:

HATÁS	KÖVETKEZMÉNYEK
Robbanás	Léglökési hullám, repeszhatás, valamint magas hőmérséklet.
Mérgezés	Mérgező anyagok kerülhetnek a szervezetbe belégzéssel vagy a bőrön keresztül.
Tűz	Hőhatás, amely égési sérüléseket okozhat.
Oxidáció	Az égés folyamatát felgyorsítja és égési sérüléseket okozhat.
Marás, irritálás	Savakkal és lúgokkal való érintkezés miatt a bőr, a szem és a nyálkahártya sérülhet.
Fagyás	Mélyhűtött folyadékok, nagy nyomás alatti gázok szabadba jutása fagyást okozhat.
Fertőzés	A szervezet megbetegedése.
Fulladás	Az égés, és az égéstermékek miatt oxigénhiányos állapot alakulhat ki.
A környezetet érő veszélyek	A víz, a talaj és a levegő szennyeződésének veszélye.

A veszélyes anyagok szabadba kerülésével járó közlekedési balesetek következményeit tekintve, alapvetően 4 hatással számolunk. Ezeket az alábbi ábra szemléltet: [6]



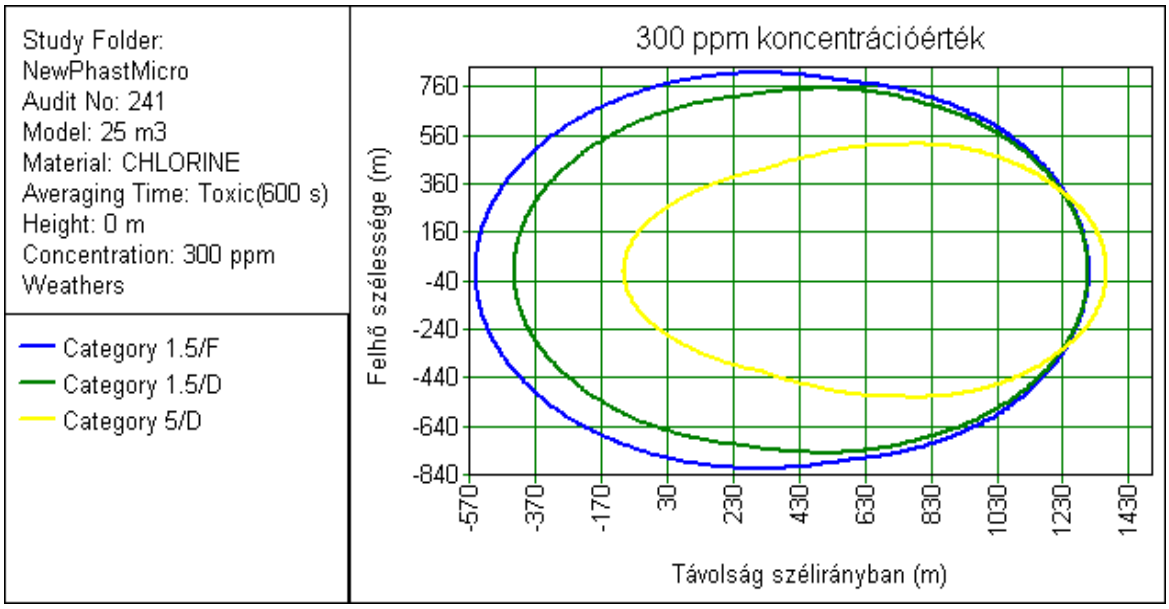
1. ábra. Az embert érő lehetséges hatások

2.2 Veszélyes anyag szabadba kerülésével járó feltételezett közlekedési baleset következményeinek elemzése

Veszélyes áruk szállításából adódó kockázatok, és következmények nagyon jól reprezentálhatók egy hipotetikus baleset következményeinek vizsgálatával.

A veszélyes áru szállítása során esetlegesen bekövetkező balesetben a veszélyes áru a szabadba kerülhet, melynek következményei szoftveresen modellezhetők. Az alábbiakban – a probléma komolyságát szemléltetve – egy klórt szállító tartány-kocsi balesetét modellezzük le a DNV Phast következményelemző szoftver segítségével. Input meteorológiai adatként az átlagos, hazánkra jellemző értékeket használjuk. A modellezés során két lehetséges eseménysort vizsgálunk meg:

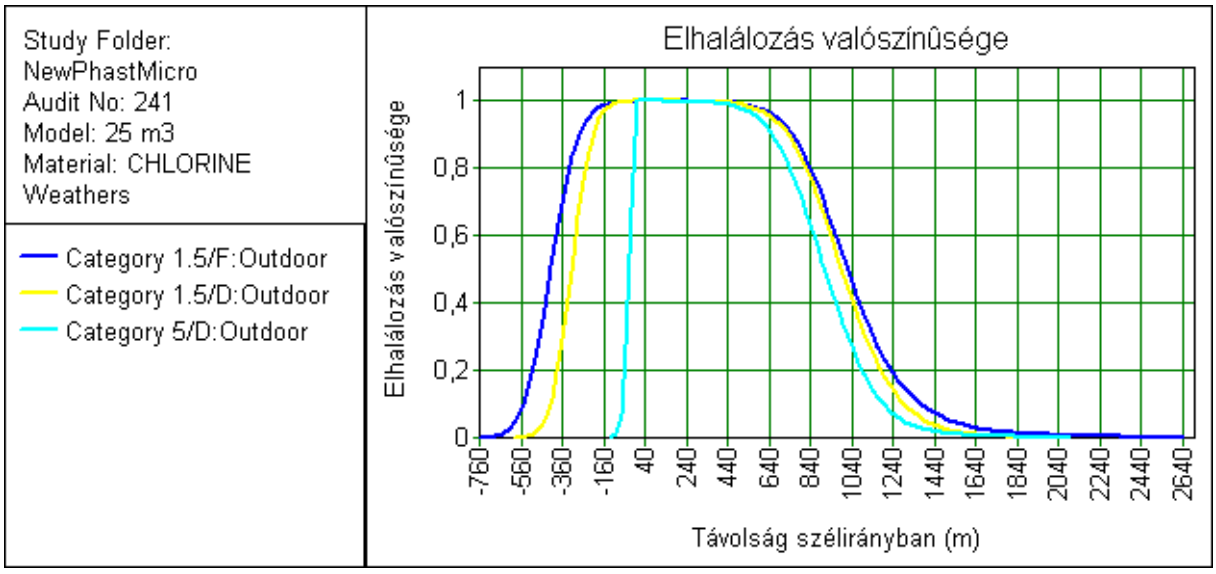
1. A tartány-kocsi katasztrofális törése következtében a veszélyes anyag pillanatszerűen a szabadba kerül és terjed. A biztonsági adatlap alapján ez az anyag 300 ppm koncentrációban – az egyént 1 órán keresztül kitéve ennek – szemirritációt, köhögést, légzési nehézséget, majd halált okoz. (Patkány LC_{50} = 293 ppm /1h) Az alábbi ábra bemutatja a 300 ppm koncentrációjú gázfelhő maximális kiterjedését a földfelszínen.



2. ábra. 300 ppm koncentrációjú gázfelhő kiterjedése

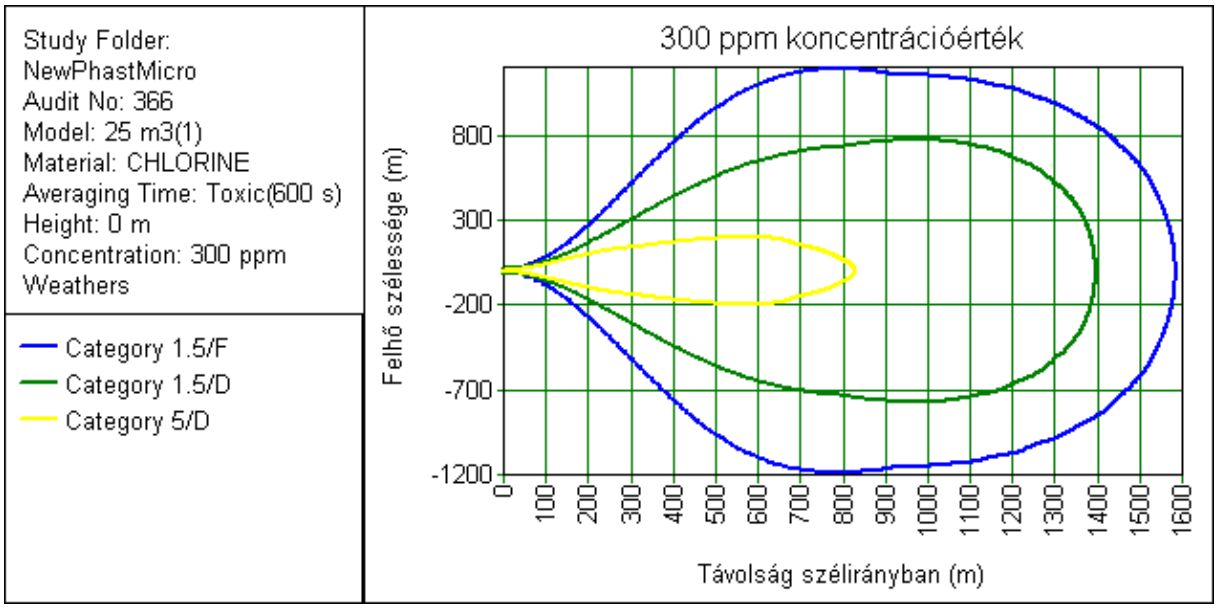
A fenti ábra alapján megállapítható, hogy szélirányban 1400 méteres távolságig alakulhat ki 300 ppm koncentrációérték.

A 2. ábra a szabadban tartózkodó személyek vonatkozásában mutatja be az elhalálozás valószínűségét a távolság függvényében. Az ábráról leolvasható, hogy amennyiben nem történik védelmi intézkedés, és a személyek szabadban tartózkodnak (nem zárkóznak el), akkor az esemény helyszínétől számított 1250 méteres övezeten belül az elhalálozás valószínűsége nagyobb, mint 20 %.



3. ábra. Elhalálozási valószínűség

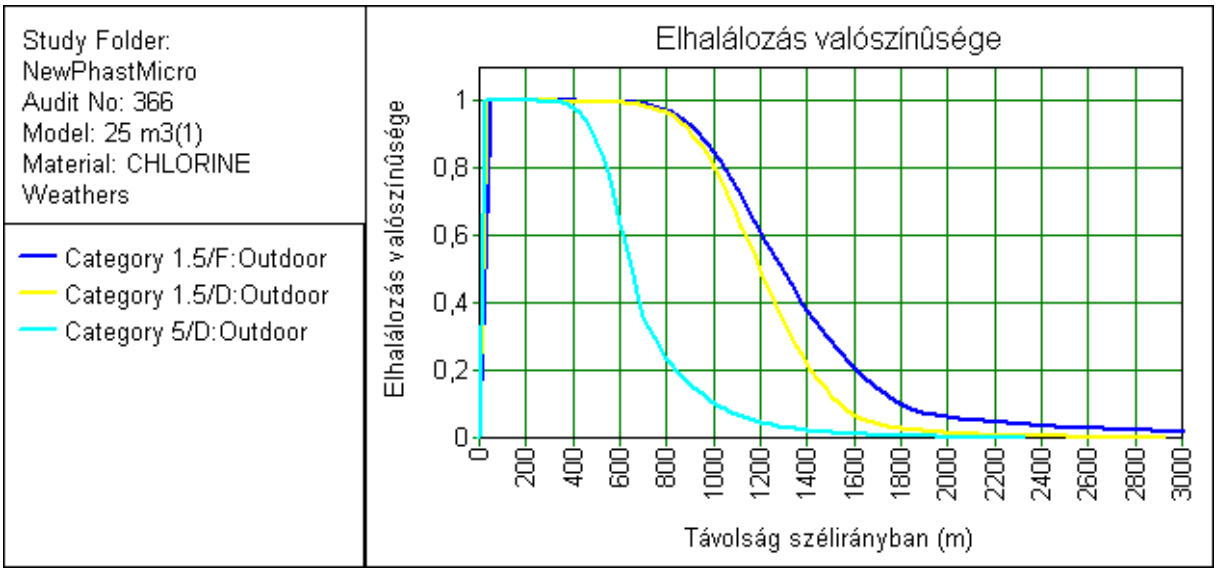
2. A tartány-kocsi sérülése következtében a klór kibocsátását folyamatosnak tekintjük, amely egy 50 mm ekvivalens átmérőjű lyukon keresztül történik. A 3. ábra mutatja be a 300 ppm koncentrációjú gázfelhő maximális kiterjedését a földfelszínen.



4. ábra. 300 ppm koncentrációjú gázfelhő kiterjedése

A fenti ábra alapján megállapítható, hogy szélirányban 1400 méteres távolságig alakulhat ki a 300 ppm koncentrációérték.

A 4. ábra – amely szintén a szabadban tartózkodó személyek esetén az esemény miatti elhalálozás valószínűségét mutatja be a távolság függvényében – alapján megállapítható, hogy amennyiben nem történik védelmi intézkedés, és a személyek szabadban tartózkodnak (nem zárkóznak el), akkor az esemény helyszínétől számított 1600 méteres övezeten belül az elhalálozás valószínűsége nagyobb, mint 20 %.



5. ábra. Elhalálozási valószínűség

A fent bemutatott példákból egyértelműen látszik az, hogy amennyiben a kárlehárítás nem megfelelő időben és hatékonysággal történik, továbbá a lakosság a szabadban tartózkodik, és a beavatkozók nem foganatosítanak megfelelő lakosságvédelmi intézkedéseket – például elzárkózás, kimenekítés – akkor a kárhelytől számított több száz méteren belül is elhalálozással számolhatunk.

Megítélésünk szerint a fenti példákban bemutatott következményeket a lakosság részéről nem tolerálható. Ugyanakkor e szállítás tiltása rendkívül súlyos gazdasági következményekkel járna, ezért fontos elérnünk azt, hogy a gazdaság és a lakosság érdekei közötti egyensúly megmaradjon. A lakosság részéről történő elfogadhatóságot a lehetséges súlyos következményeken túlmenően az is befolyásolja, hogy milyen gyakran történik ilyen veszélyes anyag szállítása a környezetükben. A tolerálhatóság feltételeként tehát a vizsgált útszakaszra jellemző veszélyes áru szállításból eredő kockázatot javasoljuk alkalmazni.

4. A VESZÉLYES ÁRU SZÁLLÍTÁS KOCKÁZATÁNAK ÉRTELMEZÉSE

A veszélyes áru közúti szállítás kockázatát a hazai jogszabályok nem értelmezik, gyakorlati útmutatók sem állnak rendelkezésre. Ezért – ha értelmezni szeretnénk a veszélyes árúk közúti szállításának a kockázatát – a hasonló területeken használatos módszerekből, normákból és kritériumokból célszerű kiindulni.

4.1 A veszélyes ipari üzem tevékenységéből származó kockázat [7, 8]

A veszélyes ipari üzemek részére „A veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről” szóló 18/2006. (I. 26.) Korm.rendelet írja elő a veszélyes anyagokkal kapcsolatos tevékenységük kockázatainak elemzését. A jelzett jogi norma szerint a veszélyes ipari üzemek tevékenységéből származó kockázatok meghatározására mennyiségi elemző-módszert kell alkalmazni. Ezek gyakorlati végrehajtására az Országos Katasztrófavédelmi Főigazgatóság, mint hatóság számos útmutatót tett közé az elmúlt években. A nálunk, az e célra legelfogadottabb mennyiségi kockázatelemzési módszereket Hollandiában dolgozták ki és vezették be. Ezek irodalmi hátttereként az un. „színes könyvek”[1] állnak rendelkezésre.

Az egyéni és társadalmi kockázatok elfogadhatóságának az a feltétele, hogy feleljenek meg 18/2006. (I. 26.) Korm.rendelet 5. mellékletében foglalt engedélyezési kritériumoknak. E szerint veszélyes ipari üzem tevékenysége csak abban az esetben engedélyezhető, - amennyiben lakóterület van a környezetében – ha a lakóterület olyan övezetben van, ahol veszélyes anyagokkal kapcsolatos súlyos baleset következtében történő halálozás egyéni kockázata nem éri el a 10^{-6} esemény/év értéket. Feltételekkel elfogadható szintű veszélyeztetettséget jelent, ha a lakóterületen a halálozás egyéni kockázata 10^{-6} esemény/év és 10^{-5} esemény/év között van. Ekkor a hatóság kötelezi az üzemeltetőt, hogy hozzon intézkedést a tevékenység kockázatának ésszerűen kivitelezhető mértékű csökkentésére, illetőleg olyan lakosságvédelmi intézkedések (riasztás, egyéni védelem, elzárkózás stb.) feltételeinek biztosítására, amelyek a kockázat szintjét csökkentik. Nem elfogadható szintű veszélyeztetettséget jelent, ha a lakóterületen a halálozás egyéni kockázata meghaladja a 10^{-5} esemény/év értéket. Ha a kockázat a településrendezési eljárás keretein belül nem csökkenthető, a hatóság kötelezi az üzemeltetőt a tevékenység korlátozására vagy megszüntetésére.

A társadalmi kockázat meghatározásakor nem csak a veszélyességi övezetben élő lakosságot, hanem az ott nagy számban időszakosan tartózkodó embereket (például munkahelyen, bevásárlóközpontban, iskolában, szórakoztató intézményben stb.) is figyelembe kell venni. A társadalmi kockázat feltétel nélkül elfogadható, ha $F<(10^{-5}xN^{-2})$ 1/év, ahol

[1] Methods for the calculation of physical effects („Yellow Book”), Hága, 1997
Methods for the determination of possible damage, („Green Book”), Hága, 1992
Methods for determining and processing probabilities („Red Book”), Hága, 1997
Guidelines for quantitative risk assesment („Purple Book”), Hága, 1999

N>=1. A társadalmi kockázat feltétellel fogadható el, ha minden F<(10^{-3}xN^{-2}) 1/év, és F>(10^{-5}xN^{-2}) 1/év tartomány közé esik, ahol N>=1. Ebben az esetben a tevékenység kockázatának csökkentése érdekében a hatóság kötelezi az üzemeltetőt, hogy gondoskodjon olyan üzemen belüli megelőző biztonsági intézkedésekről (riasztás, egyéni védelem, elzárkózás stb.), amelyek a kockázat szintjét csökkentik. Nem elfogadható szintű a veszélyeztetettség, ha F>(10^{-3}xN^{-2}) 1/év, ahol N>=1. Ebben az esetben, ha a kockázat más eszközökkel nem csökkenthető, a hatóság kötelezi az üzemeltetőt a tevékenység korlátozására vagy megszüntetésére.

4.1 A veszélyes áru közúti szállítás kockázatának meghatározása [9]

Hollandiában – hasonlóan a veszélyes ipari üzem tevékenységéből származó kockázatok meghatározására – a veszélyes áru szállítás kockázatelemzésére is dolgoztak ki eljárást. A veszélyes áru közúti szállításából származó kockázatok meghatározásának elméleti megfontolásai az alábbiak [10]:

Annak megítéléséhez, hogy a veszélyes anyagok egy meghatározott útvonalon történő szállításának kockázata megfelel-e a biztonsági kritériumoknak, mind az egyéni, mind a társadalmi kockázatot értékelni kell. Az egyes útszakaszok kockázata az alábbi három, egyre részletesebb módszer alkalmazásával értelmezhető:

1. Az éves szállítási gyakoriságok és a küszöbértékek összehasonlításával a kockázati szintek gyorsan áttekinthetők. Ha a szállítások éves gyakorisága egy útvonalon kisebb, mint a küszöbérték, nem szükséges a kockázatok mennyiségi meghatározása. Ha a szállítások éves gyakorisága meghaladja a küszöbértéket, vagy a küszöbértékek nem alkalmazhatók az adott helyzetre, akkor el kell végezni a kockázatok mennyiségi meghatározását. Az alábbi táblázatban bemutatok néhány példát a 10^{-6} egyéni kockázat túllépéséhez szükséges küszöbértékekre, propángáz szállítása esetén.

Út	Küszöbérték propángázra (szállítás/év)
autópálya	6500
lakott területen kívül	2300
lakott területen belül	8000

2. A kockázat viszonylag egyszerűen határozható meg az „Inter Province Committee for Risk Calculation Methodology” (IPORBM) szoftveres programjával, amelyet az AVIV Adviserend Ingenious szakemberei fejlesztettek ki. IPORBM szoftveres számításhoz az alábbi input adatokra van szükség:

   - a veszélyes áru osztálya, besorolása, tömege,
   - a vizsgált útszakasz típusa,
   - hossza,
   - a környezetben élő népesség adatai,
   - milyen gyakran szabadul ki veszélyes anyag az adott szállítóeszközökből,
   - az ott élő népességből mekkora az ott tartózkodók részaránya,
   - a gyújtás valószínűsége éghető gáz (gőz) terjedése esetén.

   Az IPORBM szoftver a veszélyes áru szállításából származó veszélyeztetettséget az egyéni és a társadalmi kockázat szempontjából minősíti. Bár az IPORBM általában

megfelelő pontosságú eredményeket produkál, bizonyos esetekben azonban még ennél is pontosabb és részletesebb kockázatszámításra van szükség.

3. Részletes mennyiségi kockázatbecslés. Amennyiben a fentiekben bemutatott két módszer nem vezet a várt eredményre, vagy az illetékes hatóság ezt nem tartja elfogadhatónak, akkor részletes mennyiségi kockázatelemzést kell elvégezni.

   Egy adott szállítási útvonalra vonatkozó számszerű kockázatbecslés elvégzéséhez szükséges alapadatok a következők:

   - a szállítási forgalom (évenkénti szállítóegységek száma anyagonként vagy anyag kategóriánként napszakok (nappali és éjszakai) szerint),
   - a szállítóegységek leírása (jellemző kapacitása),
   - a szállítási útvonal leírása (az út típusa, jelenlévő akadályok),
   - a balesetek számának és a forgalom mértékének leírása a baleseti gyakoriságok meghatározásához,
   - a gyújtóforrások felmérése,
   - a szállított (jellemző) anyagok tulajdonságai,
   - a szállítási útvonal környezetében lévő környezet értékelése,
   - meteorológiai adatok,
   - a vizsgált útvonal környezetében található népességi adatok.

   A veszélyes anyagok közúton történő szállításának kockázatát nagyban meghatározza a szállítmány mennyisége. A számszerű kockázatbecslés (QRA) során aszerint kell különbséget tenni a gyúlékony és mérgező anyagok (folyadékok és gázok) között, hogy atmoszférikus vagy túlnyomásos szállítóegységben történik-e a szállításuk (tartálykocsik és tartályok).

   A módszer kidolgozásakor azonosításra kerültek azok az eseménysorok, melyeket figyelembe kell venni a mennyiségi kockázatelemzés során, így:

   atmoszférikus tartálykocsik és tartályok esetében:

   - a teljes tartalom kibocsátásra kerül;
   - a tartály tartalmából 5 m^3 kerül kibocsátásra;
   - a tartály tartalmából 0,5 m^3 kerül kibocsátásra.

   túlnyomásos tartálykocsik és tartályok esetében:

   - a szállítóegység teljes tartalmának kibocsátása pillanatszerűen történik;
   - folyamatos kibocsátás egy 50 mm (2 coll) tényleges átmérőjű lyukon keresztül.

Hollandiában az útadatokat, a forgalmat és a gépjárművek baleseteit az illetékes hatóságok nyilvántartják, és adatbázisba rendezik. Az adatbázisokból a veszélyes áru közúti szállítással kapcsolatos balesetek átlagos gyakoriságát meghatározták több úttípusra. Figyelembe vették a különböző egyedi problámát is, mint például alagútban való áthaladás. Így meghatározták az autópályák, a lakott területen kívüli másodrendű és harmadrendű utak, valamint a lakott területen belüli főbb útvonalak gyakorisági adatait. Például:

Út típusa	**Kiömlési gyakoriság (/jármű x km)**	
	Túlnyomásos	**Atmoszférikus**
Autópálya	4.32×10^{-9}	8.38×10^{-9}
Lakott területen kívüli	1.22×10^{-8}	2.77×10^{-8}
Lakott területen belüli	3.54×10^{-9}	1.24×10^{-8}

A számítások végeredménye az adott útszakaszok vonatkozásában a halálozás egyéni kockázata és a társadalmi kockázata. Ezeket az engedélyezési kritériumokkal kell összevetni.

A fentiekben bemutatott kockázatelemzési módszer alkalmas a veszélyes áru közúti szállítás kockázatainak meghatározására, így a lakossági tolerálhatóság megítélésére is. Természetesen ahhoz, hogy e módszer Magyarországon is bevezetésre és alkalmazásra kerüljön, számos előfeltételnek kellene teljesülni. Ezek egyrészt kiterjednek a jogszabályi rendszer kidolgozására, beleértve a kockázatok elfogadhatósági kritériumrendszerének meghatározását is, másrészt a közúti közlekedéssel kapcsolatos – elsősorban veszélyes áru közúti szállítás – adatok gyűjtésére, adatbázisok készítésére.

ÖSSZEGZÉS - KONKLÚZIÓ

A veszélyes áruk közúti szállítása nagyon szigorú szabályokhoz kötött tevékenység, amely szabályok betartása nagymértékben hozzájárul az ebből származó kockázatok csökkentéséhez. Ugyanakkor az illetékes hatóságok célzott ellenőrzései azt mutatják, hogy az előírásokat nem minden szállító tartja be maradéktalanul, így a kockázatcsökkentő hatás sem feltétlenül teljesül.

Egy hipotetikus veszélyes áru közúti szállítás baleset következményeinek elemzésével szemléltettem azt, hogy az esetleges hatások rendkívül súlyosak lehetnek. Amennyiben a baleset lakott területen történik, és nem kellően hatékony a beavatkozás, akár több ezer ember halálához is vezethet. Ugyanakkor megállapítottuk azt is, hogy csupán a lehetséges következmények elemzése nem elégséges a lakosság veszélyeztetettségének megítéléséhez. Annak érdekében, hogy a gazdasági és a lakossági érdekek közötti egyensúly megmaradjon a tolerálhatóság megítélésénél a következményeken túl, figyelembe kell venni a vizsgált útszakaszon bekövetkezett ilyen típusú balesetek bekövetkezési gyakoriságát is. A tolerálhatóság feltételeként tehát a vizsgált útszakaszra jellemző veszélyes áru szállításból eredő kockázatot kell alkalmazni.

Magyarországon jelenleg a veszélyes áru közúti szállításából származó kockázatok meghatározására nincs jogszabályi előírás, belső módszertani útmutató. Az itt bemutatott, Hollandiában kidolgozott kockázatelemzési eljárás, megítélésem szerint alkalmazható a hazai viszonyokra is, de adaptálásának számos feltétele van. Többek között ilyen feltétel a jogszabályi normák kidolgozása, a hazai elfogadhatósági kritériumrendszer meghatározása, illetve a közúti közlekedéssel kapcsolatos – elsősorban veszélyes áru közúti szállítás – adatok gyűjtése, adatbázisok készítése.

A „holland” módszer alkalmazásával tudományosan megalapozottan határozható meg a veszélyes áru közúti szállításából eredő kockázat, amely alapján eldönthető, hogy az egyes útszakaszokon – akár lakott területen belül is – a tevékenység folytatása tolerálható szintű veszélyeztetettséget jelent-e, vagy az illetékes hatóságoknak kockázatcsökkentő intézkedést kell-e érvényesíteni (például csak éjjel lehet szállítani), esetleg a szállítás tiltását kell elrendelni.

HIVATKOZOTT IRODALOM

[1] Nagy L., Nagy K., Földi L.: Veszélyes anyagok szállítása, http://www.zmne.hu/tanszekek/vegyi/docs/fiatkut/veszagsz.htm, (letöltés: 2010.május 20.)

[2] Nagy L., Földi L: Kárelhárítás komplex feladatai, veszélyes áruk közúti szállítása során bekövetkezett baleseteknél, http://www.zmne.hu/tanszekek/vegyi/docs/fiatkut/FL_0106_karelh.htm, (letöltés: 2010.május 20.)

[3] Sárosi Gy.: Veszélyes áruk szállítása – ADR 2009. http://www.mkfe.hu/dokumentumok/pdf/sarosi_gyorgy_adr_2009.pdf (letöltés: 2010.május 20.)

[4] Dr. Vass Gy.: Veszélyes áruk közúti szállításának ellenőrzése 2008-ban, www.vedelem.hu/letoltes/szamtukor/szam34.pdf (letöltés: 2010. május 20.)

[5] Dr. Hoffmann I.: A 2009. évi katasztrófavédelmi ADR ellenőrzések és bírságolások végrehajtásának tapasztalatai, http://www.vedelem.hu/letoltes/tanulmany/tan247.pdf (letöltés: 2010. május 20.)

[6] Bíróné, Bojti I., Cimer Zs., Damjanovich I., Hoffmann I., Kátai-Urbán L., Mógor J., Dr. Szakál B., Vass Gy.: Módszertani segédlet a veszélyes anyagokkal kapcsolatos súlyos ipari balesetek elleni védekezés területi és helyi feladatainak ellátásához, Közép- és Kelet Európai Környezetfejlesztési Intézet, Budapest, 2005. http://www.vedelem.hu/letoltes/jegyzet/jegy18.pdf (letöltés: 2010.május 20.)

[7] Solymosi J.- Szakál B.- Tatár A. – Lévai Z: A súlyos balesetek megelőzéséért, Katasztrófavédelmi Szemle, 2001. II. szám 1-31. oldal

[8] Cimer Zs., Cseh G., Deák Gy., Gyenes Zs., Hoffmann I., Kátai-Urbán L., Dr. Solymosi J., Dr. Szakál B., Vass Gy.: Ipari biztonsági kockázatkezelési kézikönyv a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezés szabályozás alkalmazásához, KJK-KERSZÖV kiadványa, Budapest 2004.

[9] Cimer Zs., Dr. Szakál Béla: Risks of the road transport of dangerous goods, Konferencia so zahranicou ucast'ou, 2009.09.30 – 2009.10.01. Nyitra (ISBN 978-8085418-67-5, EAN 9788085418675)

[10] Michel Nicolet – Monnier, Adrian V. Gheorghe: Quantitative risk assessment of hazardous materials transport systems, 1996.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Giczi István
istvangiczi@gmail.com

VÍZELLÁTÁS KATASZTRÓFA HELYZETBEN

Absztrakt

Az ivóvíz ellátás rendkívüli helyzetekben különleges feladatot jelent. Rendkívüli helyzetek lehetnek a természeti- és emberi katasztrófák által előidézett állapotok, amikor a vízi-közművek nem tudják a lakosságot a hálózatukon keresztül egészséges ivóvízzel ellátni. Napjainkban, amikor a bioterrorizmus és a nukleáris technológia valóságos veszélyforrássá vált, a vízbe kerülő szennyező anyagok eltávolítása és az ivóvíz minőségének megőrzése hatalmas feladatot jelent a szolgáltató számára. A globális felmelegedés és a klimatikus viszonyok erőteljes megváltozása gyakori árvízzel, belvízzel fenyegeti a vízbásisokat és magukat a vízi-közmű létesítményeket is. Ezekben a helyzetekben is biztosítani kell a szolgáltatónak a lakosság ellátását ivóvízzel.

The supply of drinking water in emergency situations, is a special task. Emergency situations may be of natural disasters and human-induced conditions, where the water utilities are not able to provide healthy drinking water to the public using their pipelines. Today when the bioterrorism and nuclear technology has become a real threat, removal of pollutants into the water and preserve of the drinking water quality are huge tasks for the waterworks. Global warming and the stronge change of climatics threat water basis and themselves of water-utility facilities with frequently flood and inland inundation. In these situations, the provider should also ensure the public drinking water supplies.

Kulcsszavak: *vízművek, közművek, fenyegetettség, vízbázis, vészhelyzet, szennyezés, szűrés ~ waterworks, public utilities, threat, water basis, emergency, contamination, filtration*

Bevezetés

A modern városi és vidéki ivóvíz-ellátó rendszerek az ivóvizet hagyományosan nagy kiterjedésű csőhálózaton keresztül juttatják el a fogyasztókhoz. Szinte mindenhol a világon ezen a módon szolgáltatják a vizet a vízmű vállalatok. A központosított működésű vízhálózatok előnye normál körülmények között nyilvánvaló. A víztermelés, a kezelés, vízminőség ellenőrzés és elosztás a fogyasztókhoz – a vízi-közművek és a hatóságok feladata. Azonban a vízellátás központosított létesítményei (Alexander, 1993) is ki vannak téve a természeti katasztrófák és emberi katasztrófák – mint a terrorizmus és háborúk – romboló hatásainak. A San Fransiscot 1906-ban a Richter skála szerinti 8,3-es erősségű földrengés hatalmas pusztítást vitt végbe nem csak az épületekben, hanem a város ivóvízhálózatában is. (Harris, 1997; Putnam, 2000; Bruins, 2000).

A vízvezeték hálózat nagyon sok helyen megrongálódott. A földrengés következtében fellépő tüzek oltását nagyban gátolta, hogy a tűzoltók nem tudtak megfelelő mennyiségű oltóvízhez jutni a vezetékek sérülése miatt. Az iszonyú tűzvészben a város nagy része megsemmisült. (Dror, 1986; Rosenthal és Kouzmin, 1993).

Az előre nem látható veszélyek bekövetkezése esetére tervezett intézkedések létfontosságúak a városi közösségek számára. A váratlanul bekövetkező földrengés következménye tűzvész és számos más havaria helyzet alakulhat ki. (Rosenthal és mások., 1989).

A koordinált, több helyszínen elkövetett terrortámadások . mint a New Yorki Ikertornyok és Washington DC-ben a Pentagon ellen elkövetett terrortámadások hasonló következményekkel jártak.

A terroristák által megtervezett katasztrófa és az 1941. december 7-én Pearl Harbor ellen intézett japán támadás váratlansága között párhuzam húzható. Mindkettő kiszámíthatatlanságával és következményeivel sötét árnyként borul a jövőre. A nukleáris és biológiai terror veszélye aktualitássá vált napjainkban. (Foxell, 1997)

A nemzetközi politikai környezet egyre távolabb kerül a stabilitástól és egyre nő az atomfegyvert birtokló országok és szervezetek száma. Pakisztán, mint az első iszlám ország 1998-ban atomhatalommá vált és az atomfegyverrel rendelkező India szomszédjaként feszültség-gócot jelent Ázsiának ezen a részén. 2003 áprilisában Észak-Korea jelentette be, (Niksch, 2003).hogy az ország nukleáris fegyverekkel rendelkezik. A legutóbbi hónapok híreiben pedig Iránról olvasható, hogy tömegpusztító atomfegyver kifejlesztésén dolgozik.

A jövőbeli terrorista akciók, nukleáris balesetek és háborús szituációk kiszámíthatatlan hatású szennyezést okozhatnak az emberi környezetben – beleértve az ivóvízforrásokat is. A tiszta csapvíz az emberi élet alapfeltétele – mind normál mind pedig katasztrófa helyzetben. A vízellátó rendszereket valamennyi állam a kritikus infrastruktúrák közé sorolja. Ezek a rendszerek rendkívüli mértékben sebezhetőek a szabotázs cselekményekkel, bombatámadásokkal. (Clark és Deininger, 2000; Bruins, 2000)

Ezért létfontosságú azoknak a terveknek és proaktív feladatoknak az elkészítése, leírása – amelyek a természeti és emberi katasztrófák következményeként bekövetkező helyzetekben biztosítani tudják az ivóvízellátás folytonosságát. Ebben a cikkben a rendkívüli helyzetekben történő ivóvízellátást biztosító intézkedéseket próbálom bemutatni a szakmai források és tapasztalataim segítségével. A megközelítés a számos jövőbeli szcenárió miatt általános jellegű, de megemlítem a víztermelés monitoring rendszerei és az alkalmazható víztisztító rendszerek/módszerek szerepének jelentőségét, a proaktív tervezés szükségességét mind az állami szervezetek, vízi közművek és az állampolgárok szemszögéből.

Az atom-korszak születése és a II. világháború – Hiroshima és Nagaszaki

Henri Becquerel 1986-os felfedezése, amelyben bebizonyította, hogy a uránium ércből kilépő sugárzás áthatol az anyagon – hatalmas történelmi jelentőségű volt, amellyel az emberiség az atom-korszakba lépett. Ezt a speciális tulajdonságot nevezte aztán Marie Curie radioaktivitásnak. Ő és lánya, Irene az évek során a testüket ért akkumulálódott radioaktív sugárzásba belehaltak. (Schubert és Lapp, 1957).
James Chadwick 1932-ben felfedezte a neutront és ezzel az atom hatalmas energia-viszonyait keresők kezébe adta a tudás kulcsát. Két német fizikus Otto Hahn és Friedrich Strassmann, 1938-ban felfedezték, hogy a neutron segítségével uránium maghasadást lehet előidézni, amelynek során energia szabadul fel. Nagy nyugtalanságot okozott, hogy a náci Németország elsőként fejlesztheti ki az atombombát. Az Egyesült Államok és Nagy Britannia közösen indították el 1942 augusztusában a Manhattan tervet. Először önfenntartó láncreakciót tudtak generálni uránium és grafit segítségével. (Barnaby, 1971).
Az atomenergia felhasználásának lehetősége új távlatokat nyitott a hadviselés és fegyvergyártás történetében. A világon elsőként hajtottak végre kísérleti atomrobbantást 1945. július 16-án az új-mexikói Alamogordo sivatagban. Három héttel később az új fegyvert bevetették Japán ellen. 1945. augusztus 6-án, kora reggel Hirosima lakóinak valószínűleg fogalma sem lehetett arról, hogy városuk ellen egy teljesen új, félelmetesen nagy energiájú fegyvert vetettek be. Hatalmas – a nap fényénél 600-szor erősebb - fényvillanást észleltek és Hirosima központjában a 15000 tonna TNT-nek megfelelő erejű atombomba robbant 580 m magasságban. A radioaktivitás erőssége 100000 rad volt. A robbanás okozta lökéshullám következtében a „ground zéró"-tól számított 2 km sugarú körben minden épület a földdel lette egyenlő, a rendkívül magas hőmérséklet miatt minden elpusztult. A város leégett és lakosságának 40%-a elpusztult. (Barnaby és Rotblat, 1982; Pittock és mások., 1986).
Három nappal Hirosima uránium bombával történt elpusztítása után augusztus 9-én Nagaszaki plutónium bomba támadásnak esett áldozatul. Mindkét város teljes kezdetleges infrastruktúrája megsemmisült.

Three Mile Island és a Csernobili atomerőmű esete

A radioaktív szennyezés lehetősége nem csak háborús körülmények között fordulhat elő.
A nukleáris erőműveken bekövetkező baleseteknek is hasonló hatása lehet a környezetére beleértve az ivóvíz bázisokat is. 1979. március 28-án meghibásodás történt a Pennsylvaniai Susquehanna folyó menti Three Mile Island atomerőmű vízhűtésű reaktorában. Végzetes balszerencse miatt a reaktor hűtővízének mennyisége annyira lecsökkent, hogy a reaktor olvadásig hevült. Szerencsére radioaktív szennyeződés nem került a környezetbe és az atomerőmű közelében lakók között sem történt sérülés. (Rees, 1994; Hopkins, 2001).
Azonban a reaktor tönkrement és környezetének megtisztítása 10 évet vett igénybe, a költségek pedig elérték az 1 Mrd USD-t.
A legrosszabb következményekkel az egykori Szovjetunió területén lévő Csernobili atomerőmű végzetes meghibásodása járt. 1986. április 26-án a reaktor teljesítményének növekedése robbanáshoz vezetett. A reaktor teljesítményét szabályozó grafit rudak elégtek és 10 napon keresztül radioaktív részecskék kerültek az atmoszférába. (Rich, 1991)
Az időben történő és hiteles információ közlése a Csernobil közelében és a szomszédos területek és országokban lakók számára elmaradt. Az eztán történtek is rámutattak a krízis kommunikáció fontosságára. A kommunista rendszer megpróbálta titokban tartani a balesetet és a szerencsétlenség bekövetkezéséről is csak az április 28-i esti adásában számolt be a szovjet televízió. A szerencsétlenség helyszínétől csak 3 km-re lévő Pripjaty város lakóinak kitelepítését 60 órával a robbanás után kezdték meg a hatóságok. További egy hetet vett igénybe a Csernobiltől 30 km sugarú körön belül lakók evakuálása. Skandináviában és a brit

szigeteken radioaktív szennyeződéseket tartalmazott az eső, a szovjet kormány a nemzetközi kommunikációban is súlyos hibákat vétett. A radioaktív szennyeződésnek hatása volt a legeltetett állatok tartására is. A birkák szabad legeltetését korlátozni kellett, a szabadon tartott tehenek tejében a radioaktív jód koncentrációja jelentősen megnövekedett. A Pripjáty folyó a terület legjelentősebb vízgyűjtőjeként a Dnyeperbe ömlik. Ez a vízbázis 35 millió ember – beleértve a főváros, Kiev lakosait is- vízellátását biztosítja. A csernobili balesetet követő néhány évben másodlagos radioaktív szennyeződés is problémákat okozott. A kiáradt folyók, amelyek elárasztották a vízgyűjtő területeket. A Bragyinka és a Szenna folyók vizében mért stroncium és cézium izotópok koncentrációja jelentősen növekedett. Világszerte több száz atomerőmű üzemel közel negyven ország területén és ezek állítják elő a világ elektromos energia szükségletének 16%-át. Az Európai Unió területén ez a részesedés 35 %. Franciaországban az elektromos energia közel 77%-át állítják elő atomerőművek, az Egyesült Államokban pedig 110 reaktor üzemel 32 tagállamban. Hat tagállamban pedig az energia szükséglet több mint 50 %-át állítják elő az atomerőművek.

Jelenlegi tendenciák és a jövőbeli kockázatok

A Szovjetunió felbomlása, a kommunista rendszerek és a Varsói Szerződés megszűnése jelentősen enyhítette a hidegháború nukleáris kockázatait. Azonban az India és Pakisztán által folytatott nukleáris kísérletek és az a tény hogy egy iszlám állam elsőként atomfegyverrel rendelkezik – újabb kockázatot jelent a világ számára. 1999-ben a NATO akcióba lépett a Milosevic vezette Jugoszlávia (Szerbia) ellen. Paradox módon ez a háború nukleáris fenyegetést is jelentett. A NATO támadást követően Jelcin orosz elnök drámai hangú figyelmeztetést fogalmazott meg a NATO egyoldalú lépésére válaszul. Az orosz nukleáris töltetű rakétákat a NATO akcióban részt vevő tagállamok városaira irányították. Szerencsére a figyelmeztetést nem vette komolyan a nyugat. Bárhogy is de bebizonyosodott, hogy a régi reflexek működnek Oroszországban és Kínában is, és a régi logika szerint készek lennének a NATO egyoldalú lépésére nukleáris fegyverekkel válaszolni. Mindkét hatalom a nukleáris fegyverek tekintetében szuperhatalomnak számít. A gazdasági nehézségekkel küzdő Oroszország a USA-val szemben folytatott hagyományos fegyverkezési versenyben fokozatosan lemarad, ezért a nemzetközi konfliktusok kezelése során hamarabb fenyegetőzik a nukleáris rakéták „indítógombjának megnyomásával” (BBC, 2000; Bruins, 2000)

Irán folytatja az orosz segítséggel indított nukleáris programját. Ebben hatékony segítséget kapott Pakisztántól és Kínától is. A Nemzetközi Atomenergia Ügynökség erős nyomást fejtett ki Iránra, hogy engedélyezze ellenőreinek a nukleáris létesítmények látogatását. Az Iránban folyó nukleáris fejlesztések és Oroszország szerepe előkelő helyen szerepelt 2003-ban a Camp David-ben folytatott Putyin orosz és Bush amerikai elnök közötti megbeszélésen. A szeptember 11-i terrortámadást követően az USA lehetséges szcenárióként vetítette előre a terrorista csoportok nem-hagyományos fegyverekhez jutásának veszélyét.
Észak Korea az USA által gyakorolt politikai nyomásra adott válaszként újraindította a Yongbyon-ban felépített nukleáris létesítményeit és érvénytelennek nyilvánította az atomsorompó egyezményt magára nézve. Észak Korea által fejlesztett nukleáris rakétákkal és fegyverekkel kereskedni is próbál. Ezek a folyamatok növelik az atomfegyverek használatának a kockázatát, hiszen olyan államok, hatalmi csoportok is hozzáférnek ezekhez az eszközökhöz, amelyek nem riadnak vissza használatuktól egy konfliktus , területi vita vagy terrorcselekmény elkövetésekor.

Ivóvíz bázisok lehetséges elszennyeződése nukleáris esemény miatt

A csernobili események és az atmoszférában végzett kísérleti atomrobbantások utáni mérések igazolták, hogy a csapadékban – a vízkörfolyamat révén – nagy mennyiségű radioaktív szennyeződés mutatható ki. A radioaktív por és a levegőben lévő folyadékrészecskék szuszpenziót alkotva a légkörben maradnak – koncentrációtól, tömegtől, levegőáramlástól és gravitációtól függően. A nukleáris robbanást követően ez a közeg 24 órán belül kialakul és a későbbiek folyamán bárhol a világon megjelenhet a csapadékkal. A lezuhanó esőcseppek könnyedén magukkal ragadják a radioaktív szennyeződésű részecskéket és az eső szinte „kimossa" az atmoszférából a szennyeződést a földre. Ezért a csapadékosabb területek fokozottabb veszélynek vannak kitéve radioaktív szennyeződés lerakódása tekintetében.
A Csernobili katasztrófát követően a „kedvező" meteorológiai feltételek miatt radioaktív szennyeződés növekedését észlelték Skóciában, Anglia északi részén, Észak-Írországban és Wales-ben.
A föld feletti vizek és a talajvizek radioaktív szennyeződése közötti alapvető különbség a következőkben rejlik:
Egy feltételezett nukleáris csapás hatása (Ambio, 1982) az ivóvízbázisokra úgy alakul, hogy a legnagyobb koncentrációban a csapadékban jelenik meg a radioaktív szennyezés, ezt követik a folyók vizei, majd a tavak és a talajvizek. Ez avval magyarázható, hogy a csapadék földet érve a folyóvizeket és az állóvizeket éri el leghamarabb. A föld különféle típusú felső rétegei elnyelik és megkötik a legveszélyesebb hasadó anyagokat. Az 1963-ban végzett kísérleti atomrobbantások következtében Közép Európában az esővíz radioaktivitása elérte az 500 pCi/l* visszamaradó béta aktivitást, míg a folyóvizek radioaktivitása ugyanebben a régióban 30 pCi/l körül volt mérhető. Természetesen a szennyeződés mértékét befolyásolják a klimatikus viszonyok, a geológiai tulajdonságok, a talaj megkötő képessége. A felszíni vizek jelentősebb mértékben tartalmazhatnak radioaktív szennyeződést karszt-talajban, állandóan fagyott talajban, sivatagban, vagy lápos, mocsaras vidékeken.

Veszélyhelyzeti vízellátás tervezése kritikus időszakokban

Az 1906-os San Fransiscoi természeti csapásból sokat tanult az ivóvíz-hálózat üzemeltetésével kapcsolatban a vízi-közmű szakma. Kalifornia államban számos módon előzik meg a katasztrófák által lehetséges károk bekövetkezését a vízellátó rendszerekben. A folyamatos ivó vízellátási tervek kulcs-szavai a redundancia, tartalék-rendszer és helyettesítő struktúrák. (Putnam, 2000; Bruins, 2000).
Flexibilis poliuretán alapú csővezetékeket alkalmaznak, amelyek könnyedén cserélhetők sérülés esetén és gyorsan helyreállítható a csőhálózat üzeme.
Az egész államra érvényes vészhelyzeti (havaria) terveket (Standardized Emergency Management System= SEMS) dolgoztak ki, így közös mindenki által ismert és elfogadott tervek alapján végezhető a mentés, helyreállítás.
Az 1989-es Loma Prietai földrengés és az 1994-es Northridge-i földrengés következményei minimalizálhatóak voltak ezeknek a standardoknak az alapján.
A legnagyobb problémát természetesen a bizonytalan jövő jelenti… (Faludi, 1987, p. 315).

A bizonytalan jövő jelentette katasztrófa helyzetek széles skáláját tekintve mégis két alapvető szcenáriót lehet elkülöníteni. Az egyik az ivóvízbázisok nem-hagyományos elszennyeződése – nukleáris baleset, terroristatámadás, háború révén – amikor a csőhálózati rendszerek, a vízi közművek létesítményei nem sérülnek fizikailag és hagyományos értelemben működőképesek maradnak.

A másik eset, amikor az ivóvíz ellátó rendszer létesítményei is sérülnek, az ivóvízbázisok is szennyeződnek és nagy tömegeket, menekülteket, kitelepítetteket kell azonnal szükség vízellátásban részesíteni az élelmiszer és óvóhely biztosítása mellett.
Az első forgatókönyv kevésbé tűnik bonyolult esetnek, de kritikus fontosságú elemekről kell gondoskodni és vészhelyzeti mechanizmusokat kell életbe léptetni – még a vészhelyzet bekövetkezése előtt. A real-time monitoring rendszerek alkalmasak a kijelölt biológiai és kémiai szennyeződések, elemek észlelésére – és természetesen érzékelik a radioaktív anyagok jelenlétét is. A monitoring rendszerek a „vészcsengő" szerepét töltik be – segítségükkel megelőzhető hogy az emberekhez szennyezett víz jusson el és jelzik az alternatív vízforrások igénybevételének szükségességét.
Clark és Deininger (2000) jelezték a bio-terrorizmus potenciális veszélyét az ivóvíz rendszerekben. Leszögezték, hogy a városi ivóvíz-hálózatban a 0,5 mg/liter szabad klór koncentráció számos mérgező anyag és biológiai tényező elleni védekezésben alapvető fontosságú. A klór koncentrációjának váratlan csökkenése is riasztást kell kiváltson, jelezve a bio-kémiai támadást.

1986. július 10-én a Fehér Ház elnöki hivatalában megszüntették a vezetékes vízellátást miután a monitoring rendszer a klór koncentráció csökkenését jelezte. Reagan elnök ekkor kapta meg reggeli kávéját – palackozott vízből főzve. A Nyugati szárnyban nem zárták el a vizet, de a személyzet figyelmét felhívták, hogy ne fogyasszanak vezetékes vizet. (Clark and Deininger, 2000:77; New York Times, 1986)

A klór koncentráció folyamatos figyelése az ivóvíz ellátó rendszerekben rendkívül fontos, és olcsón, könnyen megoldható. Azonban a klór szint csökkenése nem ad információt arra vonatkozóan, hogy mi miatt következett be a csökkenés. A veszélyes mérgező anyagok közvetlen és gyors detektálása is létfontosságú a vészhelyzeti tervezésben. Napjaink tudományos csúcsteljesítménye a biokémiai veszélyforrások azonosítása. Ez az eljárás Robert Marks biológus (Ben Gurion University of Negev) nevéhez fűződik. Olyan bioszenzorokat (Marks és mások., 1997; Polyak és mások.,2000) fejlesztett ki, amelyek egy cipős doboz méretű készülékbe építve, és az eszközt a vízellátó rendszer bármely pontjára telepítve vagy mobil készülékként képes a mérgező anyagok kimutatására. Genetikai kutatásokkal sikerült olyan baktériumot kitenyészteni, amely mérgező anyaggal érintkezve fényt bocsájt ki magából. Ezt a genetikailag módosított baktériumot egy algából készült optikai szál végére illesztette. A szabadalmaztatott eljárással készült optikai szál vízbe helyezhető. Ha a víz olyan szennyeződést tartalmaz, amely veszélyezteti a baktérium genetikai állományát a baktérium fényt bocsájt ki. Az optikai szál a fényt egy érzékeny fényelemhez továbbítja, amely felerősíti és elemzi a fényjelet. (Schechter,2001; Siegel, 2003)

A vízminőség monitorozása, a biztonságos vízbázisok meghatározása minden államban, országban kritikus fontosságú és törvényben védett besorolású. A talajvizek a felszíni vizekhez képest általában jobban védettek terrorista behatásoktól és szennyeződésektől, ezért ezek a vízforrások jelentőséggel bírnak az ivóvízellátás folyamatossága szempontjából a vészhelyzeti tervekben. (Davies and DeWiest, 1970)
Hidrogeológiai tanulmányok alapján lehet azokat a talajvíz forrásokat behatárolni, amelyek a lehetséges szennyezések tekintetében biztonságosan védettek.

A második számú forgatókönyv, amely a vízi-közmű létesítmények megrongálódásának, a vízbázisok elszennyeződésének és tömegek vízzel való ellátásának esetére készült kell, hogy tartalmazza azokat a módszereket, amellyel biztosítható az emberek ellátása. Ebben kell választ találni arra a kérdésre, hogyan biztosítható elegendő ivóvíz havaria helyzetekben?

Lesz-e elegendő elektromos energia vagy üzemanyag a berendezések, vízszivattyúk működtetésére? Számos segélyszervezet és állami intézmény bevonása biztosítja a menekültek vagy víz nélkül maradt emberek tömegeinek ellátását. Az ivóvíz és az egészségügyi ellátás biztosítása nem új keletű feladat. (Chalinder, 1994)
Mégis az új idők új katasztrófái merőben más megközelítést igényelnek minden résztvevőtől. Az esővíz felhasználásával végzett ivóvízellátás, a ciszternákban, víztartályokban való összegyűjtés problémás lehet a radioaktív, biológiai, kémiai szennyeződések miatt. A folyó vizek felhasználása sem lehetséges a veszélyes anyagok miatt. A víztárolók kapacitása pedig elhanyagolható az ellátás szempontjából. Amennyiben a radioaktív részecskék lesüllyednek a vízfelszín alá, a víz minősége nem túl rossz, de a tisztítási módszerek használatát mindenképp előtérbe kell helyezni. A mesterséges gátak közé szorított víz, a víztározók könnyen támadhatóak, a felszínen összegyűjtött vizek hamar eltűnhetnek. A karsztos talaj feletti, a fagyott talaj feletti, a sivatagi és mocsaras területek feletti vizek megbízhatatlan minőségűek, ahogy fentebb említettem. A szennyezett felszíni vagy talaj-vizek kezelhetőek vészhelyzeti körülmények között? A korábban említett új típusú érzékelő rendszerek használata segítséget jelenthet mobil vízkezelő rendszerek építésében. A szennyezett vizet egy reaktorba szivattyúzzuk, ahol UV sugárzás éri. 10 órányi expozíció után kevesebb, mint egy százalék biológiai fertőzés marad a vízben. A mobil víztisztító berendezéseket arra a területre lehet szállítani ahol a katasztrófa helyzet miatt szükséges az emberek egészséges ivóvízzel való ellátása. (Siegel, 2003).

Ezek a mobil víztisztító berendezések széles kapacitás tartományban üzemelnek, a néhány 100 literes kapacitástól a több százezer liter napi kapacitásig. Vannak, amelyek palackba vagy műanyag zacskóba töltik az ivóvizet, amelyet így szállítanak el a szükséget szenvedőkhöz.
Bizonyos típusok akár a tengervízből is képesek ivóvizet előállítani. A kisebb berendezések napelemmel is működtethetőek, ez különösen fontos lehet azokon a területeken, ahol az elektromos energia ellátás is szünetel. (Mathew és mások, 2001)

A mobil berendezésekben alkalmazott szűrési eljárás a reverz ozmózis (RO) jelenségére épül. Ezekben a szűrőkben félig áteresztő membránszűrő található, amelyen 0,0001 µm méretű lyukak vannak. A reverz ozmózis szűrői kiszűrik a vízből a nehézfémeket, a klórt, a rovarirtót, baktériumokat, vírusokat és a radioaktív szennyeződést is.

Aluminum	97–98%	Nickel	97–99%
Ammonium	85–95%	Nitrate	93–96%
Arsenic	94–96%	Phosphate	99+%
Bacteria	99+%	Polyphosphate	98–99%
Bicarbonate	95–96%	Potassium	92%
Bromide	93–96%	Pyrogen	99+%
Cadmium	96–98%	Radioactivity	95–98%
Calcium	96–98%	Radium	97%
Chloride	94–95%	Selenium	97%
Chromate	90–98%	Silica	85–90%
Chromium	96–98%	Silicate	95–97%
Copper	97–99%	Silver	95–97%
Cyanide	90–95%	Sodium	92–98%
Ferrocyanide	98–99%	Sulphate	99+%
Fluoride	94–96%	Sulphite	96–98%
Iron	98–99%	Zinc	98–99%
Lead	96–98%	*Virus	99+%
Magnesium	96–98%	*Insecticides	97%
Manganese	96–98%	*Herbicides	97%
Mercury	96–98%	*Detergents	97%
*Total Dissolved Solids	95–99%		

TFC membránt alkalmazó reverz ozmózis alapú víztisztító berendezés szűrési hatásfoka

Forrás: PURE PAK (http://purepak.org/(S(l2k5y355alflif554jnx0345))/uro.aspx)

A bejövő, tisztítatlan víz egy része mossa ki a szűrőt így a membrán sokáig tiszta marad. A membrán cseréje általában 1 és 4 évnyi üzemidő után esedékes. A reverz ozmózis alapú szűrőberendezések alkalmasak mindenféle szennyeződés eltávolítására. Ezért javasolt ezeket a berendezéseket figyelembe venni a veszélyhelyzeti vízellátás megtervezésekor. A berendezések lehetnek személyi használatúak és egész város ivóvízszűrését biztosító nagy teljesítményű változatok. Ezek a berendezések több fázisban végzik a tiszta ivóvíz előállítását. Tartalmaznak homokszűrőt, szénszűrőt, TFC reverz ozmózis alapú membrán szűrőt, a fertőtlenítéshez UV fényforrást és végül a megfelelő íz hatás miatt ásványi anyagokat is adagolnak a steril tisztaságú vízhez.
A radioaktív szennyezőanyagok kiszűréséhez kerámia szűrőket alkalmaznak, amelyekben ezüst ion adagolása is történik. Az ezüst ion köti meg a szennyező anyagokat a szűrőben.

Összefoglalás

Az 1986-os Csernobilban történt nukleáris katasztrófa megmutatta, hogy mind a korábbi Szovjetunió mind pedig Nagy Britannia kormányzati rendszerei nagyon lassan kezelték a krízis szituációt és nem voltak felkészülve a radioaktív szennyeződéssel kapcsolatos teendőkre.

A nem-hagyományos fegyverek elterjedése folytatódik. A jövő terrorista támadásai, nukleáris balesetei és háborús konfliktusai soha nem tapasztalt károsodást okozhatnak az emberi környezetben, beleértve az ivóvíz ellátási rendszereket is.

A vízellátó rendszereket valamennyi állam a kritikus infrastruktúrák közé sorolja. Proaktív szemléletet és tervezést követel meg az ivóvíz ellátó rendszerek vészhelyzeti tervezése mind a

hatóságoktól, mind pedig a Vizi közművektől, abból a célból, hogy a nem-hagyományos szennyeződések detektálása azonnal megtörténjen.

Megfelelő kapacitású víztisztító berendezések telepítése szükséges a vészhelyzeti vízellátás biztosítása miatt.

A háztartások is képesek lehetnek kompakt kivitelű reverz ozmózis elv alapján üzemelő tisztító berendezés üzemeltetésére. A reverz ozmózis alapú berendezések képesek kiszűrni azokat a szennyeződéseket, amelyek a helyi vízmű tisztító berendezésének hibája, vagy technológiája miatt bekerültek a hálózatba.

Többféle vészhelyzeti forgatókönyvet kell készíteni a lehetséges katasztrófa helyzeteket modellezve. Redundáns, tartalék és helyettesítő elemeket is tartalmazó rendszereket kell tervezni azokra az esetekre, amikor a meglévő rendszerek megsemmisülnek vagy a kapacitásuk jelentősen csökken.

Mobil víztisztító állomásokat kell létrehozni, amelyek független áramforrással üzemeltethetőek, ezek a rendkívüli események kezelése során különös jelentőséggel bírnak.

Biztosítani kell a hidrogeológiai tanulmányok alapján kijelölt föld alatti ivóvízbázisok, mint alternatív vízforrások védelmét katasztrófa helyzetben történő igénybevétel esetére.

Katasztrófa helyzetben, amikor az ivóvíz szolgáltatás akár teljesen megszűnik a segélyszervezetek és hatóságok együttes segítségnyújtása időt vesz igénybe. Ezért ebben az időszakban az embereknek maguknak kell gondoskodniuk az ivóvíz ellátásukról. A kisteljesítményű és alternatív energiaforrást (napenergia, izomerő, stb.) használó berendezések beszerzése segít áthidalni ezt az időszakot.

Hivatkozások

Alexander, D., *Natural Disasters*, University College London Press, London, 1993.

Ambio, “Reference Scenario: How a Nuclear War Might to be Fought, *Ambio* 11(2-3): 94–99,

1982.

Barnaby, F., *Man and the Atom*. Thames and Hudson, London & Funk and Wagnalls, New York, 1971.

Barnaby, F., és J. Rotblat, “The Effects of Nuclear Weapons,” *Ambio* 11(2-3): 84–93, 1982.

BBC, “Russia Lowers Nuclear Threshold,” BBC News, Europe, January 14, 2000.

Bradford-Benini, J., “Getting Organized Pays Off for Disaster Response,” *J. Contin. Crisis*

Management 6(1): 61–63, 1998.

Bruins, H. J., “Proactive Contingency Planning vis-ŕ-vis Declining Water Security in the 21st

Century,” *J. Contin. Crisis Management* 8(2): 63–72, 2000.

Bruins, H. J., és H. Lithwick, "Proactive Planning and Interactive Management in Arid Frontier Development," in H. J. Bruins and H. Lithwick (eds.), *The Arid Frontier—Interactive Management of Environment and Development*, Kluwer Academic Publishers, Dordrecht/Boston/London, Chap. 1, . 3–29, 1998.

Chalinder, A., *Water and Sanitation in Emergencies. Good Practice Review 1*. Relief and

Rehabilitation Network, Overseas Development Institute (ODI), London, 1994.

Clark, R. M., and R. A. Deininger, "Protecting the Nation's Critical Infrastructure: the Vulnerability of U.S. Water Supply Systems," *J. Contin. Crisis Management* 8(2): 73–80, 2000.

Comfort, L. K., "Risk and Resilience: Inter-Organisational Learning Following the Northridge

Earthquake of 17 January 1994," *J. Contin. Crisis Management* 2(3): 157–170, 1994.

Davies, S. N., és R. J. M. DeWiest, *Hydrogeology*, Wiley, Chichester, 1970.

Dror, Y., *Policymaking Under Adversity*, Transaction Books, New Brunswick, 1986.

Faludi, A., *A Decision-centred View of Environmental Planning*, Pergamon Press, Oxford, 1987.

Foxell, J. W., "The Prospect of Nuclear and Biological Terrorism," *J. Contin. Crisis Management* 5(2):

98–108, 1997.

Harmancioglu, N. B., O. Fistikoglu, S. D. Ozkul, V. P. Singh, and M. N. Alpaslan, *Water Quality*

Monitoring Network Design, Water Science and Technology Library, vol. 33, Kluwer Academic Publishers, Dordrecht/Boston/London, 1999.

Harris, S. L., "Unstable Lands: the Terror of Temblors and Volcanoes," in *Restless Earth*, The Book Division, National Geographic Society, Washington, DC, . 146–215, 1997.

Hopkins, A., "Was Three Mile Island a 'normal accident," *J. Contin. Crisis Management* 9(2): 65–72, 2001.

Hutchinson, T. C., M. A. Harwell, W. P. Cropper, and H. D. Grover, "Additional Potential Effects of Nuclear War on Ecological Systems," in M. A. Harwell and T. C. Hutchinson (eds.), *Environmental Consequences of Nuclear War. Volume II. Ecological and Agricultural Effects*, SCOPE 28, Wiley, Chichester, . 173–267, 1985.

Malik, A. S., et al., *Solar Distillation*, Pergamon Press, Oxford, 1982.

Marks, R. S., E. Bassis, A. Bychenko, and M. M. Levine, "Chemiluminescent optical fiber

immunosensor for detecting cholera antitoxin," *Opt. Eng.* 36(12): 3258–3264, 1997.

Mathew, K., S. Dallas, G. Ho, és M. Anda, "Innovative Solar-Powered Village Potable Water Supply," in *Women Leaders on the Uptake of Renewable Energy Seminar*, Perth, June 2001, . 97–105, 2001.

Michel-Kerjan, E., "New Challenges in Critical Infrastructures: A U.S. Perspective," *J. Contin. Crisis Management* 11(3): 132–141, 2003.

New York Times, *White House Water Cut Off Temporarily*, July 10, p. 16, 1986.

Niksch, L. A., "North Korea's Nuclear Weapons Program," *Congressional Research Service*, The Library of Congress, IB91141, . 1–18, updated August 27, 2003.

Pittock, A. B., T. P. Ackerman, P. J. Crutzen, M. C. MacCracken, C. S. Shapiro, and R. P. Turco, *Environmental Consequences of Nuclear War. Volume I. Physical and Atmospheric Effects*. SCOPE 28, Wiley, Chichester, 1986.

Polyak, B., E. Bassis, A. Novodvorets, S. Belkin, and R. S. Marks, "Optical Fiber Bioluminescent Whole-Cell Microbial Biosensors to Genotoxicants," *Water Sci. Technol.* 42(1-2): 305–311, 2000.

Putnam, D. R., "Earthquakes and Water Security: Contingency Planning in California," *J. Contin. Crisis Management* 8(2): 103–108, 2000.

Rees, J., *Hostages of Each Other: The Transformation of Nuclear Safety since Three Mile Island*, University of Chicago Press, Chicago, 1994.

Rich, V., "An Ill Wind from Chernobyl," *New Scientist* 20 April, vol. 130, No. 1765, . 26–29, 1991.

Rosenthal, U., and A. Kouzmin, "Globalizing an Agenda for Contingencies and Crisis Management: An Editorial Statement," *J. Contin. Crisis Management* 1(1): 1–12, 1993.

Rosenthal, U., M. T. Charles, and P. 't Hart, "Introduction: The World of Crises and Crisis

Management," in U. Rosenthal, M. T. Charles, and P. 't Hart (eds.), *Coping with Crises: The*

Management of Disasters, Riots and Terrorism. Charles C. Thomas, Springfield, . 3–33, 1989.

Schechter, E., "Israeli Scientist Perfects Rapid Test to Detect Water Poisoning," *The Jerusalem Report*, December 31; vol 12, No. 18, p. 6, 2001.

Shimazu, Y. (ed.), "Lessons from Hiroshima and Nagasaki," SCOPE-ENUWAR Report HI.01.85, 1985.

Siegel, J., "BGU Scientist Develops Method to Detect, Clean Contaminated Water," *The Jerusalem Post*, March 3, vol 71, No. 21438, p. 4, 2003.

U.S. EPA, "Radionuclides Notice of Data Availability–Technical Support Document," Targeting and Analysis Branch, Standards and Risk Management Division, Office of Ground Water and Drinking Water, United States Environmental Protection Agency. Prepared by U.S. EPA Office of Ground Water and Drinking Water, in collaboration with U.S. EPA Office of Indoor Air and Radiation, and United States Geological Survey, 2000.

U.S. Water News Online, "Chemical-Free Mobile System Treats Water in Emergencies," 1995, : http://www.uswaternews.com/archives/arcquality/5chefree.html.

Wetzel, K. G., "Effects on Global Supplies of Freshwater," in *Nuclear War: The Aftermath*, Royal Swedish Academy of Sciences, Stockholm, *AMBIO*, vol. 11(2-3): . 126–131, 1982.

Wildavsky, A., *Speaking Truth to Power*, Little-Brown, Boston, 1979.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Körmendi Krisztina
krisztina.kormendi@gmail.com

Solymosi József
solymosi.jozsef@zmne.hu

AZ ENERGIAPOLITIKA MEGVÁLASZTÁSÁNAK KÖRNYEZETBIZTONSÁGI SZEMPONTJAI A VILLAMOSENERGIA TERMELÉS VONATKOZÁSÁBAN

Absztrakt

A 21. századi modern társadalom egyre növekvő villamosenergia igényének kielégítése számos problémát vet fel, ezek egyike a termelés a környezetre gyakorolt hatása, mely globális klímaváltozáshoz vezethet, károsíthatja az épített környezetet, az élővilágot, az emberi egészséget. A fenntarthatósági szempontokat figyelembe vevő energiapolitikának ezen hatásokat, környezetbiztonsági szempontokat is figyelembe kell vennie és a kedvezőbb környezeti hatású termelési módokat kell támogatnia. A különböző energiahordozókon és technológiákon alapuló termelési módok környezeti hatásai között jelentős eltérések lehetnek. Egy, a környezeti hatások összehasonlítását lehetővé tevő módszer az ún. életciklus elemzés. Jelen közleményben a magyarországi villamosenergia termelésben alkalmazott módok összehasonlítását célzó vizsgálat eredményei közül mutatunk be néhányat egy 2009.-ben megjelent kutatási összefoglaló jelentés alapján. Majd röviden áttekintjük, hogy a magyar energiapolitika mennyire van összhangban a környezetbiztonsági szempontokkal, azaz mennyire támogatja a kedvezőbb környezeti hatású termelési módok alkalmazását.

To supply the growing electricity needs of the modern life of the 21th century raises several problems, one of them is the power generation's impact to the environment. This impact could lead to the global climate change, could harm the built environment, the nature and the human health. An energy policy that considers the aspects of sustainability, should consider these environmental impacts and should promote the power generation techniques which have the most advantageous environmental impacts. The different power generation methods based on different primary energy resources and technologies have different environmental impact. The environmental impact of different power generation methods can be compared applying the so called life cycle analysis method. In this article we present some of the results of a research which aim was to compare the environmental impacts of the power generation methods used in Hungary, according to a research summary report published in 2009. After that we outlines how these environmental security aspects appear in the Hungarian energy policy, whether it promotes the power generation methods which have the most advantageous environmental impacts.

***Kulcsszavak**: villamosenergia-termelés, környezeti hatások, életciklus elemzés ~ power generation, environmental impacts, life cycle analysis*

A VILLAMOSENERGIA TERMELÉS KÖRNYEZETI HATÁSAI

A 21. századi lét alapvető kelléke a villamosenergia. A modern gazdaság működése, a modern társadalom élete elképzelhetetlen megfelelő villamosenergia ellátás nélkül. A fejlődés előrehaladásával egyelőre a villamosenergia igény is nő. A villamosenergia termelés fokozása azonban számos kedvezőtlen hatással van környezetünkre, mely következményei károsítják az épített környezetet, az élővilágot, kedvezőtlen hatással vannak az emberi egészségre, hozzájárulnak a globális klímaváltozás kialakulásához.

A különböző energiahordozókat és technológiákat használó termelési módok környezeti hatása eltérő. A következőekben ezeket a hatásokat próbáljuk szemléltetni a teljesség igénye nélkül. A fosszilis energiahordozók elégetésén alapuló termelés során számos olyan káros anyag kerül a légkörbe, mint pl.:

- üvegházhatású szén-dioxid, mely a globális felmelegedés, globális klímaváltozás okozója;
- nitrogén és kén oxidok, melyek az épített környezetet és az állatvilágot károsító savas eső okozói;
- szilárd anyagok (por, el nem égett olajszármazékok), melyek belélegzése hozzájárul különböző emberi betegség kialakulásához.

Valamint számolni kell az üzem során keletkező veszélyes hulladékok és hő terhelés környezeti hatásaival is.

Az atomenergia esetén példaként a radioaktív hulladékok környezeti hatásait, a hő terhelést, a lakossági sugárterhelést említjük meg. A radioaktív terhelés egy esetleges baleset hatására igen erős is lehet. Mindemellett az atomenergia használata nem jár szén-dioxid kibocsátással.

A megújuló energiákkal történő energiatermelés szintén nem jár szén-dioxid kibocsátással, általánosságba véve környezetszennyező hatásai is igen alacsonyak, ezért zöld energiának is nevezik. Megjegyzendő azonban, hogy ha nem csak a villamosenergia termelést, hanem a teljes életciklus tekintetében vizsgáljuk a megújuló energiát hasznosító technológiákat számos környezetszennyező hatás - köztük a szén-dioxid kibocsátás, veszélyes hulladékok – jelenik meg, nem beszélve pl. a szélenergiánál megjelenő zajszennyezésről valamint egyéb táj és természetvédelmi szempontokról (pl. élővilágra, talajszerkezetre, felszíni és felszín alatti vizekre gyakorolt hatás). A vízenergia kapcsán például a talajvízszintre, a terület vízháztartására, mikroklímájára gyakorolt hatásokat kell figyelembe venni.

Összességében a villamosenergia termelés és ellátás számos nemkívánatos hatással jár, a főbb környezet- és egészségkárosító hatások:

- Légszennyezés (légnemű anyag, szilárd lebegőanyag kibocsátás)
- Vízszennyezés (felszíni vizek, talajvizek, rétegvizek szennyezése folyékony és oldódó szilárd anyagokkal)
- Talajszennyezés (talajfelszín szennyezése kiülepedés által, mélyebb talajrétegek szennyezése beszivárgás által, szilárd, folyékony szennyezőanyagokkal
- Bioszféra (élővilág) közvetlen és közvetett károsítása (erdőpusztulás, bizonyos fajok eltűnése, mérgező anyagok felszívódása növényekbe, növényzet sugárterhelése, vizek

élővilágának (pl. halállománynak) pusztulása, mérgező anyagok felszívódása állatokba, állatok sugárterhelése)

- Mesterséges környezet károsodása (pl. műszaki létesítmények, épületek, vasszerkezetek, szerkezeti anyagok stb. károsodása, intenzív korróziója)
- Klímaváltozás (mikroklíma, vagy globális klíma esetében)
- Mezőgazdasági termékek (termelés) károsítása (hozamok csökkenése, minőségromlás, tisztítási többletköltségek felmerülése)
- Káros fizikai környezeti hatások (zajterhelés, rezgés, bűz, láthatóság romlása)
- Környezet esztétikai károsítása (romboló környezeti látvány, pl. meddőhányók, elhagyott bányák) [1]

A főbb szennyező anyagokat és hatásaikat az 1. számú táblázat foglalja össze.

Hatások	***Szennyezőanyagok***
Üvegházhatás	CO_2, CH_4, NO_x, N_2O, CFCs[1], CO
Ózonpajzs károsodása	CFCs
Savasodás	SO_2, NO_x
Fotoszmog	VOC[2], NO_2
Nitrifikáció	NO_x, foszfátok (PO_4)
Radioaktív sugárzás	Trícium, radon, ^{14}C, ^{85}Kr, ^{90}Sr, ^{238}U, ^{232}Th stb.
Biológiai degradáció	Környezetszennyezés okozta terméshozam-csökkenés, biológia életképesség csökkenése
Káros hanghatások, vibráció	Nagy forgógépek, csővezetékek, erőművi technológia, tüzelőanyag-előkészítés
Légköri láthatóság romlása	Füst, aeroszolok, fotoszmogok, vízgőz
Mikroklíma megváltozása	Nagy, intenzív párolgású vízfelületek (víztározók, hűtőtornyok, hűtőtavak stb.)
Mesterséges környezetben (épületekben, ipari létesítményekben, szerkezeti anyagokban, közlekedési eszközökben stb.) bekövetkezett, – környezetszennyezés okozta, - anyagi károk	Savas esők, szennyezés okozta intenzív korrózió

1. táblázat. *Legfontosabb szennyező hatások és szennyezőanyagok. Forrás [1]*

[1] chlorofluorocarbons, halogénezett szénhidrogének
[2] volatile organic compound, illékony szerves vegyületek

A környezeti hatások az egyes energiatermelési módoknál eltérő mértékben jelennek meg, így az egyes termelési módok környezeti hatásai között jelentős különbségek vannak. Az energiapolitika megválasztásakor – tekintettel a fenntartható fejlődés szempontjaira – figyelembe kell venni, hogy a villamosenergia termelés (ellátás) nemkívánatos környezetszennyező hatással jár. Az energiapolitikának és a környezetpolitikának egymással összhangban kell lennie.

Az objektív döntéshozáshoz azonban objektív adatokra, az egyes technológiák összehasonlíthatóságára van szűkség. A villamosenergia-termelési technológiák összehasonlításakor számos tényezőt figyelembe kell venni, értékelni kell, például:

- az energiaátalakítás alapvető jellegét,
- az egyes villamosenergia-termelési technológiák főbb műszaki jellemzőit, a technológiai fejlesztésük jelenlegi állapotát, gyakorlati alkalmazásukat, bevezetettségüket,
- a primer energia hordozók rendelkezésre állását,
- a potenciális termelési kapacitást,
- az energetikai hatékonyságot,
- a gazdasági hatékonyságot (költségeket),
- a környezetterhelést,
- az egészségkárosító és anyagi károsodást okozó hatásokat,
- a villamosenergia-rendszer irányítására gyakorolt hatásokat,
- az externális költségeket,
- a fajlagos területigényt,
- a társadalmi elfogadottságot. [1]

Mindezek közül jelen közleményben csak a környezetterhelés szempontját ragadjuk ki és megkíséreljük e mentén összehasonlítani a villamosenergia termelési módokat a magyar energiaszektor viszonylatában.

Jelen közleményben az egyes energiahordozókat csak a villamosenergia szektorban vizsgáljuk. Megjegyzendő, hogy az egyes energiahordozók értékelésénél más összképet kapnánk, ha más szektorokat (pl. a geotermikus energia a lakossági hő ellátásban vagy a bioetanol a közlekedésben betöltött szerepét stb.) is figyelembe vennénk.

A VILLAMOSENERGIA TERMELÉSI MÓDOK ÖSSZEHASONLÍTÓ ELEMZÉSE A MAGYAR ENERGIASZEKTORBAN KÖRNYEZETTERHELÉSÜK SZEMPONTJÁBÓL

A villamosenergia termelési módok környezetterhelésének összehasonlítására alkalmas egyik módszer az ún. életciklus elemzés vagy életciklus hatásvizsgálat. (Az angol nyelvű szakirodalomban Life Cycle Analysis ill. Life Cycle Assessement, LCA)

A módszer azt vizsgálja, hogy egy termék, folyamat vagy szolgáltatás milyen környezeti hatásokkal jár, annak teljes életciklusa vagy az életciklus egy szakasza[3] során. A környezeti

[3] az életciklus szakaszai: nyersanyagok kitermelése és feldolgozása, gyártás, szállítás és terjesztés, használat, újrafelhasználás, újrahasznosítás, hulladék elhelyezés [2]
Az elemzés lépései:
- a vizsgálat céljának és a vizsgált rendszer határainak kijelölése
- inputok (természeti erőforrások) és outputok (kibocsátások) szisztematikus leltárba vétele

hatások módszeres feltárása egyrészt lehetőséget teremt ezen hatások tudatos csökkentésére másrészt azonos funkcionalitású, de eltérő környezeti hatású termékek, folyamatok, szolgáltatások közötti döntés megalapozására.

Az LCA módszert használták abban a vizsgálatban is, mely eredményeit *„ A magyar energiaszektor villamosenergia-termelésének életciklus-, és „carbon footprint" elemzése"* [3] című 2009-ben megjelent kutatási jelentés mutatja be. A vizsgálat célja az energiatermelési módok összehasonlítása volt környezeti terhelésük alapján a magyarországi villamosenergia termelésre vonatkozóan.

Az alábbiakban a vizsgálat néhány eredményét mutatjuk be a kutatásról készült összefoglaló jelentés [3] alapján. A kutatás során vizsgálták valamennyi villamosenergia termelési technológiát, melyeket a vizsgálat idején Magyarországon alkalmaztak illetve amelyek alkalmazására a vizsgálat idején a közeljövőben számítani lehetett. Ezek a következőek:

- villamosenergia termelés atomenergiából;
- villamosenergia termelés fosszilis energiahordozókból: lignit, barnaszén, feketeszén, földgáz, olaj;
- villamosenergia termelés hulladéktüzeléssel;
- villamosenergia termelés megújuló forrásokból: fatüzelés (biomassza), biogáz, bioetanol, vízenergia, szélenergia, napenergia.

A vizsgálathoz szükséges adatokat több forrásból szerezték be illetve állították elő. Felhasználtak hazai aggregált, ágazati és vállalati adatokat, külföldi adatbázisokat, hatástanulmányokat, fenntarthatósági jelentéseket és becslési algoritmusokat. A kiértékeléshez az ökoindikátor'99 és CML 2001 módszereket[4] használták.

Jelen közlemény keretei között nem térünk ki a vizsgálati módszertan, az alkalmazott kiértékelési módszerek, a rendszerhatárok meghatározásának, a felhasznált adatok és az elemzés lépéseinek részletezésére, mindezen információ a kutatási összefoglaló jelentésben [3] megtalálható. Az összefoglaló jelentésből a következő vizsgálatok eredményét emeljük ki és mutatjuk be:

1. gyengepont analízis
2. technológiák összehasonlító életciklus elemzése

A gyengepont analízis célja az volt, hogy meghatározza azokat a folyamatokat, melyek a környezetre gyakorolt hatás szempontjából gyenge pontnak számítanak, azonosítsa a jelentősnek mondható környezeti hatásokat és azt, hogy ezeket a hatásokat milyen folyamatok okozzák.

A technológiák összehasonlító életciklus elemzésének célja pedig az egyes technológiák környezeti hatásainak összehasonlítása volt.

A vizsgálat során egyrészt kiértékelték a különböző termelési módokat azonos mennyiségű megtermelt energiára vetítve, másrészt vizsgálták ezeket olyan rendszerben, melyben a különböző energiatermelési módok a valóságnak megfelelő arányban vesznek részt az 1 MJ

- környezeti hatások értékelése, hatásbecslés (figyelembe véve a források felhasználását, az emberi egészséget és az ökoszisztéma állapotát)
- eredmények értelmezése, dokumentálása [2]

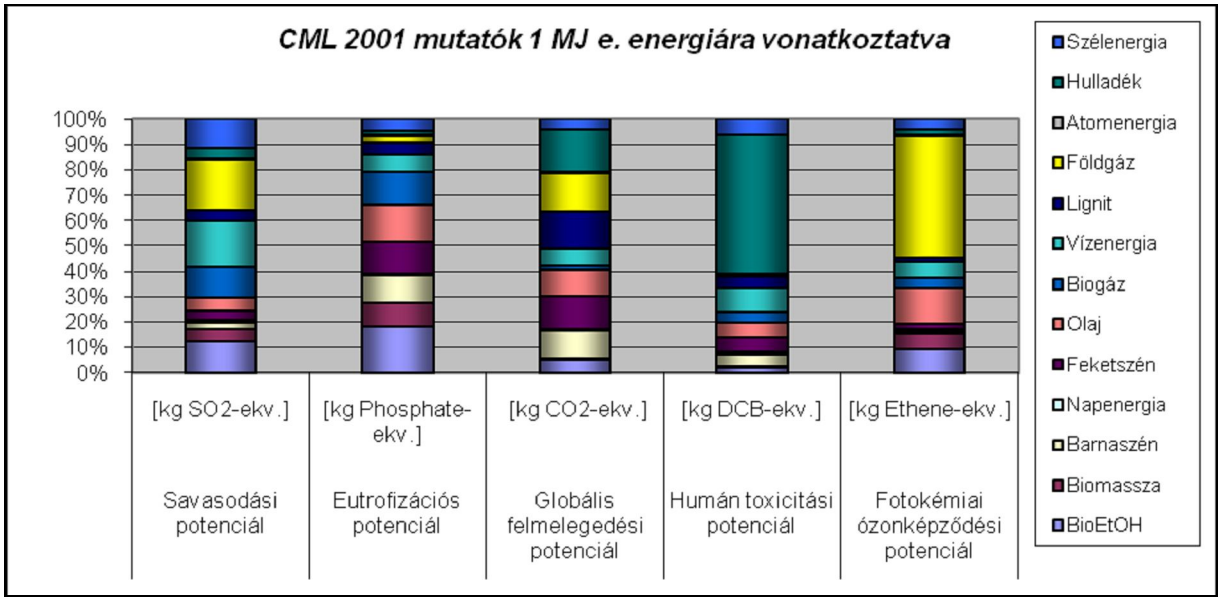
[4] Az ökoindikátor'99 módszer lehetővé teszi egy adott technológia környezeti teljesítményének jellemzését egy aggregált, dimenzió nélküli mutatószámmal. A CML 2001 módszerben alkalmazott mutatók az emissziókat referencia anyagok mennyiségére normálják. [3]

funkcionális egység villamosenergia megtermelésben, így a termelésből származó kibocsátásokat ebben az arányban vették figyelembe.

A környezeti hatások tekintetében az alábbi indikátorokat használták (CML 2001 mutatók):

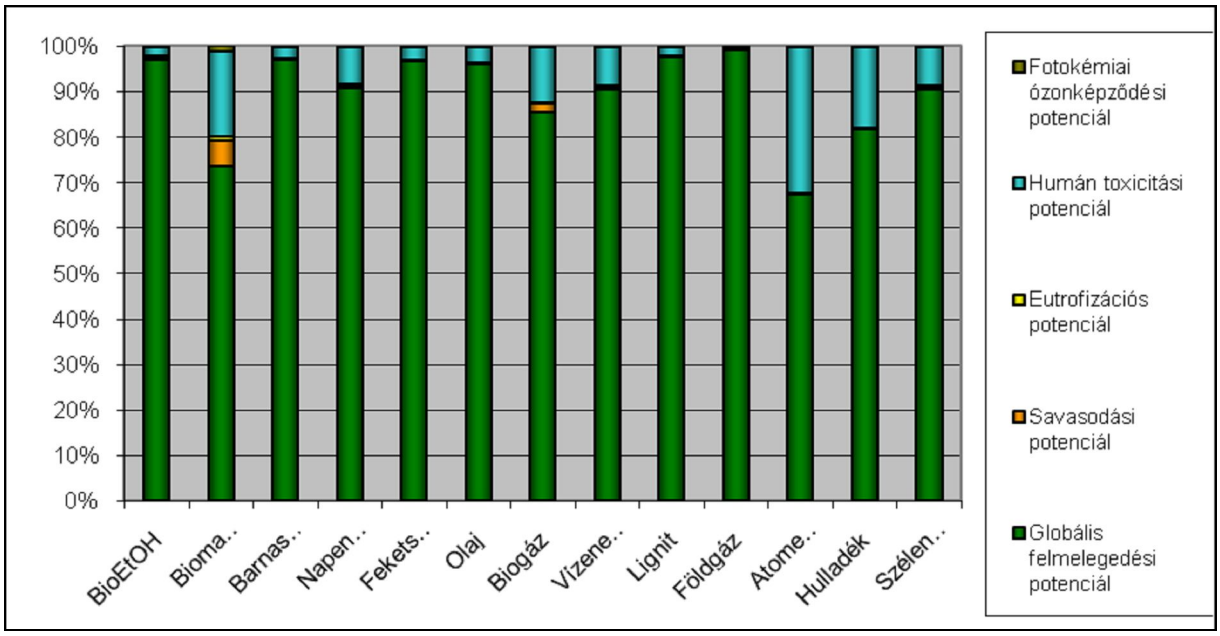
- Savasodási potenciál (regionális környezeti hatás, a környezet pH-jának változásához való hozzájárulást mutatja meg, kén-dioxidra normálva).
- Eutrofizációs potenciál (helyi hatás, a környezet tápanyagban való feldúsulásához való hozzájárulás mértékét mutatja meg, foszfátra normálva).
- Globális felmelegedési potenciál (globális hatás, a globális felmelegedéshez való hozzájárulás mértékét mutatja meg, szén-dioxidra vetítve).
- Humán toxicitási potenciál (helyi hatás, az emberre gyakorolt mérgezőséget mutatja meg, dikloro-benzolra normálva).
- Fotokémiai ózonképző potenciál (az alacsony légköri ózon képződéséhez való hozzájárulást mutatja meg, etilénre normálva). [3]

A kapott eredményt az 1. ábra mutatja be, abban az esetben amikor mindegyik termelési mód esetén azonos mennyiségű (1MJ) kiadott energiát vettek alapul.



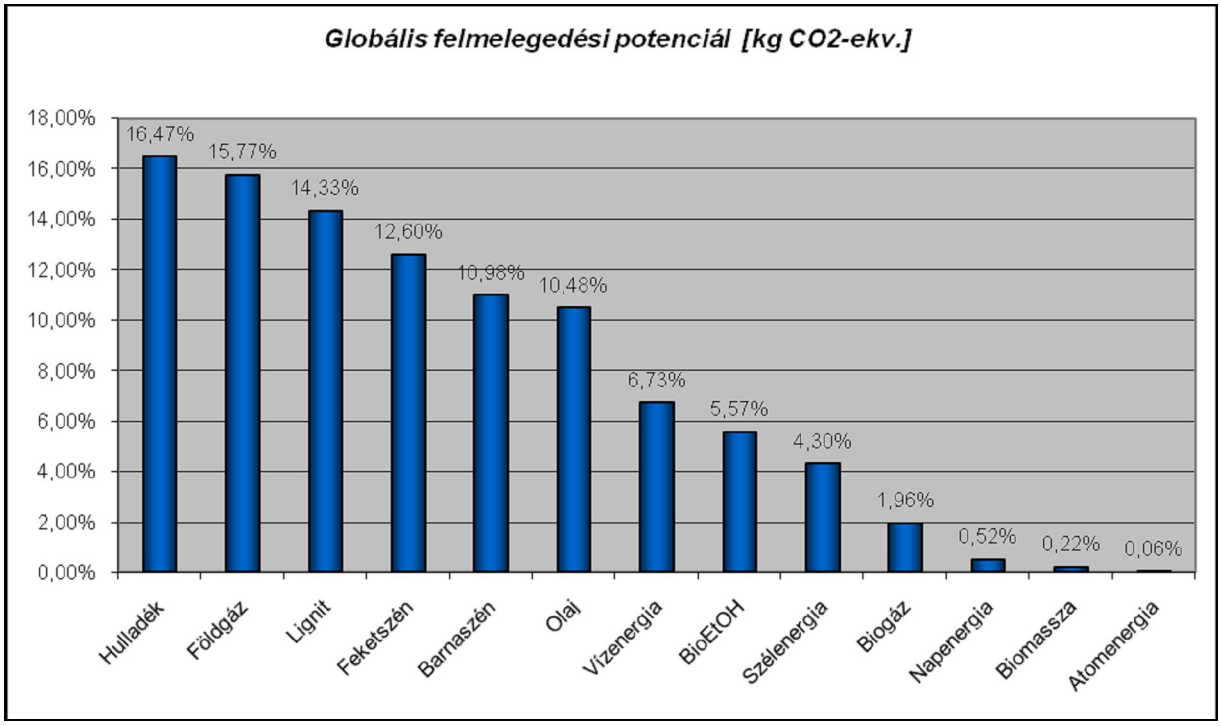
1. ábra. *A CML 2001-es mutatók megoszlása 1MJ elektromos energia funkcionális egység esetén. Forrás [3]*

Ugyanezeket az eredményeket indikátorokra rendezve a 2. ábra mutatja be.



2. ábra. *A különböző termelési módok környezetei hatásai, indikátorok szerinti rendezésben. Forrás: [3]*

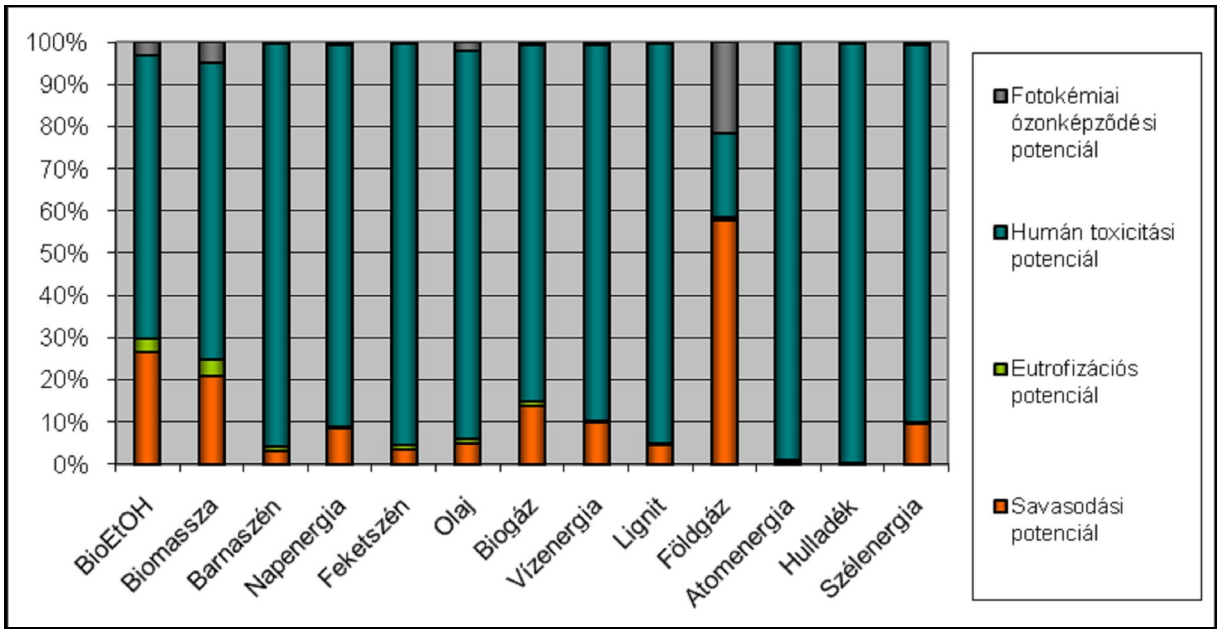
Látható, hogy valamennyi termelési mód esetén a globális felmelegedés potenciál indikátora a legmagasabb, főképp a fosszilis tüzelőanyagokon alapuló termelési módoknál, oka az üvegházhatású gáz kibocsátás. Az indikátor termelési módok szerinti alakulását a 3. ábra mutatja be.



3. ábra*. A globális felmelegedési potenciál összehasonlítása. Forrás [3]*

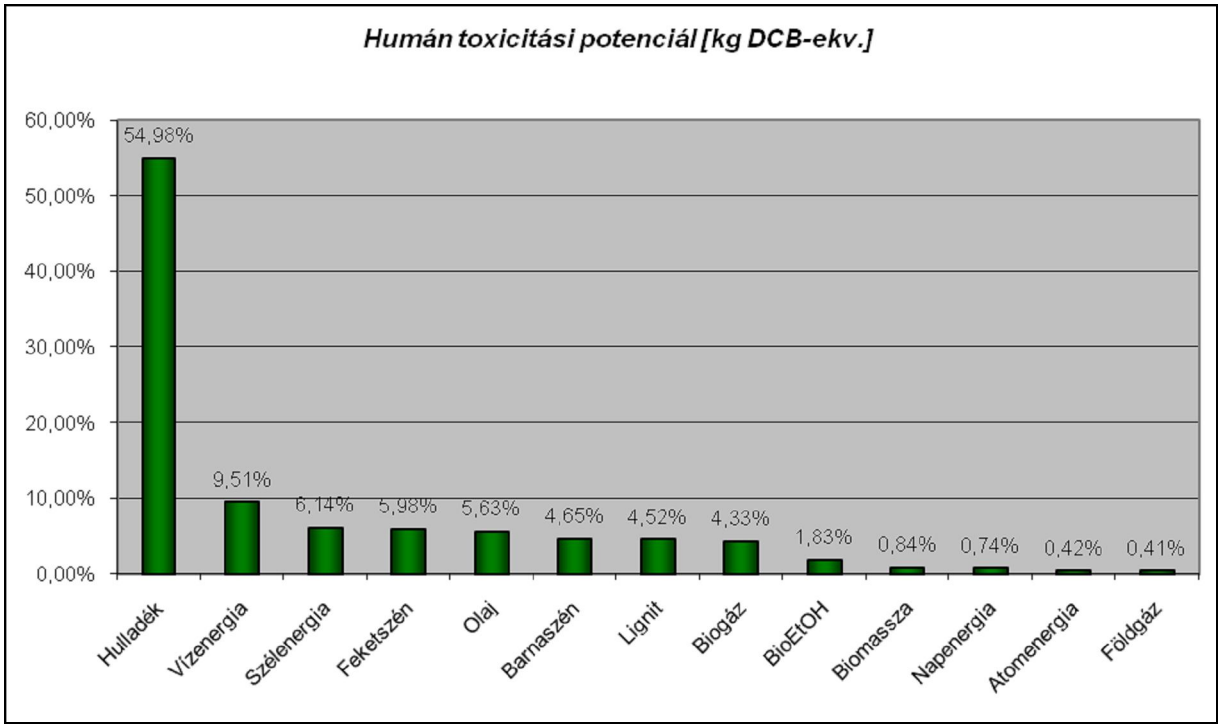
A 3. ábrán látható, hogy a legnagyobb értékek a hulladéktüzelés és a fosszilis tüzelőanyagokra alapuló termelési módoknál jelennek meg. A földgáz kivételével a hatásért döntő mértékben az erőműből származó, az égetés során keletkező szén-dioxid felelős és kisebb mértékben a metán és más szénhidrogének. A földgáz esetében a metán jelenik meg nagyobb mértékben, mely a földgáz kitermeléskor kerül a légtérbe. [3]

Az indikátorok szerinti rendezésben a globális felmelegedési potenciál indikátort leválasztva láthatóbbá válik a többi indikátor mértéke.



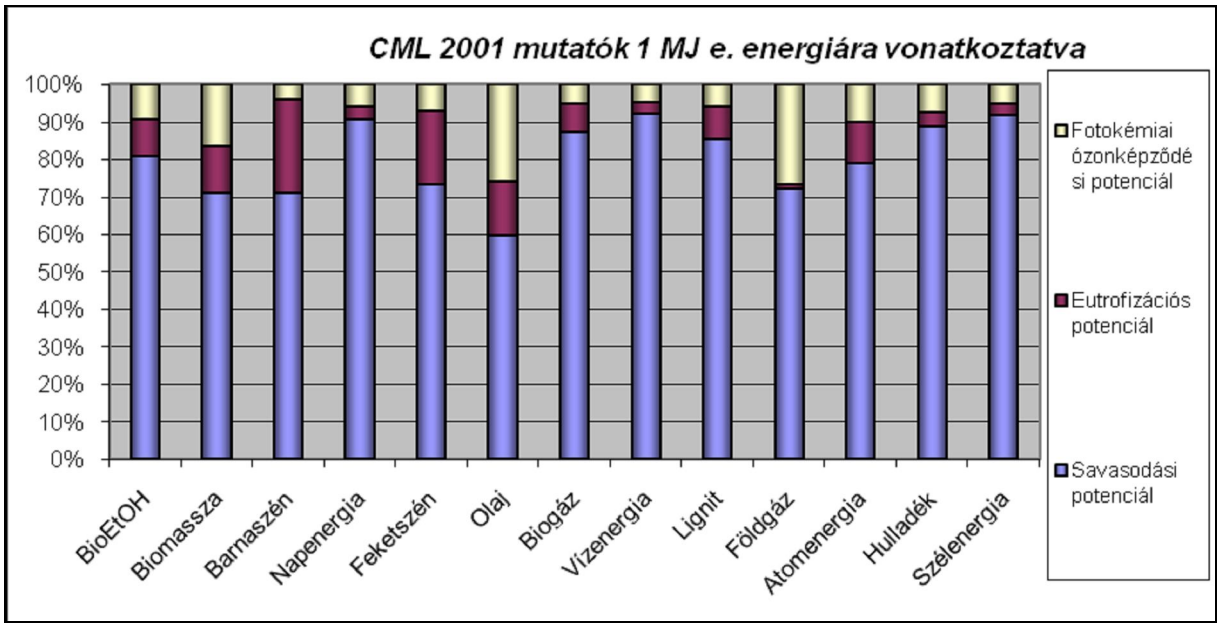
4. ábra. *A különböző termelési módok környezetei hatásai, a globális felmelegedési potenciál nélkül, indikátorok szerinti rendezésben. Forrás: [3]*

A 4. ábra szerint a globális felmelegedési potenciált követően a humán toxicitási potenciál mutatkozik a második legdominánsabb hatásnak. Elsősorban a légköri-, többek közt a nehézfém emissziók okozzák. A hatás a hulladéktüzelés esetén mutatkozik a legmagasabbnak (lásd 5. ábra) a nehézfém, dioxin származékok, hidrogén-klorid és hidrogén-fluorid kibocsátása miatt. Az atomenergiánál és a fosszilis tüzelőanyagokra alapozódó termelési módoknál ez a hatás a bányászatból származik. [3]



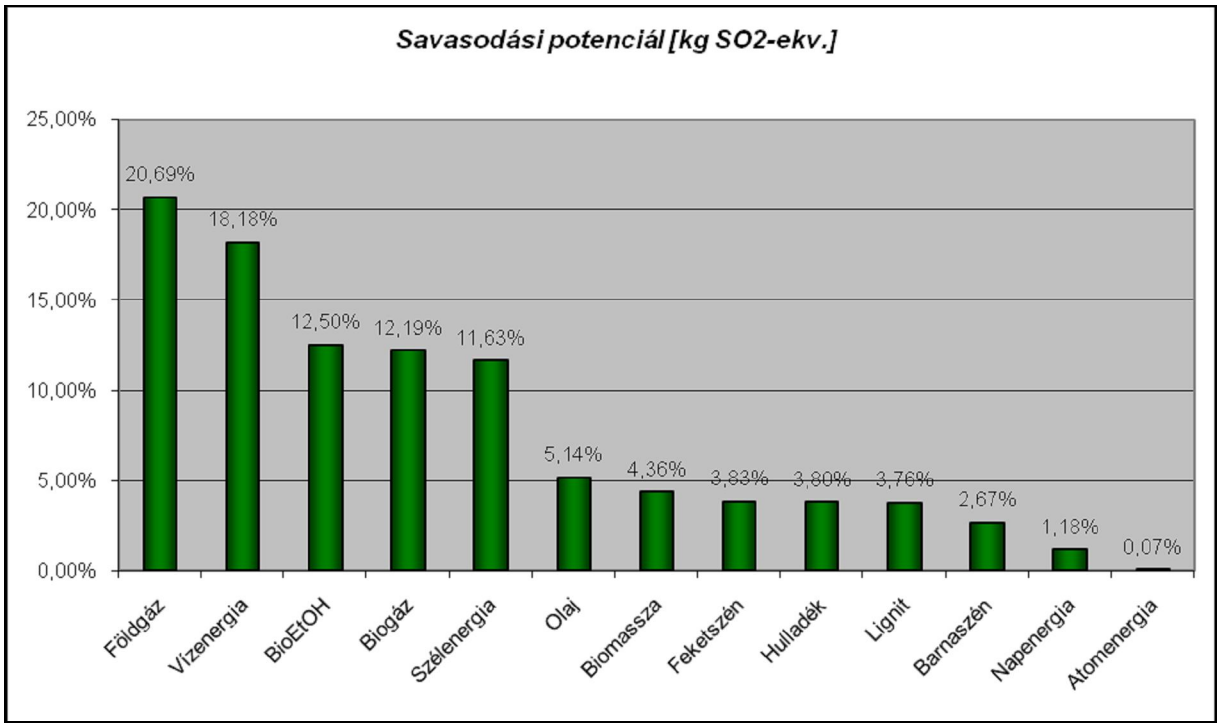
5. ábra. *A humán toxicitási potenciál összehasonlítása. Forrás [3]*

A humán toxicitási potenciált is leválasztva a savasodási potenciál jelenik meg, mint a harmadik legdominánsabb tényező. (Lásd 6. ábra) [3]



***6. ábra**. A különböző termelési módok környezetei hatásai, a globális felmelegedési potenciál és a humán toxicitási potenciál nélkül, indikátorok szerinti rendezésben. Forrás: [3]*

A savasodási potenciál a földgáz esetén a legnagyobb, oka hidrogén-szulfid kibocsátás, ami a bányászatnál és szállításnál fellépő veszteségből adódik. Megjelenik még a nitrogén-oxidok kibocsátása, mely a szállítás energiafelhasználásából, a gázbányászatból és gázégetésből származik; valamint a kén-dioxid kibocsátás, mely döntő mértékben a gázbányászatból származik. A megújulóknál a szél és vízenergia esetén az építés folyamataiból (váz és alapépítés, betongyártás, acélgyártás) származó kén-dioxid a meghatározó. Megjelenik még a betongyártásból származó nitrogén-oxidok és hidrogén-klorid kibocsátás is kisebb mértékben. A biogáznál a kén-dioxid kibocsátás a meghatározó, megjelenik a nitrogén-oxidok kibocsátása is, melyekért legnagyobb részt a vágóhídi maradék rothasztásának folyamata felelős magas energiaigénye miatt. Megjelenik továbbá a kénhidrogén és ammónia kibocsátás, melyek a kukoricatermesztésben felhasznált műtrágyák gyártásakor kerülnek a légkörbe illetve a földeken végbemenő anaerob folyamatokból származnak. [3]



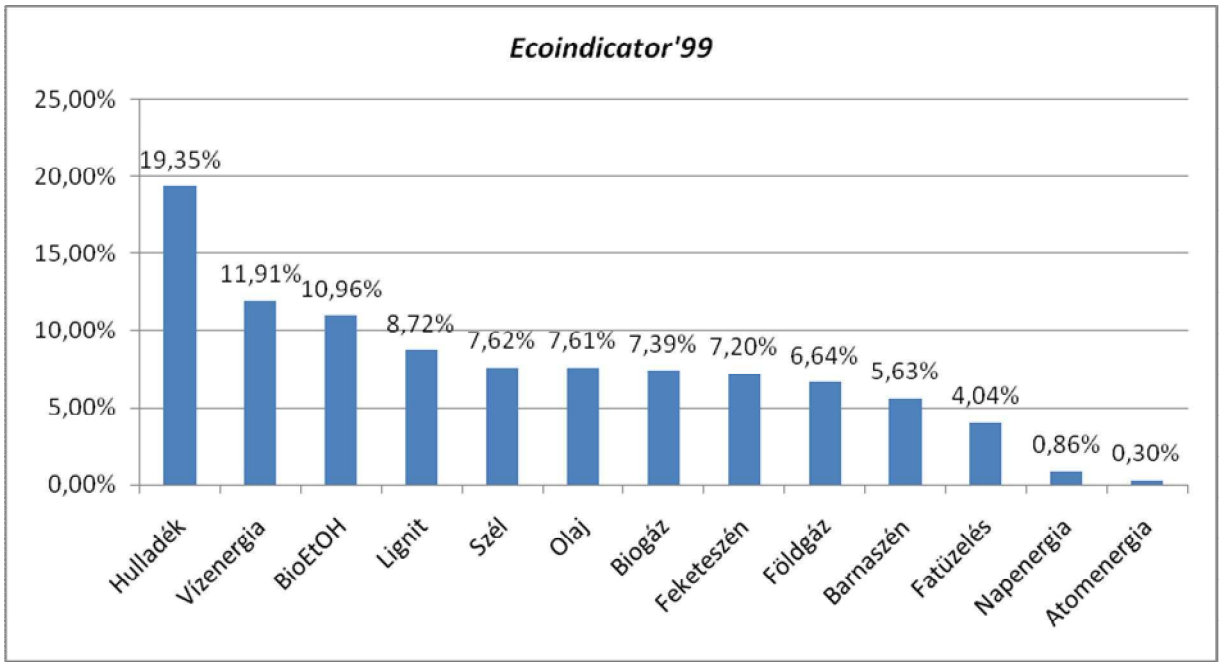
7. ábra. *A savasodási potenciál összehasonlítása. Forrás [3]*

Az eredményeket összefoglalva az egyes energiatermelési módok gyenge pontjainak a vizsgálat szerint a következőek mutatkoznak:

- A földgáz felhasználás gyenge pontja az nyersanyag kitermelés, a környezetterhelésért nagyobb részt ez a folyamat felelős.
- A többi fosszilis tüzelőanyagot felhasználó technológiák esetén az emissziók főként az energiatermelésből származnak, az üzemanyag előállításnak kisebb szerepe van a környezeti hatás kialakításában, mind a földgáznál.
- A hulladékégetés hátránya a magas humán toxicitási potenciálja.
- A biomassza savasodási, eutrofizációs és fotokémiai ózonképző potenciálja a fosszilis tüzelőanyagokéhoz hasonló, a globális felmelegedési és humán toxicitási potenciálja azoknál kedvezőbb.
- A biogáz és bioetanol savasodási, eutrofizációs, globális felmelegedési és fotokémiai ózonképző potenciálja magas a megújulókhoz képest. A főbb kibocsátások a mezőgazdasági művelésből adódnak.
- A szél és a vízenergia esetén a létesítmény építéshez használt anyagok gyártásának energiaigényessége miatt jelenik meg környezeti hatás.
- A napenergia környezeti hatása egyik hatáskategóriában sem jelenik meg értékelhető mértékben.
- Az atomenergia szintén nem jelenik meg környezetterhelőként egyik kategóriában sem. [3]

Összességében a legkedvezőbb környezeti hatást az atomenergia és a napenergia alkalmazása mutatta, emellett jó teljesítményűnek mutatkozott még a szélenergia, valamint elfogadható a földgáz a kitermelés környezeti teljesítményének javítása esetén. [3]

A különböző termelési módok környezeti hatásának egy, aggregált mutatóval történő jellemzését az ökoindikátor'99 módszer teszi lehetővé. Az értékeket a 8. ábra mutatja be.



***8. ábra**. Az egyes termelési módok EI'99 értékei. Forrás [3] alapján szerkesztve.*

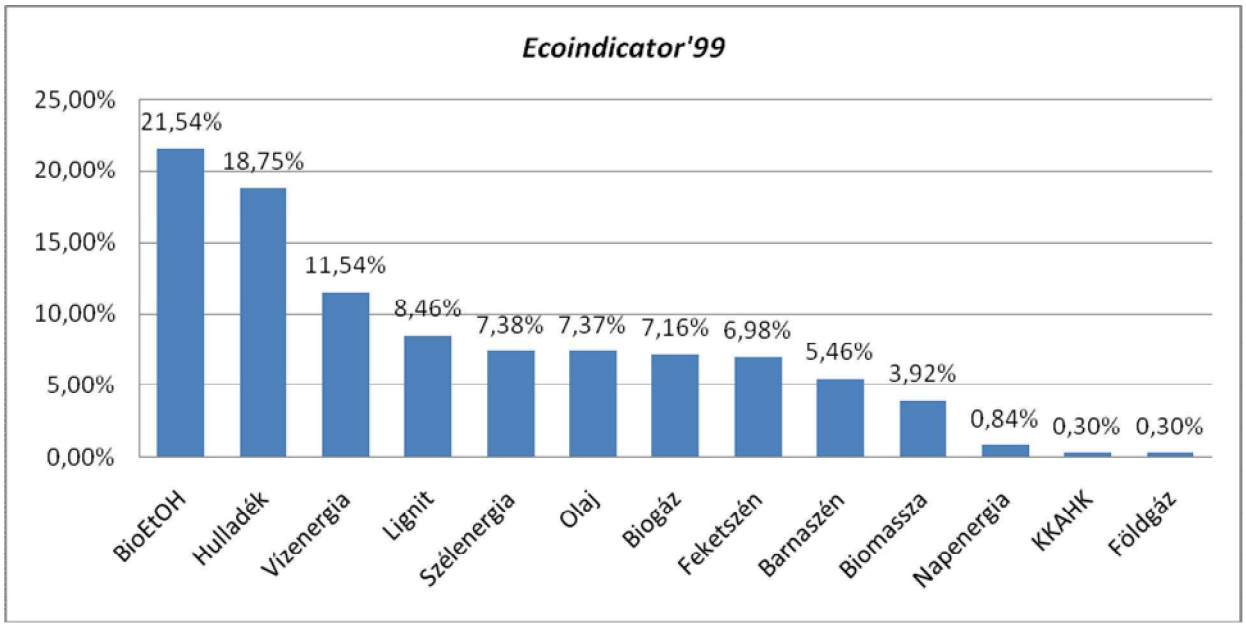
A hulladéktüzelés mutatkozik a legszennyezőbb termelési módnak. Ezt követi a vízenergia és a bioetanol, majd a fosszilis tüzelőanyagok. Legkedvezőbbek az atomenergia, a napenergia és a fatüzelés. A fosszilis tüzelőanyagok közel azonos értéket képviselnek, megjegyzendő, hogy a vizsgálatnál nem vették figyelembe a kapcsolt villamosenergia termelésnél termelt hőenergiát, csak a villamosenergia termelést. A termelt hőenergia figyelembe vétele javíthat ezen technológiák megítélésén. A vízenergia viszonylag kedvezőtlen teljesítménye a nagytömegű építőanyag felhasználásból adódik. A bioetanol környezeti terhelése főleg a mezőgazdaság környezeti hatásaiból adódik. [3]

Megjegyzendő, hogy az atomenergia esetén 4 különböző forgatókönyvet vizsgáltak:

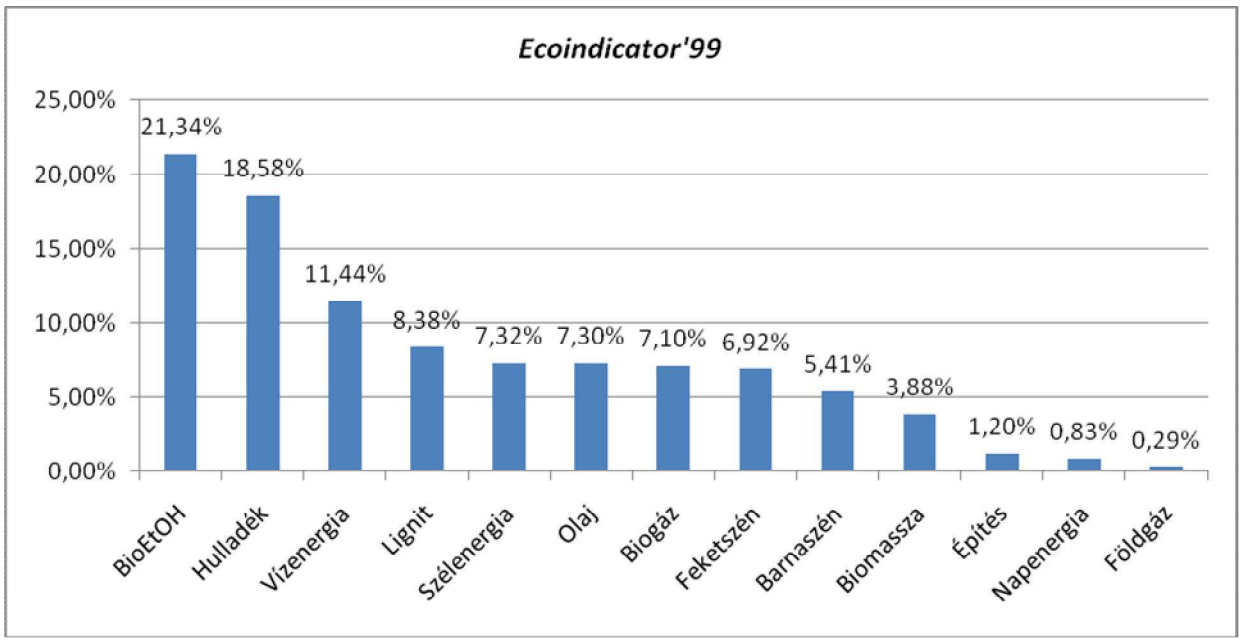
1. Az első forgatókönyv az üzemanyag előállítás és a villamosenergia termelés folyamatait veszi figyelembe az uránérc kibányászástól az energia termelésig.
2. A második forgatókönyv emellett figyelembe veszi a kis és közepes aktivitású hulladékok kezelésének folyamatait.
3. A harmadik forgatókönyv a fentieket kibővíti az atomerőmű építés és felhagyás folyamatival.
4. A negyedik forgatókönyv a harmadik forgatókönyv kiterjesztett változata, melyben az erőmű 20 éves élettartam hosszabbítását építik be a vizsgálatba. A negyedik forgatókönyv adatai - az élettartam kivételével - lényegében megegyeznek a harmadikkal. [3]

A fentiekben bemutatottak az atomenergia esetében az 1. forgatókönyv szerinti adatokat tartalmazzák, de érdemes a másik két forgatókönyv adatai szerinti összehasonlítást is megvizsgálni.

A 2. és 3. forgatókönyvvel kapott adatokat az 1. függelékben található 3. és 4. táblázat mutatja be illetve a 9. és 10. ábra szemlélteti. Fontos megjegyezni, hogy a hulladékkezelés és építés folyamatait nem vették figyelembe sem a fosszilis tüzelőanyagot használó energiatermelési módok, sem a biomasszát, biogázt és bioetanolt hasznosító termelési módok környezeti hatásának vizsgálatánál [3].



***9. ábra**. Az atomenergia 2. forgatókönyvének (KKAHK) összehasonlítása a többi energiatermelési módszerrel az EI'99 értékek alapján. Forrás [3]*



***10. ábra.** Az atomenergia 3. forgatókönyvének (Építés) összehasonlítása a többi energiatermelési módszerrel az EI'99 értékek alapján. Forrás [3]*

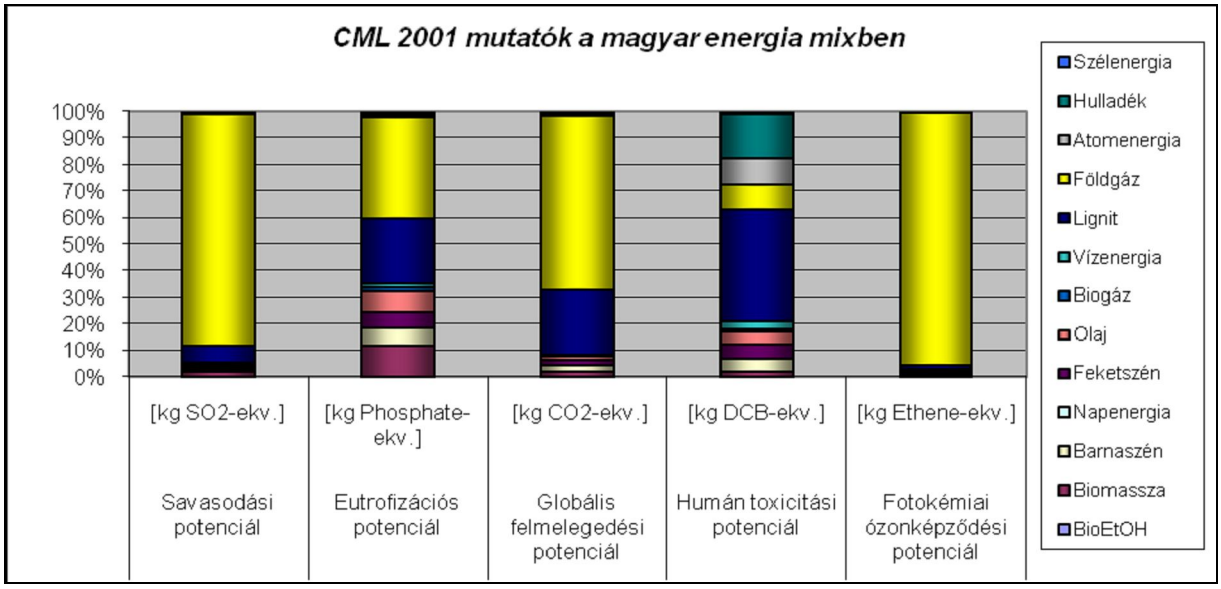
Az összesített EI'99 mutató alapján az atomenergia mindkét kibővített forgatókönyv esetén valamennyivel rosszabb helyezést kap, de még így is jóval kedvezőbb értéket mutat a termelési módok zöménél.

A következőekben bemutatásra kerülő összehasonlításnál az egyes energiatermelési módokat az energiamixben (2. táblázat) betöltött arányukban vették figyelembe és az ekkor fellépő környezeti hatást vizsgálták és hasonlították össze. A CML 2001 módszer mutatóinak alakulását a 11. ábra mutatja.

Energiatermelő egység	Megoszlás [%]
Földgáz	37,9
Atomenergia	36,8
Lignit	15,2
Fatüzelés	3,7
Barnaszén	1,8
Olaj	1,5
Feketeszén	1,4
Vízenergia	0,5
Hulladék	0,5
Biogáz	0,4
Szél	0,3
BioEtOH	0
Napenergia	0

***2. számú táblázat**. A különböző energiatermelési módok megoszlása a magyar energiamixben. Forrás [3]*

A legnagyobb arányban a földgáz, az atomenergia és a lignit tüzelés szerepel, együttesen a teljes termelés 89,9%-át teszik ki. Alapvetően azt várhatnánk, hogy a környezeti hatások között is e három termelési mód jelenik majd meg dominánsan.

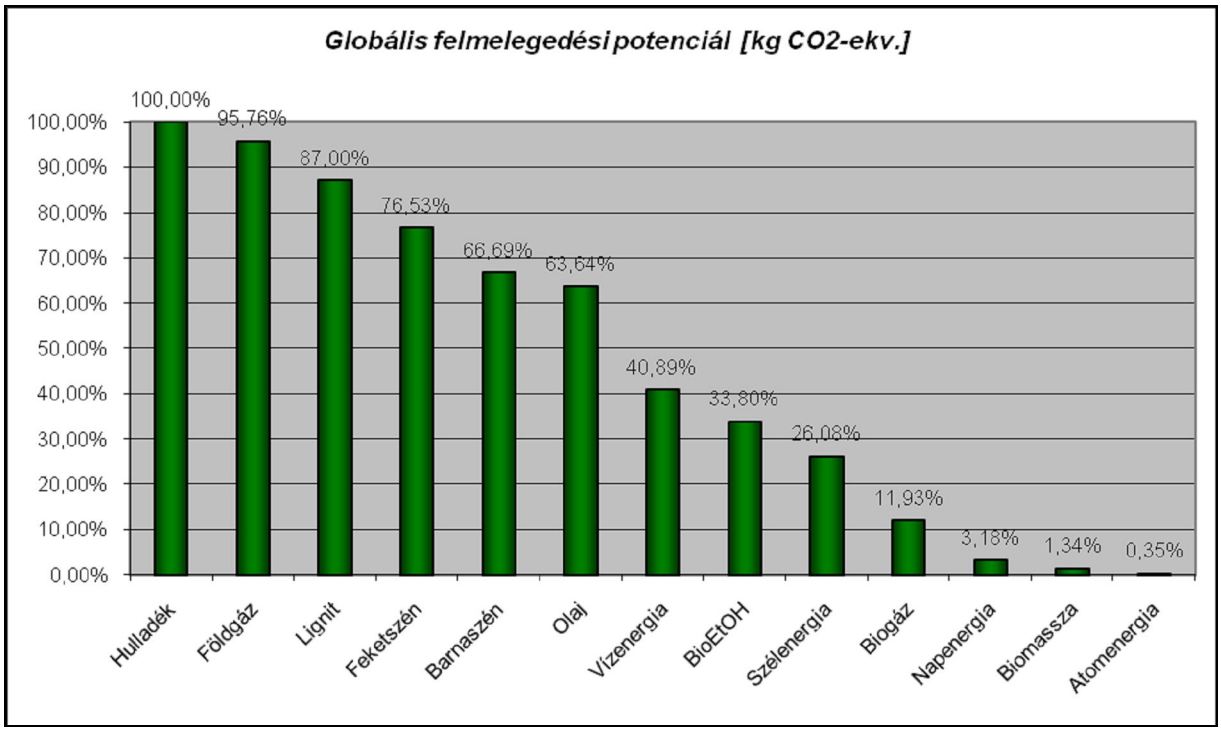


***11. ábra**. A magyar energiamix szerinti megoszlás környezeti mutatói. Forrás [3].*

A savasodási potenciál alakulásában a földgáztüzelés (35%) és a lignittüzelés (15%) a legjelentősebb hatású. Az eutrofizációs potenciál alakulásában a földgáz és a lignit mellett a többi fosszilis tüzelőanyag és a biomassza hatása is megjelenik. A globális felmelegedési potenciálban szintén a földgáz a legmagasabb hatású, az energiamixben képviselt magas részaránya miatt, mellette megjelenik a többi fosszilis tüzelőanyag is. A humán toxicitási potenciál alakulásában a legnagyobb hatást a lignit és a hulladéktüzelés mutatja, de megjelenik csaknem valamennyi termelési mód hatása; az atomenergia és a földgáz hozzájárulása közel azonos mértékű. A fotokémiai ózonképződési potenciálban láthatóan a földgáztüzelés dominál. [3]

Összességében elmondható, hogy legnagyobb környezeti hatást a földgáz és a lignit tüzelés mutatja, ami összhangban van azzal, hogy mindkettő az energiamixben viszonylag nagy százalékban szerepel. A földgáz valamennyi kategóriában megjelenik többnyire elég magas aránnyal járul hozzá a környezeti hatáshoz. A lignit egy kivételével az összes hatáskategóriában megjelenik, többnyire közepesen magas hozzájárulással. A legkedvezőbbnek az atomenergia mutatkozik: az energiamixben elfoglalt második helye ellenére, csak a humán toxicitási potenciál hatáskategóriában jelenik meg értékelhető hozzájárulással. [3]

A mutatók közül itt most csak a globális felmelegedési potenciál indikátorát ragadjuk ki és mutatjuk be arányát az egyes termelési módok esetén a 12. ábrán.



***12. ábra**. Globális felmelegedési potenciálok összevetése az energiamixben*

A hulladék, földgáz és lignittüzelés vezet, ezeket követei a többi fosszilis energiahordozó, legkedvezőbb hatásúak a megújulók és az atomenergia. A legmagasabb hatású hulladéktüzelést vették 100%-nak és ehhez viszonyították a többi termelési mód hatását. [3]

A KÖRNYEZETBIZTONSÁGI SZEMPONTOK MEGJELENÉSE A MAGYAR ENERGIAPOLITIKÁBAN

A különböző energiatermelési módok összehasonlítását bemutató előző fejezetben láthattuk, hogy a környezeti hatásuk szempontjából legkedvezőbb energiatermelési módok az atomenergia, a napenergia és a biomassza felhasználására épülnek. A környezetbiztonsági szempontokat is figyelembe vevő energiapolitikának tehát ezen termelési módokat célszerű előnyben részesítenie. Nézzük, hogy hogyan alakul mindez a magyar energiapolitikában.

A 2008-2020 közötti időszakra vonatkozó energiapolitikát [4] az Országgyűlés 40/2008. (IV. 17.) határozatával hagyta jóvá. Az energiapolitika elsődleges célokként az ellátásbiztonságot, a versenyképességet és a fenntarthatóságot jelöli meg. Előírja az összhangot a klíma- és az energiapolitika között és azt, hogy a gazdaság és a lakosság energiaigénye - biztonságos és gazdaságos módon – a környezetvédelmi szempontok

figyelembevételével kerüljön kielégítésre. Szorgalmazza az energiafelhasználás csökkentését, energiahatékonyság javítását, a megújuló energiaforrások arányának növelését és környezet- és természetbarát technológiák bevezetését, természetesen gazdaságossági, versenyképességi szempontok és a Magyarországon rendelkezésre álló természeti adottságok figyelembe vételével.

Az energiapolitika nem veti el az atomenergia alkalmazásának lehetőségét, a határozatban az Országgyűlés felkéri a Kormányt új atomerőművi kapacitások létrehozására vonatkozó döntés előkészítő munka megkezdésére; a szakmai, környezetvédelmi és társadalmi megalapozás elvégzésére valamint a beruházás szükségességére, feltételeire, az erőmű típusára és telepítésére vonatkozó javaslat előterjesztésére. Emellett a nukleáris hulladékok végleges elhelyezésére irányuló programok megvalósításához szükséges feltételek biztosítására.

Az energiapolitika támogatja a megújuló energiaforrások alkalmazásának növelését is, a határozatban az Országgyűlés felkéri a Kormányt a megújulók alkalmazása növelésére vonatkozó stratégia kidolgozására. Olyan stratégia kidolgozására, mely megfelel a legkisebb költség és környezeti fenntarthatóság elvének, összhangban áll az Európai Unió célkitűzéseivel és hozzájárul az üvegházhatású gáz kibocsátás csökkentési célok megvalósításához.

Az EU a megújuló energiaforrások 2020-ra elérendő részarányát EU szinten 20%-ban határozza meg. Erről az Európai Tanács 2007. márciusi ülésén határozott. A tagállamok szintjére lebontott elvárásokat az Európai Parlament és Tanács 2008. január 30-án megjelent, a megújuló energiahordozók támogatásáról szóló irányelv javaslata határozza meg. Magyarország felé az elvárás a megújulók részarányának 13%-ra történő emelése 2020-ig.

Az EU elvárásoknak történő megfelelés elősegítése érdekében a Kormány 2008. szeptember 3.-án elfogadta a „Stratégia a magyarországi megújuló energiaforrások felhasználásának növelésére 2008 – 2020” című KHEM előterjesztést. A stratégiai célkitűzés („policy” szkenárió) szerint a villamosenergia termelésben a megújuló energiából termelt villamosenergia mennyiségét a 2006. évi 1,63 TWh-ról 2020-ra 9,47 TWh-ra kell növelni. A tervezett megújuló energiának három fő eleme van: a szélenergia, a biomassza és a geotermikus energia. [5]

Az előző fejezetben ismertetett kutatási összefoglaló jelentés értelmében a biomassza (fatüzelés) a három legkedvezőbb környezeti mutatóval (lásd 8. ábra) rendelkező termelési mód között van. A szélenergia a közepes értékkel rendelkezik, a geotermikus energiát a bemutatott kutatás keretei között nem vizsgálták.

A jelen közleményben megjelentetett információ alapján azt mondhatjuk, hogy a magyar energiapolitika a környezetbiztonsági szempontokkal összhangban van. A megújuló stratégiában megcélzott fő termelési módok (szélenergia, biomassza, geotermikus energia) csak részben igazodnak a környezeti teljesítmények értékeihez, de ez érthető is, hiszen a stratégiában a környezetvédelmi szempontok mellett más szempontokat - pl. az egyes energiahordozók hazai adottságait, rendelkezésre állását és felhasználásának lehetőségét - is figyelembe kell venni.

ÖSSZEFOGLALÁS

A 21. századi modern lét alapvető kelléke a villamosenergia. A társadalom és a gazdaság villamosenergia igénye globálisan - az energiahatékonysági, energiatakarékossági programok mellett is – jelenleg folyamatosan nő. A termelés növelésével számolni kell a termelés környezeti hatásainak egyre erősebb megjelenésével is. Napjainkban a legnagyobb hangsúlyt a globális klímaváltozás kapja, melyet az üvegházhatású gázok légkörben való felszaporodására vezetnek vissza, de más, a légkör, a talaj a vízi környezet szennyezésével, az

épített környezet és az élővilág károsításával járó hatással is számolni kell. A különböző elsődleges energiaforrásokon és technológiákon alapuló termelés környezeti hatásai között jelentős eltérések lehetnek. Mindezek okán a környezetbiztonsági szempontokat figyelembe vevő energiapolitikának a legkedvezőbb környezeti hatású termelési módokat kell támogatnia, természetesen az egyéb – gazdaságossági, versenyképességi, fenntarthatósági – szempontok figyelembe vétele mellett.

Az egyes villamosenergia termelési módok környezeti hatásának összehasonlítására alkalmazható az ún. az életciklus elemzés módszer. 2009.-ben jelent meg egy, a magyar energiaszektor villamosenergia termelésének életciklus elemzését, az alkalmazott energiatermelési módok összehasonlítását célzó vizsgálatról készített összefoglaló kutatási jelentés [3]. A kutatás során a Magyarországon alkalmazott villamosenergia termelési technológiák LCA modelljét készítették el, vizsgálták és hasonlították össze. A kiértékelésnél az ún. EcoIndicator'99 és a CML 2001-es módszert használták.

A vizsgálat során meghatározták az egyes – Magyarországon alkalmazott – villamosenergia termelési módok környezeti hatás szempontjából vett gyenge pontjait. Azt vizsgálták, hogy az egyes termelési módok esetén melyek a hátrányos környezeti hatások és milyen folyamat felelős ezekért. Ezen gyengepont analízis során azt állapították meg, hogy a legkedvezőbb környezeti hatással az atomenergia és a napenergia bír, de jó teljesítményűnek mutatkozik a szélenergia is és a kitermelés környezeti teljesítményének javítása esetén elfogadható a földgáz is.

A környezeti hatások összehasonlító vizsgálatát elvégezték a magyar energia mixből – azaz az egyes termelési módok termelésben betöltött valóságos megoszlásából – kiindulva is, így a környezeti hatásokat a valós kibocsátások arányában hasonlították össze. Az eredmények azt mutatták, hogy a legerősebb környezeti hatással a földgáztüzelés jelentkezik, mely az energiamixben a legnagyobb arányban vesz részt. Környezeti hatása mind a hat vizsgált hatáskategóriában megjelenik. Az energiamixben harmadik helyet elfoglaló lignit tüzelés környezeti hatása szintén jelentős, egy kivételével valamennyi hatáskategóriában megjelenik. A mixben második helyet elfoglaló atomenergia környezeti hatása viszont nagyon kedvező, csupán egy hatáskategóriában jelenik meg.

A különböző termelési módok üvegházhatású gáz kibocsátásának összehasonlítása a globális felmelegedési potenciálok mentén végezhető el. Itt a legkedvezőtlenebb a hulladék, a földgáz és a lignit tüzelés. Ezeket követi a többi fosszilis energiahordozón alapuló termelés, a legkedvezőbbek az atomenergia és a megújuló energiaforrásokon alapuló termelési módok.

Végül megvizsgáltuk, hogy mennyire jutnak érvényre a magyar energiapolitikában a fenti elvek. A jelen közleményben szereplő információ alapján azt mondhatjuk, hogy a magyar energiapolitika ezekkel jó összhangot mutat: előírja az energia- és klímapolitika összhangját, támogatja a megújulók és az atomenergia használatát. A megújulók részarányának növelését célzó stratégia elsősorban a szélenergia, a biomassza és a geotermikus energia felhasználásának növelésére épít. A biomassza (fatüzelés) az egyik legkedvezőbb környezeti mutatóval rendelkezik a bemutatott kutatási jelentés szerint, a szélenergia közepesen jó értéket kapott, a geotermikus energiát a kutatás nem vizsgálta. A stratégia által preferált energiatermelési módok nem esnek teljesen egybe a legkedvezőbb környezeti hatású módokkal a megújulókon belül, de ez érthető is, hiszen a stratégiában a környezeti hatás mellett más szempontokat - pl. az egyes energiahordozók hazai adottságait, rendelkezésre állását és felhasználásának lehetőségét - is figyelembe kell venni.

Irodalomjegyzék

[1] Dr. Fazekas András István: 6. Villamosenergia termelési technológiák összehasonlítása. A komplex összehasonlítás szempontrendszere. Magyar Atomfórum Egyesület. 2005. január http://www.atomforum.hu/pdf/06%20villamosenergiatermeles%20tech%20osszehasonlitas.pdf (2009.12.15)

[2] Oktatási segédanyag a Környezetgazdaságtan című tantárgyhoz. Összeállította: dr. Tóthné Szita Klára. Miskolci Egyetem. 2003. http://www.uni-miskolc.hu/~euint/20031002zzz20031231/kornyoktseg1_2003lev.pdf (2009.12.15)

[3] Green Capital Zrt.: A magyar energia szektor villamosenergia-termelésének életciklus-, és „carbon footprint" elemzése. Budapest. 2009. http://www.greencapital.hu/dokumentumok/LCA_villeneregia_GreenCapital_osszefoglalas.pdf (2010.01.07)

[4] 40/2008. (IV. 17.) OGY határozat a 2008-2020 közötti időszakra vonatkozó energiapolitikáról. http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=A08H0040.OGY (2010.01.10)

[5] Körmendi Krisztina, Solymosi József: A villamosenergia termelés környezetre gyakorolt hatása, a szén-dioxid kibocsátással nem járó villamosenergia termelés lehetőségei és korlátai. Hadmérnök. IV. Évfolyam 3. szám. 2009. szeptember http://www.hadmernok.hu/2009_3_kormendi.pdf (2010.01.20)

I. számú függelék: Az atomenergia kibővített forgatókönyv eredményeinek összehasonlítása a többi energiatermelési mód eredményeivel

		KKAHK	BioEtOH	Biomassza	Barnaszén	Napenergia	Feketszén	Olaj	Biogáz	Vízenergia	Lignit	Földgáz	Hulladék	Szélenergia
Savasodási potenciál	[kg SO2-ekv.]	0,08%	12,40%	4,33%	2,65%	1,17%	3,80%	5,10%	12,92%	18,04%	3,73%	20,49%	3,77%	11,53%
Eutrofizációs potenciál	[kg Phosphate-ekv.]	0,12%	17,82%	9,18%	11,03%	0,49%	12,44%	14,77%	13,63%	6,77%	4,68%	2,86%	1,88%	4,32%
Globális felmelegedési potenciál	[kg CO2-ekv.]	0,06%	5,44%	0,22%	10,75%	0,51%	12,34%	10,26%	4,10%	6,59%	14,02%	15,38%	16,12%	4,20%
Humán toxicitási potenciál	[kg DCB-ekv.]	0,43%	1,83%	0,84%	4,65%	0,73%	5,98%	5,63%	4,41%	9,51%	4,52%	0,41%	54,93%	6,14%
Fotokémiai ózonképződési potenciál	[kg Ethene-ekv.]	0,06%	9,05%	6,26%	0,99%	0,49%	2,26%	13,83%	5,25%	6,16%	1,64%	47,90%	2,01%	4,10%
EI '99		0,30%	21,54%	3,92%	5,46%	0,84%	6,98%	7,37%	7,16%	11,54%	8,46%	0,30%	18,75%	7,38%

1. táblázat: Az atomenergia 2. forgatókönyv eredményeinek összehasonlítása a többi energiatermelési mód eredményeivel

		Építés	BioEtOH	Biomassza	Barnaszén	Napenergia	Feketszén	Olaj	Biogáz	Vízenergia	Lignit	Földgáz	Hulladék	Szélenergia
Savasodási potenciál	[kg SO2-ekv.]	1,49%	12,22%	4,26%	2,61%	1,15%	3,75%	5,03%	12,73%	17,78%	3,68%	20,20%	3,72%	11,37%
Eutrofizációs potenciál	[kg Phosphate-ekv.]	0,65%	17,73%	9,13%	10,97%	0,49%	12,37%	14,70%	13,56%	6,74%	4,65%	2,85%	1,87%	4,29%
Globális felmelegedési potenciál	[kg CO2-ekv.]	0,58%	5,42%	0,21%	10,69%	0,51%	12,27%	10,21%	4,08%	6,56%	13,95%	15,30%	16,04%	4,18%
Humán toxicitási potenciál	[kg DCB-ekv.]	1,22%	1,82%	0,84%	4,61%	0,73%	5,93%	5,58%	4,38%	9,43%	4,48%	0,40%	54,50%	6,09%
Fotokémiai ózonképződési potenciál	[kg Ethene-ekv.]	0,54%	9,01%	6,23%	0,98%	0,49%	2,25%	13,76%	5,22%	6,13%	1,63%	47,67%	2,00%	4,08%
EI '99		1,20%	21,34%	3,88%	5,41%	0,83%	6,92%	7,30%	7,10%	11,44%	8,38%	0,29%	18,58%	7,32%

2. táblázat: Az atomenergia 2. forgatókönyv eredményeinek összehasonlítása a többi energiatermelési mód eredményeivel

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Pellérdi Rezső
pellerdi.rezso@zmne.hu

Pete Dóra
pete.dori@gmail.com

AZ A/H1N1- INFLUENZA PANDÉMIA KATASZTRÓFAVÉDELMI ASPEKTUSAI

Absztrakt

A világ globalizációjának következtében egyre nagyobb a veszélye annak, hogy a lokális influenza járványokból könnyen világméretű humán katasztrófa válik. A nagyméretű terjedés megakadályozására az egyes országoknak jól felépített és határozott válaszokat kell adnia.
A cikk bemutatja az A/H1N1 influenza pandémia jellemzőit, kialakulásának, terjedésének körülményeit, elemzi a Magyarországra gyakorolt hatását és kiemeli a nemzetközi és a magyar egészségügyi, katasztrófavédelmi szervek és a Magyar Honvédség együttműködésének, közös helyzetértékelésének valamint az egységes beavatkozásnak a fontosságát

In the result of the world's globalisation the danger is increasingly bigger that the local flu epidemics can easily transform into worldwide human catastrophe. Onto preventing of the large spread the countries have to give well developed and determined answers.
The article presents the features, the circumstances of the development and spread of A/H1N1 flu pandemic, analyses the effect has on Hungary and emphasizes the importance of the cooperation, common situation evaluation and the uniform intervention of the international and Hungarian medical, disaster management organs and the Hungarian Armed Forces.

Kulcsszavak: *globalizáció, influenza, pandémia, katasztrófavédelem ~ globalisation, flu, pandemic, disaster management*

BEVEZETÉS

Manapság csak akkor kapjuk fel a fejünket valamilyen katasztrófa hallatára, ha a szélsőséges időjárás vagy természeti csapás hatására falvak, városok dőlnek romba és jelentős anyagi kárról, hatalmas pusztulásról, halálos áldozatokról számolnak be a hírekben. De miért nem figyelünk jobban azokra a katasztrófákra, amelyek ugyan ritkán ütik fel a fejüket, ugyanakkor veszélyességüket tekintve korántsem maradnak alul a többihez képest?

A madárinfluenza eltűnésével újból kevesebb szerepet kapott az influenzás pandémiára való felkészülés, egészen addig, amíg Mexikóban meg nem jelent egy teljesen új vírustörzs, amellyel eddig még nem találkozott az emberiség. A hatás gyors volt és kirobbanó, az új törzs virulenssége meglepő gyorsasággal fejlődött, így viszonylag kevés időbe telt, amíg a vírus elérte azt a szintet, hogy képes legyen emberről emberre terjedni. A gyors terjedésen kívül aggodalomra adott okot az is, hogy nem várt mennyiségű haláleset is történt. Így elkerülhetetlen volt, hogy a média segítségével ne ezzel foglakozzunk, szinte az egész világon.

A cikk megírását az inspirálta, hogy feltárjuk a pandémia megelőzésével kapcsolatos cselekvési rendszert, annak szükségességét és elégségességét.

A probléma gyökere az, hogy az elmúlt 100 év pandémia katasztrófái bebizonyították, hogy az emberiség nem készült fel az ilyen veszélyek elhárítására, kezelésére. Kérdéses, jelenleg van-e valami lehetőség még az emberiség birtokában, ami meggátolja a terjedést az ilyen világjárványok esetében, vagy vagyunk-e már annyira felkészültek, hogy el tudjunk hárítani egy ilyen humán katasztrófa bekövetkezését?

1. TÖRTÉNETI ÁTTEKINTÉS

Az influenza vírus okozta ragályos, heveny légúti tünetekkel járó betegség már az ősidők óta fenyegeti az emberiséget. Sok leírás maradt meg arról a jelenségről, miszerint egy- egy földrajzi területen tömegesen előforduló, súlyos lefolyású, magas lázzal járó megbetegedéseket észleltek. Ezek a járványok amilyen gyorsan kialakultak, olyan gyorsan be is fejeződtek. Az első erről szóló írásos emlékek i.e. 412-ből, Hippokratésztól maradtak fenn.

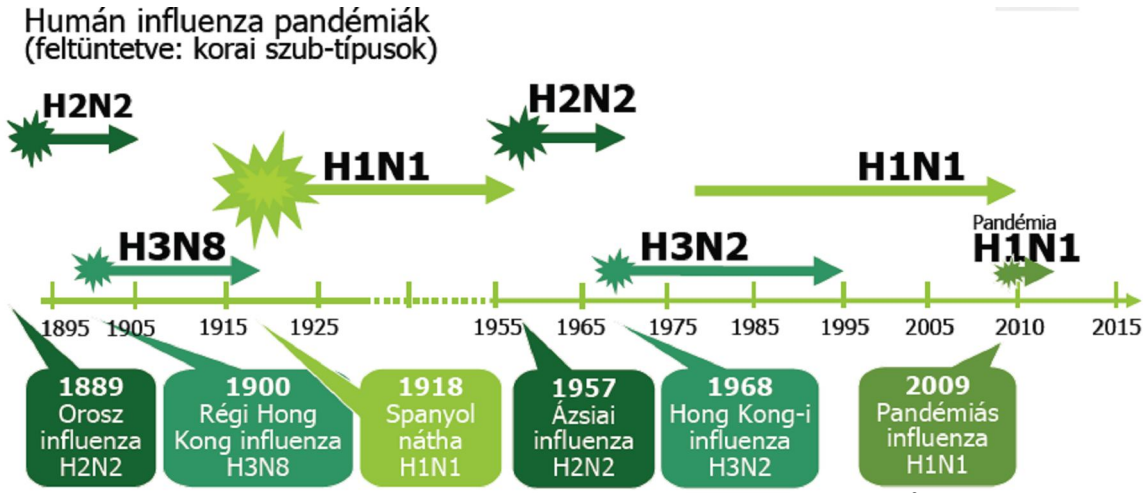
Két kutató- Webster és Hirsch- áttanulmányozta az 1500-as és 1850-es évek között született krónikákat, olyan leírásokat keresve, amelyben légúti megbetegedésekkel kapcsolatos járványokat említenek. A feltárt iratokból felismert törvényszerűségek szerint a járványok viszonylag gyakran jelentkeztek, de két járvány között a betegség szinte teljesen eltűnt. Megfigyelhető volt továbbá az is, hogy a tömeges méretű fertőzések nem voltak egyformán súlyosak, de jellemző módon a halálozás a hatvan év felettiek körében jóval magasabb volt, mint a fiatalok körében. Ám a „Spanyolnátha” minden addigi járványnál több áldozatot követelt.

1.1. A spanyolnátha

Az 1918 márciusától 1920 májusáig tartó, a történelem ilyen rövid idő alatt legpusztítóbbnak tartott járványában: világszerte 50-100 millió embert halt meg. A vírus azért volt olyan pusztító, mert az emberi szervezetben az immunrendszer túlzott reakcióját váltotta ki, az úgynevezett citokin[1] vihart. Az immunrendszer citokinok tömegét bocsátotta a tüdő szöveteibe, emiatt fehérvérsejtek özönlöttek oda, károsítva a tüdőszöveteket és vizenyőt

[1] Citokin: a jelzőmolekulák egy fajtája, amely a sejtkommunikációban játszik alapvető szerepet
Forrás: http://www.nyf.hu/others/html/biologia_intezet_elemei/immunologia/citokinek_citokinreceptorok.ppt.
Letöltés: 2009. október 23.

okozva, ami megakadályozta a légzést. Más világjárványoktól eltérően, amelyek főképp az öregekkel és a gyerekekkel végeztek, a spanyolnátha nagy számban végzett fiatal felnőttekkel, akiknek erős volt az immunrendszere és ezért erős védekező reakciót produkált. A járvány azért kapta a spanyolnátha nevet, mert Spanyolország volt az egyetlen semleges európai ország az első világháború idején, ahol nem cenzúrázták a járványról szóló híreket és az áldozatokról folyamatosan jelentéseket közöltek, miközben más országokban ezt nem engedték szerepelni a hírekben, hogy megelőzzék a pánikot. Az a vírustörzs, ami ezt a járványt okozta Kínából került az Egyesült Államokba, majd Európába, onnan már az egész világon elterjedt, főként a gyarmatok révén.



1. ábra. Influenza pandémiák 1889-től napjainkig[2]

1.2. A pandémia meghatározása

Pandémiának a világjárványokat nevezzük. Influenza pandémiáról akkor beszélünk, amikor szinte minden földrészen pusztít az influenzavírus. Mivel a vírus antigénjeiben rendkívül változatos, így időszakonként újabb és újabb variánsok bukkannak fel, amelyek ellen a lakosság nagy része nem védett, még nem alakult ki ellenük a szervezet saját védekező rendszere, így rendkívül fertőzőképesek. Pandémiáról akkor beszélhetünk, ha egy ilyen vírus jelenik meg – amely ellen az emberek többsége védtelen, nincs ellene oltóanyag sem –, és amely komoly megbetegedést okoz, valamint rendkívül gyorsan terjed országról országra, egyik földrészről a másikra.

1.3. Pandémia szakaszai

A világjárványok lezajlásának időszakait az Egészségügyi Világszervezet különböző fázisokra osztotta. Az egyes időszakok jellemzői eltérőek egymástól, és eltérő cselekvési tervet kívánnak meg. Ez a fázisfelosztás adja minden ország számára a pandémiára való felkészülés alapjait.

[2] Forrás: Dr. Csohán Ágnes: Az új influenzavírus tapasztalataink és feladataink, 2. o.

WHO fázisbeosztás[3]			
Inter-pandémiás időszak			
1. fázis	Emberből nem mutattak ki új influenzavírus altípust. Olyan influenzavírus altípus, amely már okozott emberi megbetegedést, előfordulhat állatokban, ám ha jelen is van azokban, az ember fertőződésének/megbetegedésének kockázata alacsony.		
2. fázis	Emberből nem mutattak ki új influenzavírus altípust, azonban a cirkuláló állati influenzavírus altípus komoly megbetegedési kockázatot jelent az ember számára		
Pandémiás riasztás időszaka			
3. fázis	Az állati influenzavírus altípus emberi fertőzéseket okoz, de a vírus emberről emberre nem terjed, legfeljebb nagyon ritkán, közeli érintkezés révén.		
4. fázis	Emberről emberre történő korlátozott terjedés következtében az emberi megbetegedések csupán kis gócokban jelentkeznek, a terjedés igen kis területre korlátozódik, ami arra utal, hogy a vírus még nem adaptálódott az emberi szervezethez.		
5. fázis	Az emberi megbetegedések nagyobb gócokban jelentkeznek, de az emberről emberre történő terjedés még mindig csak kis területre korlátozódik, ami arra utal, hogy a vírus egyre jobban adaptálódik az emberi szervezethez, de az emberre történő terjedési képessége még nem tökéletes.		
Pandémiás időszak			
6. fázis	Az új influenzavírus altípus fokozott intenzitással folyamatosan terjed a lakosság körében.	6. a.	Az új influenzavírus altípus terjedése abban az országban, ahol kialakult.
		6. b.	Az új influenzavírus altípus más országban is megjelenik
		6. c.	Az új influenzavírus altípus Európában is megjelenik
		6. d.	Az új influenzavírus altípus által okozott igazolt megbetegedések megjelenése Magyarországon.
		6. e.	Az új vírus Magyarországon regionális járványt okoz.
		6. f.	Az új vírus Magyarországon országos járványt okoz
		6. g.	A pandémia első hullámának lezajlása Magyarországon
		6. h.	A pandémia második/harmadik hulláma Magyarországon

[3] Forrás: http://www.pandemia.hu/pandemia-fo.html
Letöltés ideje: 2009. október 14.

A járványt követő időszak:
Az új vírus által okozott megbetegedések előfordulási gyakorisága a megfelelő surveillance-szel[4] rendelkező országok többségében a járvány csúcsán tapasztalt szint alá csökken.
Lehetséges következő járványhullám:
A pandémiát okozó influenza vírus által okozott megbetegedések előfordulási gyakorisága a megfelelő surveillance-szel rendelkező országok többségében újból emelkedik.
Pandémiát követő időszak:
Az influenza előfordulása a megfelelő surveillance-szel rendelkező országok többségében a szezonális influenza előfordulási gyakoriságának alapszintjére tér vissza.
Visszatérés az interpandémiás fázisba.

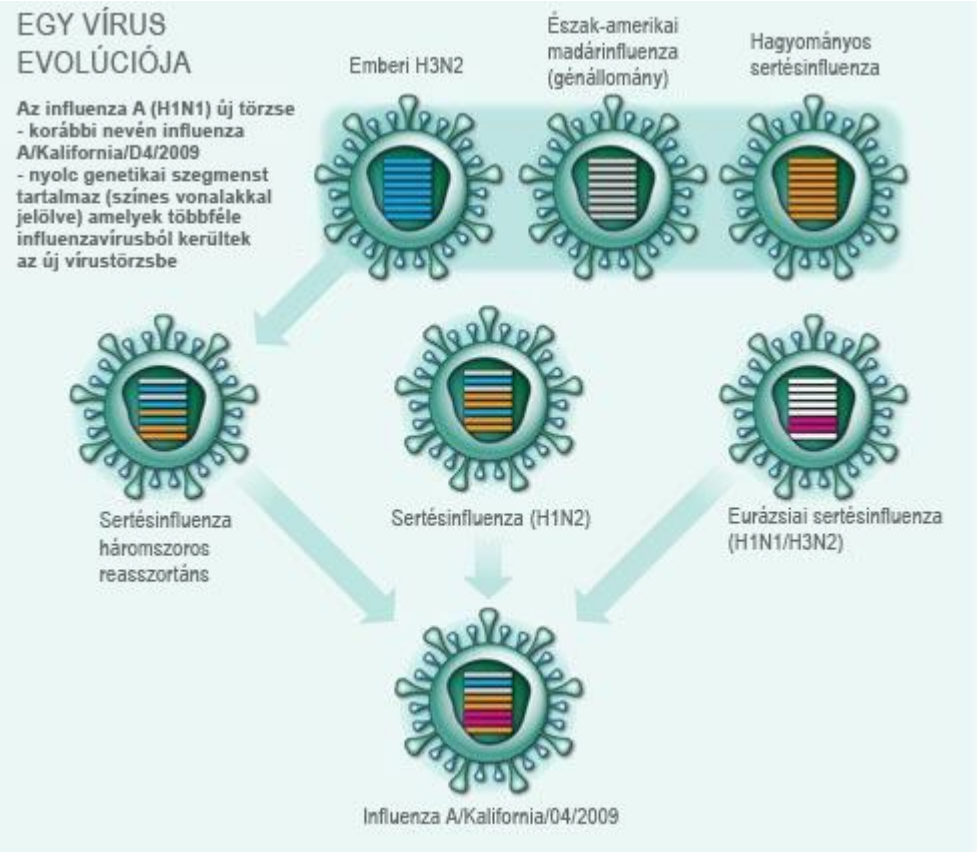
2. A/H1N1 INFLUENZA

2.1. Mi is valójában az új humán influenza (sertésinfluenza)?

A sertésinfluenza tulajdonképpen nem más, mint az influenza A vírus, H1N1 vírustörzse által okozott fertőző, akut, légúti megbetegedés. A sertésállományban ehhez hasonló influenzajárvány sokszor előfordulhat, mivel a sertések egyfajta olvasztótégelyei a különböző influenza altípusoknak, mint a madárinfluenza, humán influenza és persze a sertésinfluenza. Így fordulhat elő, hogy ezen altípusoknak a genetikai állománya keveredjen és kialakuljon egy emberre is veszélyes újfajta megbetegedés.

Ezt az új emberre is veszélyes vírust gyakran emlegetik így, mert laboratóriumi vizsgálatok során megállapították, hogy a kórokozó számos génje meglepően hasonló az észak- amerikai sertésekben kimutatott szokványosan előforduló influenzavírusokéhoz. Az új vírus nyolc genetikai szegmensének ez a kombinációja korábban sem sertés-, sem emberi influenzavírusokban nem fordult elő. Kiderült: mind a nyolc szegmens madarakban alakult ki. A madarakból aztán sertésekre került át, és bennük hosszú időn át - egészen 1918-tól, a spanyolnáthajárvány kezdetétől 1998-ig - keringett és kombinálódott. A sertésekben 1998-ra alakult ki egy úgynevezett háromszoros hibridvírus (reasszortáns), amely emberi-, madár- és sertéseredetű géneket is tartalmaz, és attól kezdve kering Észak-Amerikában és Ázsiában (az új vírus nyolc génszegmensből ez hat eredetéért felelős). Ez a vírus kombinálódott aztán eurázsiai sertésinfluenza-vírusokból származó további génekkel, így alakult ki az új vírus nyolc genetikai szegmense. A szakemberek ezért négyszeres genetikai keveredést tartalmazó, idegen gént hordozó, rekombináns vírusnak nevezik. A nyolc génszegmensben egyelőre nem találták meg a vírus emberek közötti terjedését lehetővé tévő szekvenciákat, ezek a vírusgenom egyelőre ismeretlen részén lehetnek. A további, részletes elemzések a védőoltás pontos kifejlesztése szempontjából alapvető fontosságúak.

[4] Bár a surveillance szónak van magyar megfelelője (megfigyelés), de a nemzetközi szakirodalom (így a hazai is) az eredeti angol kifejezést használja. Így dolgozatban sem térünk el ettől a sémától.



2. ábra. Az A/H1N1 vírus kialakulása[5]

2.2. Tünetek

Az új típusú influenza tünetei megtévesztésig hasonlítanak a szezonális influenza megszokott és jól ismert tüneteihez, amelyek a következők lehetnek: magas láz, köhögés, végtagfájdalom, fáradtság, kimerültség, levertség, hidegrázás, fejfájás, orrfolyás, torokfájás, légzési nehézségek, valamint súlyosabb esetben ezekhez még hányás és hasmenés is társulhat, a legrosszabb esetben a szövődmények halált is okozhatnak. Viszont van egy fontos tulajdonság, ami alapján könnyen el tudjuk dönteni, hogy szezonális influenzával vagy az új influenzával fertőződtünk meg. Mégpedig az a tény, hogy míg a szezonális influenzánál a tünetek egymás után következnek és egyre súlyosbodnak, addig az új típusú megbetegedésnél ezek a tünetek hirtelen és egyszerre jelentkeznek, előzmények nélkül. Fontos megjegyezni, hogy a sertésinfluenza súlyosbíthatja a betegek esetlegesen már meglévő krónikus orvosi állapotát.

Az influenza igazi veszélye a szövődményeiben rejlik. Felnőtteknél okozhat bakteriális tüdőgyulladást, a krónikus hörghurut heves fellángolását, agyi keringészavart, szívinfarktust, toxikus sokk tünetegyüttest, agyhártya- és agyvelőgyulladást, veseelégtelenséget, az anyagcsere betegségek (pl.: cukorbetegség) egyensúlyának felborulását, és kialakulhat még néhány ritka, de igen veszélyes más betegség is. Az influenza vírus kaput nyit a légutakat megbetegítő bakteriális korokozók előtt, ezért fontos az időbeni felismerés és kezelés!

[5] Forrás: WHO: A (H1N1) influenza 37. frissített változat-
http://www.antsz.hu/portal/portal/infl_who_kozlemenyek.html?menuid=6dd412ee-3aff-11de-85eb-6357d2760e52
Letöltés ideje: 2009. május 23.

2.3. A pandémiás oltóanyag

Az influenza ellen a jelenleg ismert leghatékonyabb védekezés a specifikus védőoltás. A pandémiás A/H1N1 vírust tartalmazó influenza vakcina humán klinikai vizsgálatai 2009. augusztus 13-án kezdődtek meg. A vizsgálatok a 18-60 év közötti felnőttekre, a 60 év felettiekre, a 3-12 éves gyerekekre, a 12-18 éves serdülőkre, valamint a 3-6 hónapos gyermekekre terjednek ki. Ezek alapján elmondható, hogy a vakcina teljesíti az ellenanyagszint növekedésére vonatkozó klinikai vizsgálati követelményeket. A vakcina beadást követő enyhe mellékhatások jellegüket és előfordulási arányukat tekintve megegyeznek a szezonális vakcinával oltottaknál tapasztalt mellékhatásokkal.

A magyarországi influenza elleni pandémiás vakcina engedélyezése az erre vonatkozó uniós ajánlások szerint zajlott. Eszerint az oltás egy úgynevezett „mock up" vakcina (modell vakcina) engedélyét felhasználva engedélyezik a gyógyszer-engedélyező hatóságok. Ez azt jelenti, hogy a készítményt már elkezdik kifejleszteni még a járvány terjedése előtt. Modellként általában a H5N1 vírustörzset használják, mivel ez az az új influenzatörzs, amely a legjobban hasonlít a pandémiát okozó vírushoz, egyik szezonális influenzavírussal sem azonos és világjárványt okozhat. A beazonosítását követően a hazai gyártó is megkapta a járványt okozó új vírustörzset: A/California/7/2009, az atlantai székhelyű Betegségmegelőzési és Járványügyi Központtól és áttért a modell vakcináról a pandémiás oltóanyag kifejlesztésére, amihez a modell vakcinához végzett vizsgálatok egy részét is felhasználta. Az engedélyezési eljárás folyamán az Országos Gyógyszerészeti Intézet által már forgalomba hozatalra engedélyezett H5N1-es vírustörzset tartalmazó Fluval P prepandémiás monovalens[6] influenza vakcina engedélyének módosítására- úgynevezett törzsváltásra- került sor a vakcinába beépített vírustörzs megváltoztatása miatt.

A vakcina megfelel a WHO és az Európai Bizottság pandémiás helyzetre vonatkozó ajánlásainak. Magyarországnak saját oltóanyag termelő kapacitása és kidolgozott gyártástechnológiája van, amivel az Omninvest cég rendelkezik. A védőoltások beadását követően mintegy 10-14 nap szükséges ahhoz, hogy a megfelelő védettség kialakuljon.

3. A KATASZTRÓFAVÉDELEM HELYI PREVENCIÓS INTÉZKEDÉSEI, MEGELŐZÉSI CSELEKVÉSTERVE ÉS A PANDÉMIÁRA VALÓ FELKÉSZÜLÉS MAGYARORSZÁGON ÉS FEJÉR MEGYÉBEN

Az egészségügyi és katasztrófavédelmi központi szervek és egyéb társszervek, már a vírus amerikai megjelenése után, az információk tükrében, meghozták az elsődleges intézkedéseket annak érdekében, hogy a magyarországi és a megyei e témában érintett szakember gárda fel tudjon készülni a beavatkozásra. Ennek érdekében mind az egészségügyi, katasztrófavédelmi és egyéb társszervek (azok, akiknek nincsen közvetlen beavatkozási feladatuk) lepontosították, kiegészítették a már meglévő pandémia terveiket, illetve az ilyen tervekkel nem rendelkező szerveknél az Országos Tisztiorvosi Szolgálat ajánlásának megfelelően új tervek készültek. A megyékben, védelmi igazgatási előadássorozat keretében a polgármesterek, a jegyzők, valamint a védelmi referensek megismerkedhettek az új humán influenza hatásmechanizmusával, a prevenció lehetséges módozataival, a magyarországi felkészülés aktuális állapotával és a világban bekövetkezett terjedés jelenlegi helyzetével. Így-

[6] Monovalens: csak és kizárólag ezt a vírust tartalmazó (vakcina)
Forrás: www.gyakorikerdesek.hu
Letöltés ideje: 2009. október 25.

talán sikerült a helyi védekezés elsőszámú irányítóit felkészíteni az élőhelyükön esetlegesen bekövetkező pandémia következményeire.

A védekezésre való felkészítést az előadások keretében A Megyei Tisztiorvosi Szolgálat, a Megyei Katasztrófavédelmi Igazgatóságok, valamint a Polgárvédelmi Kirendeltség szakemberei hajtották végre.

A Megyei Katasztrófavédelmi Igazgatóságok 2009. májusában megkezdték a hivatásos, önkéntes és létesítményi tűzoltóságok felkészítését, melynek keretében felhívták a parancsnokok, munkahelyi tűzvédelmi vezetők figyelmét a H1N1 influenza veszélyeire. Pontosították a Veszélyelhárítási Terv Influenza Pandémia résztervét. Szakmai háttéranyagokat dolgoztak ki a Nemzeti Influenza Pandémiás Terv alapján és segítségnyújtást biztosított a megye tűzoltással, kárelhárítással foglalkozó szervei részére saját influenza pandémia tervük elkészítésére.

2009 szeptemberében az Egészségügyi Miniszter tájékoztatta az Önkormányzati minisztert, hogy a WHO, valamint az EU járványügyi ajánlásainak megfelelően kialakították az influenza pandémia elleni védekezés alapvető eszközét szolgáló védőoltáshoz az oltandók prioritási sorrendjét.

Ez alapján elsőként oltandó a Magyar Honvédség és a rendvédelmi szervek állománya, továbbá a nemzetgazdaság működésének fenntartásában, a lakosság alapvető ellátásában, a közszolgáltatások fenntartásában résztvevő alapvető szolgáltatók kulcsfontosságú dolgozói.
Az OTH megkezdte az oltóanyagok disztribúciós tervének, illetve az oltásban részesültek dokumentálása előkészítését.

Mindezeknek megfelelően az Önkormányzati Miniszter iránymutatása és az Országos Katasztrófavédelmi Főigazgatóság utasítása alapján megkezdődött a megyei katasztrófavédelmi igazgatóság, hivatásos önkormányzati, az önkéntes, és a főállású létesítményi tűzoltóságok állományáról készített nyilvántartási adatok felterjesztése. Az adatok birtokában megküldésre került az oltandók létszáma, így lehetőség nyílt a FLUVAL A,B általános influenza elleni védőoltás beszerzése mellet a FLUVAL P új humán influenza elleni vakcina leszállítása.

3.1. Megyei katasztrófavédelmi feladatok járvány kitörésekor

Amikor még nincs kihirdetett járványügyi veszélyhelyzet, a Megyei Katasztrófavédelmi Igazgatóságnak elsősorban közreműködő jellegű szerepe van. Közreműködik az önkormányzatokkal, a tűzoltóságokkal és a szállítási, a fertőtlenítési, mintavételi, lakossági tájékoztatási és a karantén intézkedések végrehajtásában. Fontos a kisegítő személyzet és a nélkülözhetetlen anyagi- technikai és humán erőforrások biztosítása.
Veszélyhelyzetben továbbra is elsősorban a közreműködő feladatok a jellemzőek, a végrehajtók kiegészülnek a lakosság köréből szervezett polgári védelmi szervezetekkel, ebben az esetben a közegészség- és járványügyi-, valamint állat- és növényvédelmi szakalegységekkel is.

Amennyiben a Kormányzati Koordinációs Bizottság valamint a Megyei Védelmi Bizottság megkezdik működésüket, a koordináció feladataiban és a munkaszervek tevékenységében jelentős részt vállal a Megyei Katasztrófavédelmi Igazgatóság. Influenza pandémia esetén, amennyiben a fertőzés terjedését a prevenció eszközeivel nem sikerül kellően megelőzni, magas megbetegedési arány jelentkezhet az állomány teljes körében. Ez nagy részben függ attól, hogy a védőoltásokkal sikerül-e időben, hatásosan megvédeni az állományt. Hasonlóan az egészségügyi dolgozókhoz, a rendvédelmi szervek állománya - ezen belül az igazgatóság állománya- ebben elsőbbséget élvez.

A megbetegedések függvényében gondoskodni kell a feladatok rangsorolásáról, a helyettesítésekről, ha szükséges a betanításról, kiképzésről. A helyettesítés szempontjából már normál időszakban fontos felmérni az állomány meglévő képesítéseit. Minősített időszakban a folyamatos működés érdekében sor kerülhet a szervezetek, a munkarend, a munkaidő megváltoztatására.

3.2. Minősített időszakban a MVB és a Helyi Védelmi Bizottságok munkaszervezetei tevékenységében való részvétel, azok szakmai támogatása

A készenléti feladatot ellátóknak az átlagosat többszörösen meghaladó, folyamatosan jelentkező feladatokkal kell számolniuk. A várható járvány alapvetően befolyásolja a fekvőbeteg ellátó intézetek szakmai működését. A terveinkben foglaltaknak megfelelően támogatjuk őket jelentős többletfeladataik ellátásában.

Katasztrófa méretű járvány bekövetkezése esetén, ha a megelőzés nem elég hatékony, felértékelődik az egészségügy civil támogatásának jelentősége. Az ellátás segítésére bevonhatók a polgári védelmi kötelezettség alapján polgári védelmi szervezetbe behívásra kerülő személyek.

Az influenza pandémia által kiváltott katasztrófa, illetve járványügyi veszélyhelyzet felszámolása szakmailag elsődlegesen az egészségügyi ágazat feladata, azonban az egészségügy önmagában nem képes a járvánnyal kapcsolatos minden következmény és megoldandó kérdés kezelésére. Az eredményes védekezés és felszámolás csak a kormányzat és a társadalom együttes közreműködésével valósítható meg.

4. A MAGYAR HONVÉDSÉG INFLUENZA PANDÉMIA TERVE

4.1. A Honvédelmi ágazat kötelezettségei az ágazaton belüli veszélyeztetettség esetén:

A honvédelmi ágazatot érintő súlyos influenza pandémiás helyzet kezelése alapvetően a belső védelmi tervek alapján végzett tevékenység végrehajtásával valósul meg a Honvédelmi Katasztrófavédelmi Rendszer (a továbbiakban: HKR) bázisán. A honvédelmi ágazat elsődleges feladata a Magyar Honvédség (a továbbiakban: MH) működőképességének megőrzése és alapvető feladatainak ellátása, továbbá a hivatásos és önkormányzati katasztrófavédelmi szervekkel való fokozott együttműködés az influenza pandémia elleni védekezés valamennyi időszakában. A védekezésben és a felkészülésben alapvetően a következő szervezetek vesznek részt:

- Magyar Honvédség Közegészségügyi – Járványügyi Szolgálata (MH KJSZ)
- Honvédelmi Minisztérium Állami Egészségügyi Központ (HM ÁEK)
- Magyar Honvédség Dr. Radó György Honvéd Egészségügyi Központ (MH HEK)

4.2. Az Influenza Pandémia Terv

A terv azzal a céllal született, hogy ennek alkalmazásával az MH képes legyen saját csapatainak megóvására, egy előre kidolgozott terv alapján csökkenthető legyen az esetleges megbetegedések vagy akár halálesetek száma. Biztosítva legyen az ellátás a tömeges méretű megbetegedések esetén, valamint alapvető cél, hogy felszámolják a járványt. Ez az okmány a

HKR Ágazati Katasztrófavédelmi Terv része. Hatálya kiterjed a Honvédelmi Minisztériumra, a Honvédelmi Minisztérium közvetlen alárendeltségébe és felügyelete alá tartozó és a Magyar Honvédség hadrendje szerinti szervezetek összességére.

A tervben foglaltak megértéséhez, alapfogalmakból összeállított jegyzéket, valamint az okmány felhasználhatóságát bizonyítandó, az ebben a tervben foglaltak jogszabályi hátterének jegyzékét is megtalálhatjuk.

A pandémia szakaszainak bemutatása után - amely megegyezik az eddig ismertetettel- a tervben olvashatóak az előirányzott feladatok.

4.3. A honvédelmi ágazat feladatai a pandémia különböző időszakaiban

Az ágazat feladatai a pandémia időszakaiban a következők:

- Az egészségügyi vonatkozások tekintetében elkülönülnek a Felkészülési Időszak Feladatai és a Védekezési Időszak Feladatai.
  - A Felkészülési Időszakban Nemzeti Influenza Pandémia Prevenciós Bizottság meghatározza az aktuális teendőket, felülvizsgálja és értékeli a felkészültség helyzetét,javaslatokat tesz a további teendőkre. A Járványügyi Védekezési Munkabizottság áttekinti milyen más ágazathoz tartozó szervezetek közreműködésére lehet szükség a későbbiekben. Létrehozzák a MH Pandémiás Prevenciós Bizottságot, amely kezdeményezi a költségvetési források biztosítását, egyezteti és pontosítja az Országos Katasztrófavédelmi Főigazgatósággal azokat a feladatokat, amelyekben a katasztrófavédelmi szervek közreműködése szükséges. Az MH teljes személyi állománya részére tájékoztatót tartanak a járványveszélyről, a védekezés módjáról, az oltóanyag ellátás rendjéről. Intézkednek a külszolgálat személyi állományára vonatkozóan a járványügyi védelem megszervezésére.
  - A Védekezési Időszak Feladatai között szerepel:
    - A Surveillance, azaz influenza figyelő szolgálat működését megerősítik az alábbi szempontok alapján: folyamatos kapcsolattartás az üzemeltető Országos Epidemiológiai Központtal, aktualizálják az influenzával kapcsolatos szakmai irányelveket, az egészségügyi szolgálatok vezetője folyamatosan jelenti a munkahelyi hiányzásokat, az influenza vakcinák felhasználását, szövődmények előfordulását, a felgyógyultak állapotát.
    - A Laboratóriumi diagnózis, amelyet az ÁNTSZ rendel el, abban az esetben, ha halálos kimenetelű influenza megbetegedés történik. A diagnózissal kapcsolatban figyelni kell arra, hogy a mintagyűjtésre és szállításra az infekciókontroll szabályai érvényesek. Rapid diagnosztikai tesztek eljuttatása az alakulatokhoz.
    - Járványügyi Intézkedések keretében korlátozhatják a kiképzések, gyakorlatok végrehajtását, a napi élet egyes szakaszait. Elrendelhetik a az előzetes terveknek megfelelően a védőoltások megkezdését. MH Főepidemiológus Operatív Csoportokat jelöl ki és együttesen járványügyi vizsgálatot végeznek, elvégzik a mintavételezést, felügyelik a fertőtlenítés végrehajtását.
    - Az oltások rendjénél különböző prioritásokat kell figyelembe venni. Előzetesen meg kell állapodni az illetékes állami szervekkel, védőoltás gyártókkal, hogy az MH teljes személyi állományát lefedő mennyiségű, azonnali hozzájutási prioritást élvezzen. Az oltási prioritás is kidolgozásra kerül, különböző prioritási csoportok kijelölésével.

- A Magyar Honvédség Közegészségügyi- Járványügyi Szolgálatának szakfeladatai:
  - Az MH Influenza Pandémia Bizottsága 8 főből áll, Katasztrófavédelmi Operatív Csoportként működik a HKR részeként. Feladatai többek között, hogy meghatározza a járvány megelőzéséhez és felszámolásához szükséges anyagi- és eszköz igényeket, valamint koordinálja a MH Közegészségügyi- Járványügyi Szolgálatának tevékenységét. Meghatározza a védőoltások elosztásának rendjét. Ezen feladatok végrehajtására különböző csoportokat jelölnek ki. Így létezik Operatív csoport, Epidemiológiai csoport, Oltócsoport, Diagnosztikai csoport.
- A Honvédelmi Minisztérium Állami Egészségügyi Központ Speciális Betegellátási Feladatai
  - A WHO bejelentését követően megalakul a Járványvédelmi Operatív Bizottság, átvizsgálja és szükség szerint módosítja az Influenza Pandémia Tervet. A Bizottság megteszi a szükséges gyakorlati intézkedéseket, készenlétbe helyezi a betegek fogadására a kijelölt influenza pandémiás osztályt a rendkívüli esemény azonnali végrehajtására, biztosítja a szükséges eszközöket.
- A Védelmi Igazgatás Speciális Feladatai
  - A védelmi igazgatás Speciális feladatai mind a felkészülés, mind a védekezés időszakában a MH Védelmi Hivatal koordinálja. A pandémia elleni felkészülés céljai, hogy a védelmi igazgatás működési folyamatosan biztosítva legyen központi, területi és helyi szinten. A kormányzat folyamatosan tudjon működni a védekezés időszaka alatt. Minősített időszak bevezetése esetén zökkenőmentes legyen az átmenet, a minősített időszaki irányítás, vezetés feltételei biztosítva legyenek. Ezen kívül biztosítania kell a lakosság ellátását, a szolgáltatások és közlekedés feltételeit. A védelmi igazgatás feladatai elkülönülnek a központi államigazgatási szervek működésének, vezetésének fenntartása és támogatása érdekében végrehajtandó és a területi védelmi igazgatási szervek felügyelete, illetve azokkal való együttműködés keretében meghatározott feladatokra. Ám még, ezeket a feladatokat is külön részre bontják a szerint, hogy a pandémiára való felkészülés időszakában vagy a védekezés időszakában foganatosítják. A pandémia lezajlása után is maradnak feladatok, mint például a járványról készített összefoglaló jelentés készítése, a végrehajtott feladatok értékelése, következtetések levonása, esetlegesen az Ágazati Pandémiás Terv módosításának kezdeményezése.

Az Influenza Pandémia Terv pontosítása szükség szerint, illetve a HM Műveleti Központ (HM MK) parancsnok intézkedése alapján lapcserével együtt történik.

KÖVETKEZTETÉSEK

Végső konzekvenciaként megállapítottuk, hogy a Magyarország kormányzati, egészségügyi és más, pandémiák kapcsán érintett szervezetek szakmailag, és az anyagi lehetőségekhez képest maximálisan felkészültek egy járvány kezelésére, az okozott megbetegedések ellátására. Az ezekhez kapcsolódó intézkedések és cselekvéstervek kiadása nemcsak időben, hanem naprakészen és közérthetően, következetesen történik a nemzetközi ajánlások elfogadásával és betartásával együtt. A pandémiára való felkészülés, valamint az elhárítás során a minisztériumok, hivatalok, szolgálatok és katasztrófavédelmi szervezetek és közintézmények együttműködése is példás rendben zajlik mind a mai napig. Továbbá az ÁNTSZ, Országos Tisztifőorvosi Hivatal, Pandémiás Prevenciós Bizottság, Országos

Epidemiológiai Központ és érintett szervek közötti jó kommunikáció lehetővé teszi a veszélyek gyors és hatékony elhárítását.

Javasolnánk továbbá, hogy azok a kételkedők, akik ellenzik a pandémiás védőoltások szétosztását és beadatását, tanulmányozzák át ezt a cikket. Bizonyára ezt követően elgondolkoznak azon melyik esetnek nagyobb a valószínűsége annak, hogy direkt módon az A/H1N1 vírustól betegszenek meg, esetleg kialakul nem várt tartós egészségkárosodás, vagy a védőoltás mellékhatásai miatt alakulnak ki szövődmények.

IRODALOMJEGYZÉK

1. Bakos Ferenc: Idegen szavak és kifejezések szótára, Akadémiai Kiadó, Budapest 1973.
2. Epinfo- Epidemiológiai Információs hetilap- Madárinfluenza a leggyakrabban felmerülő kérdések és válaszok- 13. évfolyam 1. szám-2006. január 13.
3. Gergely Lajos: Orvosi mikrobiológia 2. kiadás, Alliter Kiadói és Oktatásfejlesztő Alapítvány, Budapest, 2003.
4. Herold, Gerd: Belgyógyászat 5. kiadás, Magyar kiadás, főszerkesztő: Romics László B+V Lap- és Könyvkiadó, 2007
5. Tompa Anna: Népegészségtani ismeretek, Semmelweis Kiadó, Budapest, 2008.
6. Az MH Influenza Pandémia terve, Honvédelmi Minisztérium , 2008
7. Az influenza A/H1N1 vírus által okozott, Magyarországon felderített megbetegedések 2009. május 25- 2009. augusztus 8.- Országos Epidemiológiai Központ-2009. szeptember 26.- http://www.oek.hu/oek.web?to=1248,3,1601,1609&nid=788&pid=1&lang=hun
8. Az Országgyűlés Egészségügyi Bizottságának Állásfoglalása- „Az új típusú influenza vírus elleni védekezés feladatairól”-2009. október 14.
9. Dr. Bujdosó László: Lokális válaszok globális kérdésekre, 2009. október 14.
10. Dr. Csohán Ágnes: Az új influenzavírus- tapasztalataink és feladataink, 2009. szeptember 29.
11. Dr. Csohán Ágnes: A 2009. évi A/H1N1 influenza pandémia nemzetközi tapasztalatai, 2009. szeptember 02.
12. Dr. Lencsés Gyöngyi: Teendők az „új influenza” A/H1N1 vírus által okozott megbetegedés esetén, 2009. október 10.
13. Kérdések és válaszok az új influenzáról, a megelőzésről, a védőoltásról- ÁNTSZ Országos Tisztifőorvosi Hivatal Kommunikációs Főosztály, 2009. október 18.
14. Pandémiás terv és kríziskommunikációs terv készítéséhez, intézmények, gazdasági és civil szervezetek részére- ÁNTSZ

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Péterfalvi Attila
peterfalvi@obh.hu

Solymosi József
solymosi.jozsef@zmne.hu

MINŐSÍTÉSI KATEGÓRIÁK VÁLTOZÁSA A KATASZTRÓFAVÉDELEMBEN

Absztrakt

Az Alkotmány nevesíti a minősített időszakokat, meghatározza azok életbeléptetésének feltételeit, valamint azok tartalmát. A közérdekű adatok körében a környezeti adatok nyilvánosak. A megelőzés, védekezés és elhárítás érdekében jogszabályok tájékoztatási kötelezettséget állapítanak meg, ugyanakkor katasztrófavédelemre hivatkozással a nyilvánosság korlátozható.

The Constitution defines the qualified periods of time, determines the conditions of their introduction, as well as their legal content. Among data of public interest environmental data are publicly accessible. In the interest of prevention, defence or doing away with the consequences the rules of law lay down an obligation of information, this public access to information may, however, be restricted by disaster management.

Kulcsszavak: *minősített időszak, környezeti információ, katasztrófavédelem, nyilvánosság korlátozása ~ qualified periods, environmental data, disaster management, restriction of information*

TÁJÉKOZTATÁS ÉS INFORMÁCIÓHOZ VALÓ HOZZÁFÉRÉS A KATASZTRÓFAVÉDELEMBEN

A minősített időszakokat, az egyes intézkedések tartalmát és bevezetésük feltételeit alapvetően az Alkotmány határozza meg. Minősített időszakban megváltoznak a normál időszaki jogok és kötelezettségek, a békeidőszaki működéshez képest szigorításokat jelentő, úgynevezett rendkívüli intézkedések lépnek életbe. A minősített időszakok alatt 2004. december 31-ig a rendkívüli állapotot, a szükségállapotot, veszélyhelyzetet és az Alkotmány 19/E. § szerinti helyzetet értettük. 2005. január 1-el változott a helyzet, az önkéntes haderőre történt áttérés, a hadkötelezettség békeidőszaki megszüntetése kapcsán, a 2004. évi CIV.

törvénnyel módosításra került az Alkotmány, és egy új minősített időszak, a megelőző védelmi helyzet került beemelésre a szabályozási rendszerbe. A módosított Alkotmány - a felhatalmazást adó rendelkezések sorszámozásának sorrendjében - az alábbi minősített időszakokat különbözteti:

- rendkívüli állapot,
- szükségállapot,
- megelőző védelmi helyzet,
- az Alkotmány 19/E § szerinti minősített időszak,
- veszélyhelyzet.

A minősített időszakok közös jellemzője, hogy az állam normál működését, az állampolgárok élet- és vagyonbiztonságát külső vagy belső társadalmi, illetve természeti veszély fenyegeti. A veszélyek elhárítására, illetve következményeinek felszámolására a rendkívüli jogrend eszközei vehetők igénybe [1]. Horváth Zita megállapítását annyiban egészítjük ki, hogy a rendkívüli jogrend intézkedésein túl a minősített időszakokban – így a katasztrófa idején, de a katasztrófavédelemi feladatok ellátása során is, az alapvető jogok is korlátozhatók a szükségesség és arányosság követelményének megfelelően.

A katasztrófa fogalma a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 1999. évi LXXIV. törvény (továbbiakban: Kat.) szerint: a szükséghelyzet vagy a veszélyhelyzet kihirdetésére alkalmas, illetőleg a minősített helyzetek kihirdetését el nem érő mértékű olyan állapot vagy helyzet (pl. természeti, biológiai eredetű, tűz okozta), amely emberek életét, egészségét, anyagi értékeiket, a lakosság alapvető ellátását, a természeti környezetet, a természeti értékeket olyan módon vagy mértékben veszélyezteti, károsítja, hogy a kár megelőzése, elhárítása vagy a következmények felszámolása meghaladja az erre rendelt szervezetek előírt együttműködési rendben történő védekezési lehetőségeit, és különleges intézkedések bevezetését, valamint az önkormányzatok és az állami szervek folyamatos és szigorúan összehangolt együttműködését, illetve nemzetközi segítség igénybevételét igényli.

Noha a hidegháború lezárulásával jelentősen csökkent egy világméretű fegyveres konfliktus kialakulásának veszélye, a potenciális veszélyforrások összetettebbé váltak, és ezzel egyidejűleg instabilabbak és kevésbé kiszámíthatók. Milyen új veszélyforrások jelentek meg? Bukovics István klasszifikációja szerint [2] a Magyarországon lehetséges katasztrófák a technikai fejlődés következtében átalakultak, és kiszélesedtek. Ma már veszélyforrásként kell tekintenünk a világ instabil zónáira, és amelyek számos gazdasági és társadalmi konfliktus tűzfészke, számolnunk kell a nemzetközi terrorizmus veszélyeivel, a proliferációval, de a globalizációval összefüggésben a pénzügyi rendszerek instabilitásával is. Az információs társadalom infokommunikációs eszközeinek sérülékenysége jelentős kihatással van a társadalmi, gazdasági rendszerekre, és az ökológiai és civilizációs veszélyek is katasztrófa helyzetet idézhetnek elő (ún. globális kihívások). Ezeken túl a regionális és belső kockázati tényezőkre (határon túli magyarok helyzete, avagy bűncselekmények elterjedtsége) is akként kell tekintenünk, mint potenciális veszélyhordozó társadalmi jelenségekre.

Bukovics [2] osztályozásában a katasztrófavédelemre új kihívásként jelenik meg a tömegpusztító fegyverek jelenléte és a technológiák elterjedtsége, de különösen azok terrorszervezetek számára való hozzáférhetősége. Hanka László, Vincze Árpád és Solymosi József [3] osztják Bukovics álláspontját abban, hogy a hidegháború elmúltával új típusú fenyegetésekkel kell szembenézni, de nem hagyható figyelmen kívül az a tény, hogy a nukleáris arzenál továbbra is jelenlévő a nemzetek fegyverarzenáljában. A veszélyt az jelenti, ha ezek a fegyverek terrorszervezetek kezébe kerülnek, avagy terrorista csoportok

megpróbálkoznak ilyen fegyverek előállításával. Alternatív veszélyként kínálkozik továbbá szerintük a nukleáris létesítmények és/vagy az atomerőművek elleni támadás lehetősége is.

Halász László védendő értékként a kritikus infrastruktúrákat jelöli meg, amelyek a modern társadalom létfeltételeit képezik [4]. A kritikus infrastruktúra védelem alatt az ország mindennapi körülményeinek fenntartását, így az állam, a gazdasági szereplők, valamint a lakosság részéről jelentkező igények biztosításához szükséges létfontosságú infrastruktúrák lehető legnagyobb biztonsággal és magas fokú koordináció mellett történő működtetésének megvalósítását szolgáló intézkedések összességét érti. Láthatjuk, hogy ez a megközelítés sokkal átfogóbb, mint amivel a jogi norma operál. Valójában erre a kritikus infrastruktúrára jelentenek veszélyt a környezetszennyezés és a civilizációs és természeti katasztrófák.

Az életet, a vagyonbiztonságot, a természetes és épített környezetet tehát természeti és civilizációs katasztrófák veszélyeztetik, melyek megelőzése és károsító hatásai elleni védekezés nemzeti ügy, közfeladat. A katasztrófavédelemben eljáró szervek közfeladatot látnak el, a tevékenységükre vonatokozó adatok közérdekű adatnak minősülnek. Nemkülönben közérdekű adat lehet a katasztrófa előidézőjére vonatkozó adat is (pl. nukleáris erőmű).

A katasztrófavédelmi feladatok ellátása során az Alkotmány következő rendelkezéseire kell figyelemmel lennünk. Az Alkotmány 2. §-a deklarálja, hogy a Magyar Köztársaság független, demokratikus jogállam. Az Alkotmány elismeri az ember sérthetetlen és elidegeníthetetlen alapvető jogait, sőt ezek tiszteletben tartását és védelmét az állam elsőrendű kötelességévé teszi. Ezek közé az alapvető jogok közé tartozik a közérdekű adatok nyilvánosságához való jog (61. §), és az egészséges környezethez való jog (18. § és 70/D. §). Rendkívül fontos rendelkezése az Alkotmánynak, hogy az alapvető jogokra és kötelességekre vonatkozó szabályokat törvénynek kell megállapítania, de az alapvető jog lényeges tartalmát még az sem korlátozhatja. Ugyanakkor a jogok egy részének gyakorlása - pontosan körülhatárolt kivételekkel - rendkívüli állapot, szükségállapot vagy veszélyhelyzet idején felfüggeszthető vagy korlátozható (8. §).

A közérdekű adatok nyilvánosságához való jog érvényesüléséhez illetve annak alkotmányos korlátozásához a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.) rendelkezései alapvetőek. A környezeti adatok nyilvánosságát hivatott biztosítani a környezet védelméről szóló LIII. törvény (Kt.), illetve a környezeti ügyekben az információhoz való hozzáférésről, a nyilvánosságnak a döntéshozatalban történő részvételéről és az igazságszolgáltatáshoz való jog biztosításáról szóló, Aarhusban, 1998. június 25-én elfogadott Egyezmény kihirdetéséről szóló 2001. évi LXXXI. törvény, amely a környezeti adatokhoz való hozzáférés lehetséges korlátait is meghatározza. A nyilvánosság korlátozásának lehetőségét a minősített adatok védelméről szóló 2009. évi CLV. törvény is tartalmazza.

Az Avtv., a környezet védelméről szóló törvény és az Aarhusi Egyezmény egyaránt kimondják az általános tájékoztatási kötelezettséget, illetve annak ellenpólusaként a tájékozódáshoz való jogot. A közfeladatot ellátó szervek mindenki számára lehetővé teszik a a közérdekű adatok, a környezet és az egészség lényeges összefüggéseinek, a környezetkárosító tevékenységek és azok fontosságának megismerését. Az információszolgáltatás azonban nem csupán az állami feladatot ellátó szerv kötelezettsége, hanem a környezethasználóé is. Az információszabadság aktív oldalán tehát a közfeladatot ellátó szervek, személyek, a közérdekű adatokat kezelő szervek, személyek tájékoztatási kötelezettsége áll. Az információszabadság másik olvasata, hogy bárki kérheti a közérdekű

adatokat, és mindenkinek joga van a külön jogszabályban meghatározott környezeti információkat - mint közérdekű adatokat - megismerni. A Kat. értelmében minden állampolgárnak, illetve személynek joga van arra, hogy megismerje a környezetében lévő katasztrófaveszélyt, elsajátítsa az irányadó védekezési szabályokat, továbbá joga és kötelessége, hogy közreműködjön a katasztrófavédelemben. A Kt. 12. §-a alapján pedig a környezeti információval rendelkező szerv biztosítja a nyilvánosság, illetve a környezeti információt igénylő számára, hogy a környezeti információ megismerésére vonatkozó jogosultságairól tudomást szerezzen, továbbá elősegíti a környezeti információhoz való hozzájutást. Az Aarhusi Egyezmény kihirdetéséről szóló törvény definiálja a környezeti információt, és általános alapelvként rögzíti, hogy „valamennyi Fél törekszik biztosítani azt, hogy a tisztségviselők és a hatóságok nyújtsanak segítséget és útbaigazítást a nyilvánosságnak a környezeti információhoz való hozzáférésben." Mind a természeti, mind a civilizációs katasztrófa a környezet állapotát befolyásolja, ezért a katasztrófavédelemmel összefüggésben bármely hatóságnál, szervnél vagy gazdálkodó szervezetnél keletkezett, vagy kezelt adat környezeti információ lehet. Az Egyezmény szerint „környezeti információ" jelent bármely írott, látható, hallható, elektronikus vagy egyéb formában megjelenő információt, melynek tárgya:
- a környezet elemeinek, úgymint a levegőnek és az atmoszférának, a víznek, a talajnak, a földnek, a tájképnek, a természetes élőhelyeknek, a biológiai sokféleségnek és összetevőinek, beleértve a genetikailag módosított szervezeteket is, illetve ezen elemek közti kölcsönhatásnak az állapota;
- tényezők, úgymint anyagok, energia, zaj és sugárzás, tevékenységek és intézkedések, beleértve a közigazgatási intézkedéseket, a környezetet érintő megállapodásokat, irányelveket, jogalkotást, terveket és programokat, amelyek befolyásolják vagy befolyásolhatják a fenti említett környezeti elemeket, valamint a környezeti döntéshozatalban felhasznált költség-haszon, továbbá egyéb gazdasági elemzések és becslések;
- az emberi egészség és biztonság állapota, az emberi élet, a kulturális helyszínek és az épített környezet állapota, olyan mértékben, amilyen mértékben ezeket befolyásolja vagy befolyásolhatja a környezeti elemek állapota, vagy ezen környezeti elemeken keresztül fent említett tényezők, tevékenységek vagy intézkedések.

Az Egyezmény részletesen meghatározza azokat az eseteket, amikor a környezeti információra vonatkozó kérés elutasítható. Ilyen esetek: a hatóság, melyhez a kérést benyújtották, nem rendelkezik a kért környezeti információval; a kérés egyértelműen ésszerűtlen, vagy túlságosan általános módon fogalmazták meg; továbbá a kérés olyan anyagra vonatkozik, mely előkészítés alatt áll, vagy hatóságok belső kommunikációjára vonatkozik, abban az esetben, ha a nemzeti jog vagy szokásjogi joggyakorlat e kivételeket megállapítja, tekintetbe véve a közérdeket, amely az információ feltárásához fűződik. A környezeti információra vonatkozó kérés elutasítható akkor is, amennyiben az információ feltárása hátrányosan érintené: a hatósági eljárások titkosságát, ahol ezen titkosságot a nemzeti jog előírja; a nemzetközi kapcsolatokat, a honvédelmet vagy a közbiztonságot; az igazságszolgáltatás menetét, valamely hatóság azon képességét, hogy büntetőjogi vagy fegyelmi természetű vizsgálatot folytasson le; a kereskedelmi és ipari információ bizalmas jellegét, ahol ez a bizalmas jelleg méltányolható gazdasági érdekekre figyelemmel a jog által védett. E körben azonban a környezetvédelem szempontjából releváns kibocsátási adatok nyilvánosak kell hogy legyenek; természetes személy személyi adataira és/vagy annak irataira vonatkozó titoktartási kötelezettséget, amennyiben az adott személy nem adott hozzájárulást adatainak nyilvánosságra hozatalához, feltéve, hogy a bizalmas kezelést a nemzeti jog előírja; egy harmadik fél érdekeit, amely a kért információt úgy biztosította, hogy az nem volt

kötelessége, nem is volt rá jogilag kötelezhető, és nem adta jóváhagyását az anyagok kiadására; vagy a környezet azon részét, amelyre az információ vonatkozik.
Az információszolgáltatás fent említett okai szűken értelmezendők, figyelembe véve az információ feltárásához fűződő közérdeket, valamint azt, hogy a kért információ mennyiben vonatkozik a környezetbe történő kibocsátásokra.

A környezetbe történő kibocsátással kapcsolatos információt a környezeti adatok között is az abszolút nyilvánosság jellemzi, mert a Kt. szerint megismerését nem lehet arra hivatkozva megtagadni, hogy az személyes adat, üzleti titok, adótitok, fokozottan védett növény vagy állat élőhelyére, kimerülőben lévő természeti erőforrások lelőhelyére, fokozottan védett földtani természeti érték előfordulási helyére vonatkozó adat.
A katasztrófavédelemben a közérdekű adatokhoz való hozzáférés a megelőzés és a védekezés, majd a rehabilitáció időszakában más és más lehet.

A megelőzés időszakában a hangsúly azon műszaki, szervezési és jogi intézkedések, eszközök nyilvánosságán és hozzáférhetőségén van, amelyek ismeretében a környezethasználó, az engedélyes tevékenysége feltérképezhető, és annak következményei kiszámíthatók, és megelőzhetők – avagy következményei hatása csökkenthető.
A civilizációs katasztrófa elleni védelem a veszélyes ipari üzem engedélyesének is kötelezettsége. A Kat. 30. §-a szerint a veszélyes ipari üzemre, veszélyes létesítményre építési engedély, használatbavételi engedély, továbbá veszélyes tevékenység megkezdésének engedélyezése csak az Országos Katasztrófavédelmi Főigazgatóságnak (a IV. fejezet alkalmazásában: hatóság) a katasztrófavédelmi engedélye alapján adható. Az engedély iránti kérelemhez az üzemeltetőnek csatolni kell a biztonsági jelentés vagy biztonsági elemzés egy-egy példányát. A biztonsági jelentés (elemzés) nyilvánossága meghatározott körben korlátozható, ugyanis ha az védendő adatot tartalmaz, az üzemeltető egyidejűleg a nyilvánosságra hozható, védendő adatot nem tartalmazó biztonsági jelentést vagy biztonsági elemzést is köteles a hatóság részére benyújtani. A törvény értelmezésében védendő adat az üzemeltető által meghatározott üzleti titok, illetőleg az üzem külső támadás elleni biztonságára vonatkozó lényeges adat.
A veszélyes üzem üzemeltetője által készített biztonsági jelentés nyilvános és a veszélyeztetett település polgármesterének biztosítania kell, hogy abba a külön jogszabályban meghatározottaknak megfelelően bárki betekinthessen. De a biztonsági jelentésnek csak a védendő adatot nem tartalmazó változata bocsátható nyilvános megtekintésre. A védendő adatot tartalmazó biztonsági jelentésbe, illetve biztonsági elemzésbe csak az üzemeltető vagy írásban meghatalmazott képviselője, a hatóság és - szakhatóság közreműködése esetén - a szakhatóság eljárásban érintett képviselői, valamint a külön jogszabály alapján arra jogosultak tekinthetnek be. A külső védelmi terveket az Országos Katasztrófavédelmi Főigazgatóság illetékes területi szerve a veszélyeztetett települések polgármestereinek közreműködésével készíti el. A külső védelmi tervek tartalmi követelményeit és elkészítésének határidejét külön jogszabály állapítja meg. A külső védelmi tervek nyilvánosak.

A védekezés időszakában a nyilvánosság hangsúlya eltolódik az aktív tájékoztatás irányába: a lakosság riasztása, tájékoztatása prioritást kap, hogy a katasztrófa lehetséges következményei elháríthatók legyenek, csökkenjenek. Az információáramlás másik iránya a védekezésben résztvevő szervek között történik a hatékony kárelhárítás és megelőzés érdekében. A katasztrófa esetén a védelmi feladatok között értelemszerűen elengedhetetlen a lakosság tájékoztatása. A katasztrófa-, illetve a kríziskommunikáció meghatározó szerepű a válságidőszak kezelésében. A kis területű, vagy a kiterjedtebb események következtében előforduló válságmegoldásban a lakosság, és a közelben tartózkodók tájékoztatása, és a

válságkezelők megfelelő kommunikációja meghatározó jelentőségű. Hanák Tibor álláspontja szerint [5] a katasztrófahelyzetben ezért szükséges a jelentési rendszereket előzetesen megtervezni. Ezzel elősegíthető a hatékony kommunikáció, illetve elkerülhető a pánikkeltés. A szerzők Marlin Fitzwaterre hivatkozva támasztják alá az előtervezés fontosságát a hatékony kríziskommunikációban. „A jó kríziskommunikáció egy eleve jól működő rendszeren alapszik. Ha krízis van, csak gördülékenyebbé és jobbá kell tenni. A krízis közben nem lehet egy új rendszert megformálni."

Lássuk, hogy a magyar hatályos jogi szabályozás miként gondoskodik a kommunikációról.

Az Alkotmány értelmében az élet- és vagyonbiztonságot tömeges méretekben veszélyeztető, fegyveresen vagy felfegyverkezve elkövetett súlyos erőszakos cselekmények, elemi csapás vagy ipari szerencsétlenség esetén (szükséghelyzet) az Országgyűlés szükségállapotot hirdet ki. Garanciális szempontból fontos szabály, hogy az Alkotmányban meghatározott esetekben a döntéshez a jelenlévő országgyűlési képviselők kétharmadának szavazata szükséges.
A Kormány a veszélyhelyzet kihirdetését igénylő méretű katasztrófahelyzetben rendeletben kihirdeti a veszélyhelyzetet és dönt az ország egész területének vagy meghatározott részének katasztrófa sújtotta területté nyilvánításáról, a veszélyhelyzetet meghaladó méretű katasztrófa esetén kezdeményezi a szükségállapot kihirdetését. Halasztást nem tűrő esetben a Kormány rendeletei a közszolgálati (országos, területi és helyi) műsorszórók útján is kihirdethetők (rendkívüli kihirdetés), és a nap meghatározott időpontjától hatályba helyezhetők. Az így kihirdetett rendeletet a Magyar Közlöny legközelebbi számában közzé kell tenni. A rendkívüli kihirdetéssel közzétett rendeletet a kihirdetés napján vagy az azt követő napon megjelenő országos és helyi napilapokban közzé kell tenni (Kat. 7. §).
A megyei, fővárosi és helyi védelmi bizottság feladata a települések (a kerületek) közötti kölcsönös segítségnyújtás, értesítés, riasztás és tájékoztatás szervezése, továbbá a lakosság és a védekezésben érintett szervezetek riasztásának és tájékoztatásának előkészítésének és végrehajtásának a megszervezése. A megyei, fővárosi védelmi bizottság elnöke folyamatosan értékeli a kialakult helyzetet, a védekezés helyzetét, és erről a Bizottságot és a közvéleményt tájékoztatja.
A polgármester gondoskodik az illetékességi területen élő vagy tartózkodó személyek részére, a katasztrófaveszélyekről szóló, a magatartási szabályokat is tartalmazó tájékoztatásról.
A Kormány kivételes intézkedési lehetőségéről elemi csapás esetén az Alkotmány 35. § (1) bekezdésének i) pontja rendelkezik, amely szerint a Kormány az élet- és vagyonbiztonságot veszélyeztető elemi csapás, illetőleg következményeinek az elhárítása (veszélyhelyzet), valamint a közrend és a közbiztonság védelme érdekében megteszi a szükséges intézkedéseket. Veszélyhelyzetben a Kormány az Országgyűlés felhatalmazása alapján egyes törvények rendelkezéseitől eltérő rendeleteket és intézkedéseket hozhat. A veszélyhelyzetben alkalmazható szabályokról szóló törvény elfogadásához szintén a jelenlévő országgyűlési képviselők kétharmadának szavazata szükséges.
Az Alkotmány szerinti veszélyhelyzet fogalmát a polgári védelemről szóló 1996. évi XXXVII. törvény tovább pontosítja.

A rehabilitáció során az információgyűjtés, elemzés, majd a következtetések levonása válik hangsúlyossá. A közérdekű adatok megismeréséhez való jog szempontjából ez a szakasz a legérzékenyebb, mert védelemben eljáró szervek, a civilizációs katasztrófa előidézőjének a belső vizsgálatai, jelentései számos adatot és információt keletkeztetnek. A katasztrófavédelemben eljárt, a közfeladatot ellátó szervek tevékenysége során keletkezett adatok közérdekűnek minősülnek, de a döntést igénylő adatok, illetve más, biztonsági szempontból prioritást élvező adatok esetén mégsem beszélhetünk automatikus

nyilvánosságról. Korlátozást jelent az a szabály, hogy a döntés-előkészítő iratok nem nyilvánosak, emellett külön minősíteni kell azokat az adatokat, amelyek a minősített adatok védelméről szóló jogszabály hatálya alá esnek.

A továbbiakban azt kívánjuk bemutatni, hogy a katasztrófavédelem során a vonatkozó jogszabályi rendelkezések betartásával alkotmányosan korlátozható-e a közérdekű adatok nyilvánosságához való jog. A nyilvánosság korlátozása a titkosításon keresztül valósítható meg. Írásunkban ismertetjük a minősítési kategóriák változását.

A NYILVÁNOSSÁG KORLÁTOZÁSÁNAK LEHETŐSÉGEI AZ ADATOK MINŐSÍTÉSÉVEL

Az Avtv. alapján közérdekű adatnak minősül az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő, valamint a tevékenységére vonatkozó, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől (2. §) A közérdekű adatok nyilvánosságához fűződő alkotmányos alapjog érvényesülése érdekében az Avtv. úgy rendelkezik, hogy az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy a feladatkörébe tartozó ügyekben köteles elősegíteni és biztosítani a közvélemény pontos és gyors tájékoztatását. (19. §) Ez azt jelenti, hogy lehetővé kell tenniük, hogy a kezelésükben lévő közérdekű adatot bárki megismerhesse. A megismerési jog azonban nem korlátlan: ha az adatot törvény alapján az arra jogosult szerv minősítette, illetve ha az nemzetközi szerződésből eredő kötelezettség alapján minősített adat, továbbá, ha a közérdekű adatok nyilvánosságához való jogot - az adatfajták meghatározásával – törvény: honvédelmi; nemzetbiztonsági; bűnüldözési vagy bűnmegelőzési; központi pénzügyi vagy devizapolitikai érdekből; külügyi kapcsolatokra, nemzetközi szervezetekkel való kapcsolatokra; bírósági vagy közigazgatási hatósági eljárásra tekintettel korlátozza, az adat a nyilvánosság elől elzárható.
A minősített adat védelméről szóló 2009. évi CLV. törvény hatályba lépéséig – 2010. április 1-ig – a katasztrófavédelemmel összefüggésben adatot, információt az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény alapján lehetett minősíteni. Minősítési kategóriaként az államtitok vagy a szolgálati titok merülhetett fel. A minősítés az a döntés, melynek meghozatala során az arra felhatalmazott személy megállapítja, hogy a minősíteni kívánt adat megfelel a törvényben meghatározott valamennyi feltételnek és megállapítja a minősítési jelölést. Államtitoknak akkor volt minősíthető az adat, ha beletartozott a törvény mellékletében felsorolt államtitokkörbe, továbbá a minősítési eljárás keretében az arra jogosult minősítő megállapította, hogy az adatnak az érvényességi idő lejárta előtti nyilvánosságra hozatala, jogosulatlan megszerzése vagy felhasználása, illetéktelen személy tudomására hozása, továbbá az arra jogosult részére hozzáférhetetlenné tétele közvetlenül sérti vagy veszélyezteti a Magyar Köztársaság törvényben meghatározott honvédelmi, nemzetbiztonsági, bűnüldözési vagy bűnmegelőzési, központi pénzügyi, külügyi vagy nemzetközi kapcsolataival összefüggő, valamint igazságszolgáltatási érdekeit. Szolgálati titoknak pedig akkor, ha a minősítésre felhatalmazott által meghatározott szolgálati titokkörbe tartozott az adat, és a minősítő megállapította, hogy az adat érvényességi idő lejárta előtti nyilvánosságra hozatala, jogosulatlan megszerzése és felhasználása, illetéktelen személy részére hozzáférhetővé tétele, továbbá az arra jogosult részére hozzáférhetetlenné tétele sérti vagy veszélyezteti az állami vagy közfeladatot ellátó szerv működésének rendjét, akadályozza

a feladat- és hatáskörének illetéktelen befolyástól mentes gyakorlását, és ezáltal közvetve a Magyar Köztársaság törvényben meghatározott érdekeit hátrányosan érinti. Az államtitok és a szolgálati titok fogalmi körében mind közérdekű adatok, mind személyes adatok szerepelhetnek. Az államtitok és a szolgálati titok fogalma a törvényi definíció szerint eltér, azonban Majtényi László által felvázolt rendszer szerint – amely az adatcsoportok közötti lehetséges logikai kapcsolatokat veszi számba – nem kell közöttük különbséget tenni. Csak olyan információ minősíthető államtitoknak, amely minősítésre felhatalmazott közfeladatot ellátó szerv kezelésében van. Az állam és szolgálati titok olyan adat tehát, amely egyaránt lehet közérdekű adat, illetve személyes adat, de közfeladatot ellátó szervnél keletkezik, és közfeladatot ellátó szerv kezeli. [6]

A minősítés alkalmával az államtitkot képező adat hordozóján az „Államtitok!" megjelölést és a „Szigorúan titkos!" minősítési jelölést; a szolgálati titkot képező adat hordozóján a „Szolgálati titok!" megjelölést és a minősítő döntésétől függően a „Titkos!", a „Bizalmas!",vagy a „Korlátozott terjesztésű!" minősítési jelölést kellett feltűntetni. Ezen felül az érvényességi időt, a minősítő nevét és beosztását, továbbá az adat magyar származását jelölő országjelet (MK/HU) is fel kellett a dokumentumon tüntetni. A minősítésre jogosultak körét a törvény taxatívan felsorolta. A minősítést a minősítő, illetve jogutódja rendszeresen, de államtitok esetén legalább 3 évente, szolgálati titok esetén legalább 5 évente köteles felülvizsgálni. A vizsgálat eredményeként a minősítés fenntartható, megszüntethető, vagy módosítható. Ez utóbbiakról mindazokat értesíteni kell, akinek a minősített adatot továbbították. A katasztrófavédelem területén a fenti feltételek megléte esetén minősítésre lehetőség volt a honvédelmi tárca keretében készült katasztrófaelhárítás tervei vonatkozásában. Az államtitokká minősítés leghosszabb érvényességi ideje: 90 év. A Népjóléti Minisztérium tevékenysége keretében pl. a nukleáris anyagra vagy sugárzó anyagra vonatkozó adatot lehetett a vonatkozó feltételek fennállása esetén minősíteni, míg az Országos Atomenergia Bizottság tevékenysége során keletkezett adatok közül azokat lehetett minősíteni, amelyek pl. a nukleáris üzemanyagok őrzésére, védelmére, szállítására vonatkozó adatok körében feletek meg a törvényes feltételeknek. Az első esetben a minősítési időszak maximum 90 év, az utóbbi esetben 30 év lehetett. A minősítési jelölések alkalmazásához a törvény káralapú irányadó szempontokat adott meg: „Szigorúan titkos!" minősítési jelöléshez különösen súlyos kár, „Titkos!" minősítési jelöléshez súlyos kár, „Bizalmas!" minősítési jelöléshez jelentős mértékű érdek sérelem, „Korlátozott terjesztésű!" minősítési jelölés esetén a törvényben meghatározott lehetséges hátrányos következmények fennállását rendelte.

Az Országgyűlés a minősített adat védelméről szóló 2009. évi CLV. törvény elfogadásával megváltoztatta a törvényi szabályozást. Az új jogszabály 2010. április 1-én lépett hatályba. A törvény egységesen szabályozza a nemzeti és a külföldi minősített adatok védelmét, alapelveiben az Európai Unió minősített adatainak védelmével összefüggő jogi aktusokkal összeegyeztethető szabályozást tartalmaz. A törvény indoklása szerint a jogi szabályozás megváltoztatásának elsődleges célja „a magasan minősített adatok számának radikális csökkentése, ezáltal védelmük hatékonyságának növelése és hosszabb távon a védelmi igényüknek megfelelő magas költségvetési ráfordítások csökkentése". Azon követelménynek, hogy „a közérdekű adatok nyilvánossága alkotmányos jogának korlátozására csak a jogállami keretek között, alkotmányosan indokolható esetekben kerülhet sor, a jogalkotó a káralapú minősítési rendszer további erősítésével kíván eleget tenni". A törvény a korábbi szabályozással megegyezően, taxatíve meghatározza a minősítésre jogosultak körét. E közhatalmi jogosítványokkal felruházott személyeknek, illetve a közjogi és közigazgatási szervezetek vezetőinek írásban kell meghatározniuk - bizonyos korlátozással - azokat a beosztásokat, amelyek betöltői részére minősítői jogkört biztosítanak. A

minősítésre csak a meghatározott védhető állami érdekek közvetlen sérelme, illetve veszélyeztetése esetén van mód. A korábbi államtitokköri jegyzék helyett a minősítéssel védhető érdekek körét határozza meg a törvény. A hatályos szabályozás szerint a minősítéssel védhető közérdek a Magyar Köztársaság: szuverenitása, területi integritása, alkotmányos rendje, honvédelmi, nemzetbiztonsági, bűnüldözési és bűnmegelőzési tevékenysége, igazságszolgáltatási, központi pénzügyi, gazdasági tevékenysége, külügyi vagy nemzetközi kapcsolatai, állami szerve illetéktelen külső befolyástól mentes, zavartalan működésének biztosítása.

Ugyanakkor fontos hangsúlyozni, hogy a minősítéssel védhető érdekek körébe való tartozás önmagában nem elegendő indok a minősítésre. A minősítés a kárközpontú minősítési rendszer alapul vételével történik. Ennek lényege, hogy minél nagyobb kárt okoz a minősített adat „illetéktelen kezekbe kerülése", illetéktelen által történő megváltoztatása, annál magasabb szintű személyi, fizikai, adminisztratív és elektronikus biztonsági követelményeknek kell érvényesülniük a védelem során. A kármérték tehát a védelmi intézkedések szintjét határozza meg. A törvény szerint tehát minősítéssel az adat csak akkor védhető, ha az

- minősítéssel védhető közérdekek körébe tartozik,
- nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele károsítja a minősítéssel védhető közérdeket, és
- az adat nyilvánosságát és arra feljogosított személyen kívüli megismerhetőségét meghatározott ideig korlátozni szükséges.

Fenti feltételek konjunktívak, ami azt jelenti, hogy az adat minősítéssel csak valamennyi törvényi feltétel fennállása esetén védhető, és ebben az esetben is csak a legszükségesebb ideig. A kármérték úgy veendő figyelembe, hogy amennyiben az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele:

- rendkívül súlyosan károsítja a minősítéssel védhető közérdeket, akkor „Szigorúan titkos!",
- súlyosan károsítja a minősítéssel védhető közérdeket, akkor „Titkos!",
- károsítja a minősítéssel védhető közérdeket, akkor „Bizalmas!",
- hátrányosan érinti a minősítéssel védhető közérdeket, akkor „Korlátozott terjesztésű!"

minősítéssel kell ellátni. Az érvényességi idő a „Szigorúan titkos!" és „Titkos!" minősítési szintű adat esetén legfeljebb 30 év, a „Bizalmas!" minősítési szintű adat esetén legfeljebb 20 év, míg a „Korlátozott terjesztésű!" minősítési szintű adat esetén legfeljebb 10 év lehet.

Mint ahogyan az a fentiekből látható, a törvény abból indul ki, hogy a minősítésnek objektív alapja van: azért lesz az adat minősített, mert az adathoz való illetéktelen hozzáférés az állam valamely védhető érdekét ténylegesen károsítja és a kezdeményező, illetve a minősítő ezt a tényt állapítja meg, valamint ezt felismerhetővé teszi. Ez a kárközpontú rendszer az egyes védelmi (biztonsági) intézkedések szempontjából döntő, az állampolgárok oldaláról nézve nem jelent különbséget. Az új szabályozás azzal, hogy a korábbi szabályozásban az egyes minősítők által kiadott szolgálati titokköri jegyzékeket az egységes rendszerbe integrálta, megszűntette azt az aggályos helyzetet, hogy törvénynél alacsonyabb szintű norma állapított meg alapjogi korlátozást. Fontos garanciális szabály, hogy a minősített adat e minősége érvényességi ideje csak egy, illetve a törvényben meghatározott szűk körben két alkalommal, megismételt új minősítési eljárás lefolytatása után lehetséges. Minősíteni - az eddigi gyakorlatnak megfelelően - indokolással ellátott minősítési javaslatot alapján lehetséges. Az új szabályozás megfelelő átmenetet biztosít azzal a rendelkezéssel, amely

szerint a törvény hatálybalépéséig terjedő időszakban keletkezett (korábbi) állam- vagy szolgálati titkot képező adatokat a minősítő legkésőbb 2013. június 30-ig köteles az új törvény szerint felülvizsgálni és a felülvizsgálat eredményéről a címzetteket értesíteni. Fontos garanciális szabály, hogy határidő elteltével a felül nem vizsgált nemzeti minősített adatok minősítése megszűnik.

ÖSSZEGZÉS

A szükségesség és arányosság elve mentén a közérdekű adat nyilvánosságához fűződő jogot korlátozni csak a törvényekben meghatározott feltételek fennállása, a védelemhez szükséges minősítéssel védett közérdek esetén, a megfelelő minősítési szinttel és a feltétlenül szükséges ideig lehet. Az információszabadság akkor korlátozható a katasztrófavédelemben, ha a vonatkozó jogszabályi rendelkezések ezt lehetővé teszik. További vizsgálatot igényel azonban annak a kérdésnek a megválaszolása, hogy az új minősítési kategóriák, és a minősítéssel védhető közérdekek jogszabályi meghatározása erre milyen lehetőséget ad.

E törvény számos rendelkezését több civilszervezet megtámadta az Alkotmánybíróság előtt [7]. Az alkotmányossági aggályaik arra vonatkoznak, hogy a titkosítás során a jogszabály nem kötelezi a minősítőt a nyilvánossághoz fűződő közérdek mérlegelésére.

HIVATKOZÁSOK

[1] Horváth Zita: A minősített időszakok szabályozásának rendszere, tartalma. Hadmérnök. III. Évfolyam 2. szám - 2008. június, pp: 157-160, http://hadmernok.hu/archivum/2008/2/2008_2_horvath.html (letöltés dátuma: 2009. október 19.)

[2] Dr. Bukovics István: Katasztrófavédelmi igazgatás. Verlag Dashöfer Szakkiadó Kft. Budapest, 2008.

[3] Hanka László - Vincze Árpád - Solymosi József:A nukleáris terrorizmus mint potenciális fenyegetettség napjainkban. Hadmérnök. II. évfolyam 4. szám – 2007. december, pp: 4-24., http://hadmernok.hu/archivum/2007/4/2007_4_hanka.html (letöltés dátuma: 2010. május 17.)

[4] Halász László: Monitoring és lakossági riasztó rendszer és a kritikus infrastruktúra-védelem összefüggései. Hadmérnök. III. évfolyam 2. szám – 2008. június. http://hadmernok.hu/archivum/2008/2/2008_2_nagyr.html (letöltés dátuma: 2010. május 19.)

[5] Hanák Tibor: Katasztrófajelentési rendszerek. Hadmérnök. III. Évfolyam 2. szám - 2008. június. http://hadmernok.hu/archivum/2008/2/2008_2_hanak.html (letöltés dátuma: 2010. május 19.)

[6] Majtényi László: Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága. Complex Kft. Budapest, 2006.

[7] Magyar Péter: Egységben rajong a titkokért a Fidesz és az MSZP http://index.hu/belfold/2010/05/19/egysegben_rajong_a_titkokert_a_fidesz_es_az_mszp/ (letöltés dátuma: 2010. május 19.)

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Petró Tibor
petro.tibor@zmne.hu

A MAGYARORSZÁGI PATAKOK, KISEBB FOLYÓK ÁRADÁSA OKOZTA VESZÉLYHELYZETEK, A VÉDEKEZÉS LEHETŐSÉGEI

Absztrakt

Korunk egyik legnagyobb kihívása a vízzel való komplex gazdálkodás a fenntartható fejlődés figyelembevételével. Napjainkban, a klímaváltozás hatásaként, egyre többször találkozhatunk lokális árvízi eseményekkel, amikor egy település, kistérség, vagy régió szembesül a hirtelen lezúduló nagy mennyiségű csapadék hatásaként jelentkező lokális árvízi jelenségekkel. A hirtelen, gyors lefolyású, nagy pusztító erővel bíró eseményekre fel kell készülnünk, melynek egyik fő eleme a megelőzés kell, hogy legyen. Ebben az időszakban nem szabad elhanyagolni a megelőző intézkedéseket, illetve számba kell vennünk a védekezés lehetőségeit. A cikk megírásának célja, hogy a szerző bemutassa a védekezés korszerű lehetőségeit az olyan speciális árvízi helyzetekben, ahol kisebb vízfolyások esetében az árvízvédelmi védőtöltések hiányában azonnali szükségmegoldásokat kell alkalmazni a lakosság és a javak megóvása érdekében.

One of the greatest challenges of our times is the comprehensive management of water concerning sustainable development. Today, as the consequence of global climate change, we can meet local floods more often, when a settlement, county or region have to face them after sudden, heavy rainfalls. We must be prepared for these quick, fast-moving, devastating events mainly with preventive measures. In these times we don't have to neglect prevention, and we have to clear up our defense possibilities. The aim of this paper was to present modern defensive solutions in special flood situations, along smaller creeks without bulwarks, where immediate stop-gap arrangements should be necessary to defend population and materials.

***Kulcsszavak**: árvíz elleni védelem, mobilgát, vízkár elhárítási feladatok ~ flood control, mobile dam, water damage relief tasks*

Bevezetés

Napjainkban a globális klímaváltozás okozta helyzetben, egyre többször találkozhatunk nem megszokott időjárási jelenségekkel. Ezen időjárási jelenségek a múltban is okoztak veszélyhelyzetek, pl. nagy mennyiségű, hirtelen lezúduló nagymennyiségű formájában, melyeknek árvizek, belvizek voltak a következményei. Azonban, ha megkérdezzük a környezetünkben élő idősebb embereket, akkor olyan válaszokat hallhatunk, hogy nem emlékszem volt e valaha ilyen ítéletidő, az utóbbi harminc évben egyszerre esett-e ennyi eső, mint manapság. A 2010-es év valószínűleg Magyarországon a patakok, vízfolyások, kisebb folyók és a belvíz okozta károk éve lesz, bár még csak az év első fele telt el.

Az éghajlatváltozás következtében akár 40 százalékkal is csökkenhet a következő évtizedekben a folyók nyári lefolyása Európa nagy részében, így Magyarországon is, ezzel párhuzamosan várhatóan gyakoribbak és intenzívebbek lesznek Magyarországon a potenciálisan heves árvizeket okozó "nagycsapadékok" különösen Borsod térségében. Az éghajlatváltozás hatása fokozottan érvényesül a vizeknél, heves árhullámok várhatók, és a tavak vízháztartása is várhatóan romlik majd. Feltehetően nőni fog az aszályok gyakorisága, az aszályok egyre inkább átterjedhetnek a Dunántúlra is.[1]

A lakosság anyagi javainak, életének védelme érdekében hozott hosszú távú árvízvédelmi infrastruktúra meghatározásakor ezt a kettőséget kell figyelembe vennünk. Az elmúlt évek szélsőséges időjárási körülményei és az eseményeket követő beavatkozások során szerzett tapasztalatok ismét felhívták a figyelmet arra, hogy országunk földrajzi és geológiai adottságai között a vízgazdálkodás kiemelt feladatunk. A patakok károkozása elleni védelemi infrastruktúrára jellemző a védőművek hiánya ill. hiányossága. A védekezés megszervezésekor a megelőzésre, a kialakuló káros vizek elleni fellépésre, valamint az elöntések folytán szétterült vizeknek a vízfolyásokba és csatornákba történő visszavezetésére, a károk gyors felszámolására kell terveznünk, feladatot végrehajtanunk. Tisztában kell lennünk azzal, hogy vízügyi-műszaki védelmi eszközökkel csupán mérsékelni tudjuk a károkat, nem pedig megakadályozni. Tovább nehezíti a beavatkozást, és kárfelszámolást a lezúduló nagy mennyiségű csapadék mellett megjelenő földcsuszamlás, sárlavina. Az iszap és hordalék jobb esetben csak elzárja a műtárgyakat, rosszabb esetben meg is rongálja azokat. Az ár visszahúzódása után pedig többletfeladatot jelent az elöntött területek hordalékoktól történő megtisztítás is. [1]

Árvizek elleni védelem szabályozása

A védelmi tevékenységek számbavétele előtt érdemes néhány fogalmat tisztázni, melyeket az alábbi jogszabályok fogalmaznak meg:

A vizek kártételei elleni védekezés szabályairól szóló 232/1996. (XII.26.)Korm. rendelet értelmező rendelkezése szerint:

a. *védekezés:* az élet- és vagyonbiztonság érdekében, az árvíz, a belvíz kártételeinek megelőzését, elhárítását, illetőleg mérséklését szolgáló műszaki és államigazgatási feladatok végrehajtása
b. *védekezés műszaki feladatai:* az árvizek, a belvizek időszakában a védőműveken és/vagy azok mentén, a védőművek védő-, illetőleg működőképességének megőrzése
c. *védekezés államigazgatási feladatai:* a védekezéssel összefüggő rendvédelmi, szociális és egészségügyi hatósági, továbbá a műszaki feladatok ellátásához szükséges

[1] Nováki Béla (hidrológus mérnök, a műszaki tudomány kandidátusa) nyilatkozata: www.Privatbankar.hu

munkaerő, eszköz, anyag, felszerelés rendelkezésre állása, valamint a vizek kártételei által fenyegetett területeken az élet- és vagyonbiztonság érdekében végzendő megelőző és operatív feladatok

d. *helyi vízkárelhárítás:* az árvíz-, belvízvédekezés céljából kiépített védőművek hiányában a fellépő káros vizek elleni védekezés, továbbá az elöntések folytán a területen szétterült vizeknek a vízfolyásokba, csatornákba vezetése
e. *védekezési készültség:* a veszély mértéke szerint meghatározott, a biztonság érdekben szükséges intézkedések megtételének intézményes kerete
f. *védekezési készültség fokozatai:* I., II., III. és rendkívüli védekezési készültség
g. *veszélyhelyzet:* a polgári védelemről szóló 1996. évi XXXVII. törvény (a továbbiakban: Pvtv.) 2. §-a (2) bekezdésének *g)* és *j)* pontja szerinti állapot.[2]

A Vízgazdálkodásról szóló 1995. évi LVII. törvény alapján:

a. *vízgazdálkodás:* a vizek hasznosítása, hasznosítási lehetőségeik megőrzése, a vizek kártételei elleni védelem és védekezés (vízkár-elhárítás)
b. *vízkár-elhárítás:* a károsan sok vagy kevés víz elleni szervezett tevékenység
c. *Csatorna:* egy v. egyidejűleg több vízgazdálkodási feladat (vízáteresztés, vízpótlás, belvízelvezetés, mezőgazdasági és egyéb vízszolgáltatás) ellátására alkalmas vízi-létesítmény
d. *Vízfolyás:* minden olyan természetes vagy mesterséges terepalakulat, amelyben állandóan v. időszakosan víz áramlik
e. *Meder:* a vízfolyást v. állóvizet magába foglaló természetes mélyedés v. kiépített terepalakulat, melyet meghatározott partvonalig a víz rendszeresen elborít
f. *Védmű:* a vizek kártételei elleni védekezéshez szükséges vízi-létesítmény.[3]

A vizek többletéből eredő kockázattal érintett területek meghatározásáról szóló 178/2010. (V. 13.) Korm. Rendelet alapján:

a. *vizek többlete*: az árvíz és a belvíz;
b. *árvíz*: a rendes körülmények között vízzel nem borított földterületnek a folyókból vagy kis vízfolyásokból származó ideiglenes víz alá kerülése (elöntése);
c. *belvíz*: a rendes körülmények között vízzel nem borított földterületnek a talajvízből származó vagy a csapadékvízből összegyülekező víz alá kerülése (elöntése);
d. *vizek többletéből eredő kockázat*: az árvízi, belvízi esemény valószínűségének és az árvízi, belvízi esemény által az emberi egészségben, emberi javakban, a környezetben, a kulturális örökségben és a gazdaság vonatkozásában okozott lehetséges káros következményeknek az együttese;
e. *nem szerkezeti jellegű intézkedések*: azok a beavatkozások, módszerek, eljárások, szabályok, amelyek az árvizek károkozása elleni védelmet és védekezést létesítmények nélkül segítik, így különösen: védelmi szervezet, előrejelzés, fenntartás, jogszabályok, védelmi- és lokalizációs tervek, hírközlés, adatátvitel.[4]

A védekezés szabályozása a jelenlegi magyarországi jogi környezetben jól szabályozott. Magyarország területe vízrajzi szempontok alapján 12 környezetvédelmi és vízügyi igazgatóságra (Alsó-Duna-völgyi , Alsó-Tisza vidéki, Dél-dunántúli, Észak-dunántúli, Észak-magyaroszági, Felső-Tisza vidéki, Körös-vidéki, Közép-Duna-völgyi, Közép-dunántúli, Közép-Tisza, Nyugat-Dunántúli; Tiszántúli) oszlik. A vízügyi igazgatóságok az önkormányzatokkal közösen kell, hogy megszervezzék védelmi tevékenységüket. Az állami védvonalak mentén a vízügyi igazgatóságok, míg az önkormányzati területeken az önkormányzat vezetője látja el a védelem-vezetői feladatokat. Itt az önkormányzatok saját

hatáskörben, vagy viziközmű társulatok segítségével kell, hogy biztosítsák lakóik részére a biztonságot.

Magyarország földrajzi és természeti adottságai tájegységenként nagyon változatosak. A patakok, gyors vízfolyások természetüknél fogva a hegységeink vízgyűjtő területéről indulva végezhetik pusztító tevékenységüket. Példaként napjaink egyik nagy pusztítása éppen a Borsodi tájegységet érte el, mely országunk egyik legváltozatosabb tájegysége. Itt a természetes vízfolyások vízgyűjtő területének döntő többsége, több mint háromnegyed része külföldön található, ezért a határt átszelő folyók (Tisza, Bodrog, Sajó, Hernád, Bódva) vízhozama, minősége, használhatósága jelentős mértékben a szomszéd országok természeti tényezőitől és az emberi beavatkozásoktól függ. A Tisza és a mellékfolyóinak felső szakasza különösen heves vízjárású. Gyakori, hogy az év bármely szakában nagyobb mennyiségű csapadék hatására a határszelvényekben 1 nap alatt akár több métert is emelkedhet a vízszint.

Vízkár-elhárítási fontosabb feladatai

Megelőző védelmi feladatként az önkormányzatoknak saját hatáskörben kell gondoskodniuk a tulajdonukban lévő vízfolyások, belvízcsatornák és belterületi vízrendezési művek vízkár-elhárítási, karbantartási és üzemeltetési feladatairól. E feladat eredményes elvégzése érdekében az önkormányzatnak rendelkeznie kell megbízható közműtérképpel, amely mérethelyesen rögzíti a csapadékvíz, szennyvíz, út, víz, gáz, telefonvezetékek nyomvonalát, magassági elhelyezkedését. E térképek segítségével végezhetőek el a bel és külterületi vízfolyások, medrek megfelelő karbantartása, melyek nagyban megkönnyítik a védekezési tevékenység eredményes végrehajtását. Gondoskodniuk kell az önkormányzatoknak a tulajdonukban lévő medrek felújításáról, azok áteresztő képességének felülvizsgálatáról is. E feladatok elvégzésére viziközmű társulatokat hozhatnak létre, akik ezt a feladatot, mint szakemberek átvállalják.[5]

A felkészülés időszakának következő fő eleme, hogy a védekezésre kötelezett szervezetnek ár ill. belvíz-védekezési, lokalizációs, jeges ár elleni védekezési tervet kell készíteniük. A védelmi terveknek tartalmazniuk kell mindazon dokumentumokat, adatokat, nyilvántartásokat és egyéb tervelemeket, amelyek az eredményes védekezéshez szükségesek. A vízkár-elhárítási terv tartalmi követelményeit a 10/1997. (VII.17.) KHVM Rendelet tartalmazza.

A védelmi tevékenységre felkészülés során a védelmi művek, felszerelések, eszközök, gépek és anyagok meglétének, használhatóságának ellenőrzése, az információs és kommunikációs eszközök próbája évente kötelező feladat. A felmerült hiányosságok pótlásáról a védekezésre kötelezett köteles gondoskodni.

A védekezésre történő felkészítés keretei között védekezési és vezetési gyakorlatot lehet tartani. A gyakorlatokat az önkormányzatoknál általában a polgári védelmi felkészítés keretei között hajtják végre. Szakmai gyakorlatot a Környezetvédelmi és Vízügyi Igazgatóságoknál legalább kétévenként, a víztársulatoknál négyévenként tartanak, melyeket érdemes a védelmi bizottsági gyakorlattal összehangolni a védekezésben közreműködő szervek felkészítése érdekében.

Az árvízvédelmi készültség tartalmi elemei

A védekezés megszervezése a 10/1997. (VII.17.) KHVM Rendelet 7.§-a alapján történik. Védekezéskor a védelmet ellátó szervezetek elsősorban saját erővel (munkaerő, anyag, felszerelés, gép és eszköz) kötelesek tevékenységet végezni. Azonban ha a védekezés műszaki feladatainak ellátásához a rendelkezésre álló saját erő már nem elegendő, akkor a vízügyi

igazgatóság szakemberei nyújthatnak segítséget. Az önkormányzatok vízügyi felkérésre szintén biztosítanak kiegészítő személyzetet, technikai eszközt lehetőségeik függvényében.[6]

Az árvízvédelmi készültség fokozatait (I-III., rendkívüli készenlét) ill. a hozzá kapcsolódó intézkedések végrehajtását akkor kell elrendelni, amennyiben az adott fokozatra mértékadó vízállást elérte az áradó víz mértéke, valamint további áradás várható. Amennyiben jeges árvíz veszélye áll fenn, a heves vízjárású folyók gyors áradása várható, továbbá, ha a védművek állapota ezt indokolja, a mértékadó vízállástól függetlenül magasabb készültségi fokozat is elrendelhető. A gyors lefolyású patakok elleni védekezés során azonban nem mindig van idő a megfelelő védelmi fokozat elrendelésére, de mindenképpen törekedni a helyes készenléti szint kihirdetésére, melynek főbb feladatai a következőek.

Az I. fokú készültség elrendelésekor a szakasz-védelemvezetőnek a védelmi szakaszt be kell járnia, és a védőművek, zsilipek és egyéb műtárgyak állapotát meg kell vizsgálnia. A készültség ideje alatt 12 órás nappali őrszolgálatot kell tartani. A vízállásokat szükség szerint, de naponta legalább 6 és 18 órakor kell leolvasni, feljegyezni és jelenteni.

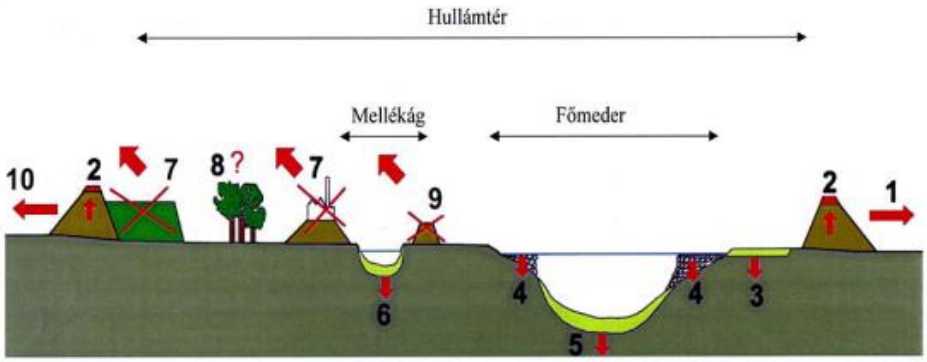
A II. fokú készültség tartama alatt éjjel-nappali őrszolgálatot kell tartani. A vízállásokat naponta 6, 12, 18, 24 órakor kell leolvasni, feljegyezni és jelenteni. A vízügyi igazgató a készültség elrendelésekor - ha további jelentős áradástól kell tartani - mozgósíthatja a védelmi osztagát vagy az osztag egyes részlegeit.

A III. fokú készültség beálltakor vészőröket kell állítani a védmű olyan pontjaihoz és műtárgyaihoz, ahol az állékonyságot súlyosan veszélyeztető jelenséget észlelnek, vagy az árvíz-védekezési terv szerint arra számítani lehet. A vízállásokat kétóránként (páros órákban) kell leolvasni, feljegyezni és jelenteni. A tetőző árvízszintek rögzítéséről és beméréséről, a vízhozam-mérésről, továbbá - szükség szerint - a légi megfigyelésről gondoskodni kell. Azt a helyet, ahol a védvonal meghibásodhat, a védekezési készletben rendszeresített jelzőzászló-készletből a fehér színűvel kell megjelölni. A megjelölt helyek felülvizsgálata alapján a fokozott megfigyelés alatt tartandó helyeket sárga, az azonnali beavatkozást igénylő helyeket piros zászlóval kell ellátni.

Rendkívüli készültségben a védelemvezető ill. vízügyi igazgató köteles gátszakadás veszélye esetén a lokalizációs tevékenység megkezdését elrendelni, és szükség esetén új lokalizációs mű kiépítése iránt a miniszternek javaslatot tenni. A veszély mértékének megfelelő számú, de legalább két árvízvédelmi osztagot, továbbá - szükség szerint - a töltések és a műtárgyak vizsgálatára különleges felszerelésű csoportokat a Törzs útján igényelni és a helyszínen készenlétben tartani.

A vízügyi igazgató javaslatot tehet a védelmi bizottságnak: a védvonalak fegyveres őrzésére, járőrszolgálat megszervezésére, a veszélyeztetett védvonalszakaszok megvilágítására; a védvonalon a védekezést ellátók kimentéséhez szükséges szállítóeszközök és mentőfelszerelés helyszíni készenlétben tartására; a veszélyeztetett területről a lakosság és az anyagi javak kimenekítésére.

Azokon a területeken, ahol a patakok, folyók töltéssel védettek, könnyebb helyzetben vannak a védekezők. A töltés, ill. magas part vonala, még ha egy-egy csúcsesemény kezelésére kevésbé alkalmas, akkor is támpontot ad a hagyományos védelmi tevékenység elvégzéséhez. Ilyen védelmi tevékenység lehet pl. a nyúlgátépítés, töltésmagasítás, bordás megtámasztás, ellennyomó medence kialakítása.



1. Az árvízvédelmi töltések áthelyezése, a hullámtér növelése
2. Az árvízvédelmi töltések magasítása
3. A hullámtér magasságának csökkentése kotrással
4. A folyószabályozási művek lehetőség szerinti átalakítása
5. A főmeder mélyítése, kotrása
6. Mellékágak kotrása, rehabilitálása
7. Épületek, egyéb létesítmények eltávolítása hullámtérről
8. Művelési ág megváltoztatása, optimalizálása
9. Nyári gátak ill. övzátonyok eltávolítása a hullámtérről
10. Szükségtározók kialakítása

1. ábra. Az árvízvédelem feladatainak összefoglalása
(Forrás: Dr. Halász László, Dr. Pellérdi Rezső, Dr. Földi László: Katasztrófavédelem I. ZMNE E Jegyzet 2009.)

Mobil gátak típusai, jellemzői

A vízgyűjtő területek egyre magasabb fokú beépítettsége, a burkolt felületek nagyságának megnövekedése miatt, a belterületi csapadékvíz-elvezetés miatt felduzzadó vízmennyiség, olyan problémák elé állítják a védekezésben résztvevő szervezeteket, melyek nem minden esetben végezhetők hatékonyan a hagyományos módon. Míg korábban a burkolatlan árkok, a patakok természetes vízmedrei lassították a lefolyás mértékét, ez napjaikra megváltozott. A külterületi csatornarendszerek viszonylagos elhanyagoltsága, a hirtelen lezúduló nagy mennyiségű csapadék tovább rontja a hagyományos védekezés lehetőségét. Ezen túl a települések egy részénél a településkép átformálásának érdekében, új alternatív védelmi módokat keresése indult.[7]

A kis vízfolyások településeken belüli, belterületi szakaszainak hossza kb. 6000 km. A jól kiépített medrek a nagy árvizeket is képesek elöntés nélkül elvezetni, ugyanakkor a külterületi levezetés, annak kiépítettsége sok esetben kívánnivalót hagy maga után. Egyes, az árvíz által fenyegetett partszakaszokon ökológiai, sport vagy turisztikai, látképvédelmi szempontok miatt egyáltalán nem épült gát, ugyanakkor a hullámtérre épült, értékes üdülő- és lakóingatlanok védelmére szükség van.

A gátak tervezésekor, telepítésekor a biztonság érdekében az alábbi tényezőket figyelembe kell venni:

a. mértékadó árvízszint,
b. gát magassága,
c. keresztmetszeti mérek,
d. egy geotechnikai fogalom, miszerint a biztonsági tényezőnek nagyobbnak kell lennie 1,6 méternél.

Árvízi védekezés újszerű technológiái

BAUER-IBS árvízvédelmi fal

A mobil árvízvédelmi fal – azért nevezik így, mert eredetileg egy betonfalból fejlődött ki - kb. 10 éves múltra tekint vissza, jelenleg ez az egyik legfejlettebb védekezési módszer. Egy viszonylag egyszerűen telepíthető mobilgát, mely a helyszínen összeszerelt extrudált

alumíniumprofilokból (oszlopokból és gerendákból) áll. A védekezés előtt a műszaki terveknek megfelelően a már korábban megépített alapra és véglegesen telepített tartóoszlopok közé szerelik. A gát maximális magassága 5 m lehet. A gát hátránya, hogy előre telepített helyen alkalmazható csak, melyet az alapozás, a mélytalaji munka kell, hogy megelőzzön. Ekkor a tervezett mobilgát alá vízzáró fal épül, amely lehet pl. szádfal, zagyfal MIP-fal vagy összemetsző cölöpfal. Az elkészült vízzáró fal tetejére egy vasbeton alapgerendát kell elhelyezni, melyre rakják a gerendákat. Szintén előzetesen építendő meg, véglegesen bennmaradó szerkezeti elemként néhány tartóoszlop. A mobiloszlopok távolsága általában 2,5–3,5 m, a teherbírási követelményeknek megfelelően.[8] Az oszlopközökbe kerülnek vízszintesen egymásra a gerendák, melynek szélessége 150 mm vagy 300 mm, vastagsága 50 mm vagy 100 mm.



2. ábra. IBS fal építése
(forrás: http://domo-bau-kft.internettudakozo.hu/domo/810qd.htm)

Minden oszlopközben a legalsó gerenda alá, speciális IBS szigetelőelem kerül, így biztosítva a megfelelő vízzárást. A gerendák a kellő magasság eléréséig egyszerűen rakódnak egymásra, a hornyos kialakítás és a feszítőékek, csavarok révén a gerenda-gerenda és a gerenda-oszlop illesztések is vízzáróak.

Az árvíz levonultával a mobilelemeket le kell szerelni, az elemeket tiszta vízzel el kell mosni, és a rendszer részét képező tároló polcokon raktárba kell szállítani, és ott tárolni, egészen a következő felhasználásig. A speciális polcrendszer alkalmazásával az elemek tartós rögzítése és szellőzése egyaránt megoldott. Előbbi a szállítás és tárolás, utóbbi a korrózió miatt lényeges, mivel így az alumínium-profilok biztosan nem érintkeznek egymással.

Előnye:

- Szabályos kialakítás és rendeltetésszerű használat esetén a mobilfal vízáteresztési mutatója ≤10 liter/óra/m2.
- Rugalmasan alkalmazható egyenetlen felületen és sarkoknál, valamint 5 méternél kisebb szintugrás esetében is.
- Értelemszerűen az élettartamán belül újrafelhasználható.
- A rozsdamentes acél és korrózióálló extrudált alumínium-elemek kezelése és fenntartása könnyű.
- A mobilgát gyorsan összerakható, az elemek egyszerű formájúak, kellően robosztusak, szimmetrikusak és funkciónként teljesen azonos kialakításúak, ezért

nem áll fenn az összecserélés miatti hibalehetőség. Mozgó vagy elektronikus alkatrész nincs.
- A szereléshez nem szükséges szakképzett munkaerő, segédmunkások is rövid, néhány órás képzést követően el tudják végezni a feladatot.

Hátránya:

- Drága
- Speciális tárolási körülményeket igényel
- Összeszereléséhez speciális szerszámok szükségesek
- Előre telepített, áthelyezése időigényes
- A szigetelőelemeket a napsugárzástól óvni kell.

Az IBS mobilgát egy oszlopközét önállóan is alkalmazhatjuk, például egy kapu, ablak, ajtó lezárására. A hullámtéri épületek esetén praktikus megoldás lehet a nyílászárók védelmének kialakításakor. Ekkor az oszlopokat előzetesen, az árvíz elől lezárandó falnyílás két oldalára kell telepíteni, majd az árhullám megérkezése előtt gyorsan helyére kell illeszteni a szigetelőelemeket és a gerendákat, így a vízmentes lezárás gyorsan megoldható.



3. ábra. Nyílászárók árvízvédelme
(forrás:http://www.hochwasserschutz.de/en/produktbereiche/hochwasserschutz-tueren-fenster.php)

Quick Damm mobil gát

Egy viszonylag gyorsan felépíthető mobil gát típus, amely egy ellenálló geomembrán anyag egy fémvázra rögzítve. Az elemek általában 2-2- méteres darabokból állnak, melyek rendszerbe köthetőek. A védmű magassága általában 150-160 cm lehet. A vályú formájú szerkezet stabilitását a beletöltött, víz vagy homok súlya adja. A föld-, vagy víztöltés súlya hozzápréseli a geomembránt a szomszédos felületekhez, - ez lehet a talaj, egy függőleges fal vagy egy másik Quick Damm elem - megakadályozva ezzel a folyadék szivárgását a szerkezet alatt és a függőleges csatlakozási helyeknél. Ugyanakkor homokzsákokból emelt nyúlgáthoz is lehet csatlakozni a Quick Damm elemet.



4. ábra. Mobil árvízvédelmi töltés
(forrás: http://www.domobau.hu/kornyezetvedelem/arviz.html)

Előnye:

- Gyorsan építhető, viszonylag kis munkaerő igénnyel
- Helyi viszonyokhoz igazítható egyedi gyártási lehetőség
- Rendszerbe köthető, különböző típusú elemek kaphatóak, melyek a következők:
  - Ajtóvédő, mely segítségével megoldható, hogy egy elöntött terepre nyíló ajtót a víztől megvédjünk, miközben működését nem akadályozzuk.
  - sarokelem segítségével akár 90°-os kanyar is kialakítható a gát vonalán, megtartva annak előnyös tulajdonságait, vízbiztonságát.
  - lefolyóvédő felhasználása révén a lefolyók árvíz idején is problémamentesen tovább használhatók, tartalmuk nem fog az útra kifolyni.

Hátránya:

- drága
- nem tudja felvenni a talaj egyenetlenségeit
- altalaji szivárgás ellen nem nyújt védelmet
- sérülése esetén veszélyforrássá válhat
- speciális karbantartási, tárolási igényű
- használat után fertőtleníteni kell az árvízi hatások miatt

A mobilgát építése különös szakértelmet nem kíván a rendszer telepítése, műszaki leírása szerint 4-6 ember egy óra alatt, feltöltés nélkül 100 fm mobilgátat tud felépíteni.[9]



5. ábra. Mobilgát szerelés
(forrás: http://domo-bau-kft.internettudakozo.hu/domo/810qd.htm)

A Quick Damm mobilgát ajánlott felhasználási területe lehet:

- Ideiglenes nyúlgátként burkolt és tömörített földalapokon egyaránt

- Gátmagasító elemként, statikus víznyomás és hullámverés ellen is
- Gátmegszakítások vagy kulissza nyílások (út, bejárat, átvezetések) lezárására
- Belvízi védekezés során

Környezetvédelemben

- Olaj és oltóvíz visszatartására
- Olaj, szennyvíz, higított vegyszerek ideiglenes tárolására
- Oltóvíz tárolására

Aqua-Barrier árvízvédelmi rendszer

Ez az árvízvédelmi rendszer csekély össze ill. szétszerelési ráfordítással építhető ki. A rendszer alapja egy galvanizált acéllemezből előállított megtámasztó lemez. A védekezés során 1,8 m-es védekezési magasságot érhetünk el. A rendszer összeszerelése során a felállított megtámasztó lemezre 45°-ban döntve kerülnek az EUR raklapok. Annyi megtámasztást ill. raklapot kell egy más mellé állítani, amíg el nem érjük a kívánt hosszt. A megtámasztott raklapra szálerősített műanyag fóliát fektetünk, aminek az alját homokzsákkal leterheljük, és felülről kapcsokkal biztosítjuk. Amikor az elzárás megkapja a vízterhelést, a nyomás és az önsúly hatására a rögzítő karmok lenyomódnak és a súrlódási erő rögzíti a szerkezetet. A megtámasztások nem igényelnek külön rögzítést.[10]



6. ábra. Aqua Barrier árvízvédelmi rendszere
(forrás: www.vidranet.hu)

előnye:

- flexibilis, ugyanakkor nagyon gyorsan, csekély élőmunka ráfordítással felépíthető.
- A használat után a rendszer szétszerelhető, letisztítható és helytakarékosan raktározható. Csak az állványrendszert és a fóliákat kell raktározni, a raklapok bérelhetőek, nem igényelnek saját raktározást
- Egy álló helyzetű raklappal (1,25 raklap/m) lehetővé válik a hagyományos rendszerű 80 cm magas homokzsák-elzárás (nyúlgát) kiváltása, ami 45-50 db homokzsákot, és 1,5 t homokot jelent.
- felhasznált homok mennyisége 5%-a homokzsákos elzárásnak, így a helyreállítás költsége is csak kb. 5%-a a hagyományos, homokzsákos módszernek.

hátránya:

- Homokzsák használatát teljes mértékben nem váltja ki
- nem tudja felvenni a talaj egyenetlenségeit
- altalaji szivárgás ellen nem nyújt védelmet
- sérülése esetén veszélyforrássá válhat
- speciális karbantartási, tárolási igény
- használat után fertőtleníteni kell az árvízi hatások miatt

A mobilgát rendszerek fejlesztőinek általában a célja, hogy az árvízvédelemben a hagyományos eszközökkel egyáltalán nem vagy csak nehezen megoldható, lokális jellegű problémákra műszaki, gazdaságossági és esztétikai szempontokból egyaránt kedvező, hosszú távon alkalmazható megoldást találjanak, amellyel magánszemélyek, közösségek biztonságban tudhatják az életüket, anyagi javaikat. E változatos védelmi rendszerek egy-egy jól körülhatárolt probléma megoldására alkalmasak lehetnek, sok esetben azonban a fizikai munkát, a homok és homokzsákolás problematikáját nem oldják meg. Minden döntés előtt meg kell vizsgálni és mérlegelni kell a rendszerek előnyeit, hátrányát, csak így hozható felelős döntés az emberélet és anyagi javak védelmének érdekében.

Összefoglalás

Magyarország természeti, ezen belül az ár- és belvízi veszélyeztetésének főbb okai között a földrajzi,- és éghajlati viszonyait, a vízgyűjtő területeken az emberi beavatkozások, időjárási viszonyok hatásait találjuk. A folyók, patakok árvízi tevékenységével együtt kell élnünk, azonban folyamatosan fel kell készülnünk az árvíz pusztító hatásai elleni leghatékonyabb védelemre.

Napjainkban a kisebb vízhozamú patakok, folyók árvízi védelme egyre fontosabb tényezővé válik. A hagyományos védelmi technológiák mellett, megjelennek új, korszerű védelmi lehetőségek is, melyek használatát a helyi védelmi tevékenység megszervezésekor érdemes megfontolni. A lakosság önvédelmének fejlődésével, a kézi erő háttérbe szorulásával, ezen technológiáknak létjogosultsága folyamatosan nő. Sokszínű megoldás létezik egy-egy védelmi tevékenység megoldására, melyek közül nem könnyű dönteni. A dolgozat célja volt néhány új technológia felvillantása, - a teljesség igénye nélkül - azok előnyének, hátrányának kihangsúlyozása mellett.

E technológiák meghonosítása viszonylag magas beruházási költsége és a helyi viszonyokra történő egyedi adaptálása miatt lassú, így sok esetben marad a hagyományos árvízvédelmi tevékenység, melynek költséghatékonysága szintén hagy kívánni valót maga után, főleg a kárenyhítés, kártalanítás költségeit is beemeljük a védelmi költségek közé.

Irodalomjegyzék

[1] Hankó Márta - Földi László „Divatos” gondolatok a klímaváltozásról Hadmérnök III. Évfolyam 1. szám - 2008. március (20-26.o.)

[2] 232/1996. (XII. 26.) korm. rendelet A vizek kártételei elleni védekezés szabályairól

[3] 1995. évi LVII. törvény A vízgazdálkodásról

[4] 178/2010. (V. 13.) korm. rendelet A vizek többletéből eredő kockázattal érintett területek meghatározásáról, a veszély- és kockázati térképek, valamint a kockázatkezelési tervek készítéséről, tartalmáról

[5] Tunyogi Dóra - Földi László 2006. évi magyarországi árvíz során végzett elhárítási munkálatok elemzése, különös tekintettel a Magyar Honvédség szerepvállalására Hadmérnök II. Évfolyam 2. szám - 2007. június (50-61.o.)

[6] 10/1997. (VII.17.) KHVM Rendelet az ár és belvízvédekezésről

[7] Dr. Halász László, Dr. Pellérdi Rezső, Dr. Földi László: Katasztrófavédelem I. ZMNE e-jegyzet 2009.)

[8] http://www.muszakilapok.hu/kornyezetvedelem/mobilgatak-arvizvedelemben

[9] http://www.domobau.hu/kornyezetvedelem/arviz.html

[10] http://www.vidranet.hu/honlap/mobilgat.htm

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Révai Róbert

Bedros J. Róbert

Istvanovszki László

Huszár András

Székely György

A SZERVEZETT BŰNÖZÉS EGÉSZSÉGBIZTONSÁGI ASPEKTUSAI

Absztrakt

Szerzők áttekintik a szervezett bűnözés modern megjelenését és az ellene kidolgozott stratégiát. A stratégia része a fenyegetettség értékelési metodika (OCTA), mely az utóbbi időben szemléleti változáson ment át.
Az OCTA módszertana vizsgálja a szervezett bűnözés tevékenységének hatását a politikára, a gazdaságra, a társadalomra, a műszaki életre, a környezetre és a jogrendszerre.
A szerzők megállapítják, hogy a vizsgált területek sorában az egészségügy területét még nem nevesítették, pedig a szervezett bűnözés egészségügyi problémákat okozó tevékenysége széleskörű: illegális orvosi tevékenység, illegális gyógyszerkutatás-, előállítás ill. kereskedelem, beleértve a kábítószer hatású szereket is.
Az emberkereskedelem összefügg az illegális szervkereskedelemmel ill. szexiparral.
Mindezen tevékenységekben közös a közegészségügyi helyzetre gyakorolt káros hatásuk. Szerzők emiatt indokoltnak tartják, hogy a szervezett bűnözés fenyegetettségének vizsgálati területei között az egészségügy is nevesítve legyen.

Autors review the emergence of modern organized crime and against the strategy. The strategy is part of the organised crime threat assessment (OCTA) methodology, which has recently undergone a drastic change in thinking. The OCTA methodology to examine the impact of organized crime in politics, economy, society, the technical life, the environment and the legal system. The authors found that the test areas, health areans have not yet quantify, and the

activities of organized crime, causing widespread health problems: illegal medicial activity, illegal drug research, production, and trade, including narcotic drugs as well.
Human trafficking is linked to the illegal organ trade and prostitution. All of these activities to the public health situation, common adverse effects. Authors are therefore appropriate that the threat of organized crime in the areas of health care can be named.

Kulcsszavak: *szervezett bűnözés, egészségügy ~ organized crime, public health*

BEVEZETÉS

Korunkat soha nem tapasztalt intenzitású fejlődés jellemzi, melynek pozitív és negatív velejárói együttesen érzékelhetők a társadalom, gazdaság különböző szegmenseiben. Hatásaként mind szélesebb igény jelentkezik a problémák összetett, több tudományterületet együttesen alkalmazó komplex megközelítésre.

Különösen helytálló ez a megállapítás a szervezett bűnözés elleni harcra, ahol az ellenfél szinte korlátlan anyagi bázissal, technikai felszereltséggel és szakértői támogatottsággal rendelkezik. További térnyerésének megakadályozására a tudomány és technika nyújtotta lehetőségek koncentrációjával, a nemzetbiztonsági, rendvédelmi és igazságszolgáltatási szervek tevékenységének hazai és nemzetközi összehangolásával nyílik reális esélyünk.

Az ezredfordulót követő tíz év megrázó eseményei még a változások szükségessége iránt leginkább kétkedőket is rádöbbentette arra, hogy a bűnüldözés korábbi módszerei önmagukban nem alkalmasak az új típusú kihívások észlelésére és kezelésére. A *szervezett bűnözés* globális térhódítása, a főként vallási alapokon nyugvó *terrorizmus* világméretű előretörése megmutatta, hogy még a legnagyobb, leggazdagabb országok sem képesek hagyományos módszerekkel gátat szabni az állam demokratikus intézményrendszereit és polgárait fenyegető veszélyeknek.

A bűnözés immár világméretű, határokon és kontinenseken átnyúló globalizációja mindenképpen egy új típusú bűnüldözés megteremtését és működtetését követeli meg, melyet a nemzetközi szervezetek (ENSZ, EU) egyöntetűen szorgalmazzák.

A FENYEGETETTSÉG ÉRTÉKELÉSI METODIKA

Ez a felismerés és törekvés érhető tetten az Európai Unió Tanácsa által 2005-ben, a Hágai Program keretében kidolgozott koncepciójában.[1] A Közösség jövőbeli biztonságpolitikáját jelentős mértékben meghatározó uniós norma és végrehajtására készített akcióterv összegezte, egyben súlyozta a Közösség biztonságát leginkább fenyegető tényezőket, prioritásokat. Az integrált fellépés egyik fontos eszköze a szervezett bűnözés helyzetének értékelését biztosító új módszertan bevezetése volt.[2]

Az fenyegetettség értékelési metodika (**O**rganised **C**rime **T**hreat **A**ssessment=OCTA) szemléletbeli változást igényelt. Szakítva a korábbi években alkalmazott éves visszatekintő

[1] The Hague Programme (2005/C 53/01)
[2] Action Plan Implementing the Hague Programme (2005/C 198/01)

jellegű helyzetértékelésekkel, a proaktív, jövőbe mutató, a biztonsági kockázatokat vizsgáló és feltáró tematika pilléreit rakta le. Bevezetésével az Europol a minőségi műveleti információkra épülő értékelési mechanizmus irányába szorgalmaz elmozdulást annak érdekében, hogy mind nemzeti, mind pedig nemzetközi szinten előrelépés történjen a határokon átnyúló bűnözés elleni harcban.

Az OCTA módszertana a vizsgált bűnszervezetek és alacsonyabb szervezettségi szintű bűnöző csoportok tevékenységének politikára, gazdaságra, társadalomra és a műszaki életre (**P**olitical, **E**conomical, **S**ocial, **T**echnological = PEST) gyakorolt hatásmechanizmusára koncentrál, mely 2006-ban kiegészült további két vizsgálati területtel: környezeti (**E**nvironmental) és jogi (**L**egal) szempontok = PESTEL.
A szervezett bűnözésnek az államszervekre, társadalomra, gazdaságra és egyénre gyakorolt hatásait a megtámadott célpontok és a támadó struktúrák erősségének és gyengeségeinek, továbbá a beavatkozás lehetőségeinek és veszélyeztetettségeinek (**S**trenghts, **W**eaknesses, **O**pportunities, **T**hreats = SWOT) függvényében praktikus vizsgálni.[3]

A fenyegetett területek bővülő listája

A fentiekből látható, hogy a nemzetközi és hazai bűnüldözést támogató elemző és koordinatív szervek pontosan érzékelik a nemzetközi és honos szervezett bűnözés aktivitását és befolyási törekvéseit, a hagyományosnak tekintett bűnözési szektorokon kívül eső területekre gyakorolt hatásait.

Azt már egyetlen külföldi és hazai tanulmány sem vitatja, hogy a szervezett bűnözés - a bűnözés e magasabb minőségi formája - egyaránt hatást gyakorol a klasszikus bűnözési területekre és a legális szférákra. Több mint tíz évvel ezelőtt jelezték a szakértők műveleti adatokra hivatkozva, hogy a bűnszervezetek a felhalmozott pénzügyi erejüket felhasználva a legális gazdasági struktúrákat támadják, egyben maguk is létrehoznak, működtetnek törvényes vagy annak látszó vállalkozásokat. Az ezredforduló táján már egyértelművé vált, hogy a befolyásolás következő színtere a központi és helyi államigazgatás, az igazságszolgáltatás valamint a média.

A fenyegetett célpontok bővülő listája (PESTEL) azonban nem, vagy önállóan még nem nevesítette az *egészségügy* területét, annak ellenére, hogy több – a már az új elemzési metodika felhasználásával készített – tanulmány, a kormányzat és a nemzetbiztonsági, rendvédelmi szervek számára gyártott stratégiai elemzés foglalkozott a bűnszervezetek egészségbiztonságot is érintő bűnös megnyilvánulásaival.[4]

AZ ORVOSTUDOMÁNY HELYE ÉS LEHETŐSÉGEI A SZERVEZETT BŰNÖZÉS ELLENI HARCBAN

Az orvostudomány bővülő nemzetközi és hazai ismeretanyagának mind szélesebb körű bevonását a szervezett bűnözés elleni küzdelembe több racionális ok is indokolja. Egyrészt maga a bűnözés is alkalmaz egészségügyi ismeretekkel rendelkező szakértőket, legtriviálisabb példája a szúrt és lőtt sebek illegális ellátása. Az orvosi ismeretek felhasználása ettől

[3] Istvanovszki László.-Kenedli Tamás: Új értékelési módszerek alkalmazása a szervezett bűnözésre (Magyar Rendészet 2007/1-2)
[4] Jelentés a korábbi évek bűnügyi helyzetképéről és végrehajtott intézkedésekről OBmB. 2009.

lényegesen szélesebb spektrumon mozog, a kábítószer hatású, tiltólistán nem szereplő szerek kidolgozásától, az illegális gyógyszerkereskedelmen, az embercsempészet-, emberkereskedelem alanyainak egészségügyi ellátásán túl, a szervkereskedelemig bezárólag.

Más megközelítésben viszont a hazai tapasztalatok is azt mutatják, hogy az orvosi szakértelem, különösen az igazságügyi orvostan jól hasznosíthatóan egészíti ki a felderítők, bűnüldözők egyes szakterületre, vagy konkrét bűnügyi probléma megoldására vonatkozó ismeretanyagát.

Különösen indokolt ez a komplex megközelítés és a több szakmai területet érintő együttműködés a különböző békefenntartó missziókban való katonai és rendőri részvételre való felkészítés során, illetve a feladatteljesítésnél, ahol együttesen és koncentráltan jelentkezik a terrorizmus és szervezett bűnözés, valamint az egyéb egészségbiztonsági, élelmezésbiztonsági kockázat.

A bűnszervezetek egészségbiztonsági szempontból kockázatosnak ítélt tevékenysége változatos képet mutat. A továbbiakban részletes elemzés tárgyává tesszük az egyes bűnügyi területeket és saját értékelést adunk az adott probléma egészségbiztonsági megoldási lehetőségeiről.

Prostitúció – nemi betegségek

A klasszikusnak tekinthető női - és az utóbbi 15 évben mind jobban terjedő férfi - prostitúciós tevékenység a bűnügyi alapproblémán túl számos egészségügyi veszélyt hordoz.

A szervezett bűnözés elleni törvénycsomagként megismert 1999. évi LXXV. törvény egyik legfőbb célkitűzése az uniós integráció időszakában rendkívül irritáló mértéket öltött utcai prostitúció szabályozott keretek közé történő szorítása volt, mind közigazgatási, mind pedig közegészségügyi szempontból. Az ellenőrzöttség kívánalma természetesen magába foglalta volna a rendszeres egészségügyi szűrővizsgálatokat is.

Ez a komplex jogalkotói igény azonban csak részben valósult meg, okainak részletezése nem e tárgyú tanulmány feladata, a kialakult helyzet egészségbiztonsági aspektusainak bemutatása sokkal inkább. A felemás módon megvalósított jogszabály következtében az utcai prostitúció valóban visszaszorult, ezzel párhuzamosan megszaporodtak a média, később az internet felhasználású hirdetések, az éjszakai szórakozóhelynek, masszázsszalonnak álcázott szex-klubok, bordélyok száma mindkét nem számára.

A *nemzetközi emberkereskedelem* közvetítésével - gazdasági vagy fizikai kényszer hatására - prostitúcióra kényszerített külföldiek jelentek meg mind nagyobb számban a magyar és nyugat-európai szex-piacokon. A kelet-nyugat irányú szex-kereskedelem rendkívüli egészségügyi kockázatokat hordoz a HIV fertőzések vonatkozásában, hiszen Nyugat-Európában 6-800 ezer, Kelet-Európában ugyancsak 8-900 ezer főre becsülik a fertőzést hordozók számát.
Számottevő növekedést tapasztaltak az utóbbi években Oroszországban és a közeli Ukrajnában, mely országok jelentős exportőrei a szex-iparnak. A világ távolabbi, de az emberkereskedelem hatókörébe tartozó ázsiai és afrikai térségekben további 30 millió fertőzött él.[5]

[5] Reports on the globál AIDS epidemic UNAIDS 2008

A folyamat közegészségügyre gyakorolt hatásaként hazánkban 2006-tól növekvő tendencia mutatkozik az újonnan regisztrált HIV fertőzöttek viszonylatában. Az ismertté vált betegek száma az 1985 óta történő összesítő adatgyűjtés szerint 1730 fő körüli. Az ország legfertőzöttebb térségei Budapest mellett Pest és Fejér megye. A regisztrált betegek jelentős része nemi úton szerezte a fertőzést, 52 % igazoltan homo-, illetve biszexuális. A bizonyíthatóan kábítószer-fogyasztással összefüggő fertőzések száma nem éri el a 2%-ot. Megjegyzést érdemel, hogy az esetek egynegyed részében nem tisztázott a betegség megszerzésének módja. [6]

Ugyancsak növekvő tendenciát mutat az egyéb nemi úton terjedő fertőző betegségek száma, a klasszikusnak tekintett három alapbetegségből éves szinten mintegy 1500 új esetet regisztrálva. Nyugtalanító képet mutat a szifilisz fertőzöttek számának emelkedése.

Illegális kábítószer-kereskedelem

Szorosan kapcsolódik a témához az illegális kábítószer-kereskedelem, az előállítás, terjesztés és fogyasztás, mely egyszerre jelent közvetlen és közvetett egészségügyi problémát. Az EU 2008-ig tartó, majd második ütemében 2009-2012 időszakára szóló kábítószer-bűnözés elleni stratégiája kiemelt figyelemben részesíti a probléma szociális és egészségügyi aspektusait mind a prevenció, mind pedig a rehabilitáció, reintegráció vonatkozásában.

A munkaképesség csökkenése, a kiesett munkaidő, az elvégzett munka minőségének és mennyiségének megváltozása, továbbá a rehabilitáció társadalombiztosítási költsége ugyanis mindenképpen kalkulálható anyagi- és humán erőforrási tényező.

A kábítószer-bűnözés a nemzetközi szervezett bűnözés legjövedelmezőbb üzletága. Mindez jól tükröződik a magyarországi bűnszervezetekkel kapcsolatos felmérésekből, az éves lefoglalási adatokból, melyek a regisztrált bűnszervezetek mind nagyobb aktivitásáról, a hazai felvevő piac folyamatos (lassú) bővüléséről tanúskodnak.

A kábítószert fogyasztók számát kétféle megközelítés alapján tudjuk meghatározni, egyrészt az egészségügyi, másrészt a bűnügyi statisztikai adatok figyelembevételével.
Hangsúlyozni kell, hogy mindkét érték csupán a kezelés vagy eljárás során regisztrált eseteket tartalmazza, a fogyasztók másik csoportja kívül esik az állami kontrollon, a rájuk vonatkozó számadat már csak a különböző módszerek felhasználásával kombinált becsült érték.

Éves szinten egészségügyi ellátásban részesülő fogyasztók száma a 14 ezret meghaladja, az újonnan regisztrált betegek száma az ellátottak 28%-a. A rendszeres kábítószerélvezők esetében 24 ezer fővel, ezen belül is a kritikusabb csoportnak tekintett heroin-használók vonatkozásában 3-6 ezer fővel kalkulálnak.[7] Utóbbiak közül a jelentős egészségügyi kockázatot a kezelésben nem részesülő úgynevezett rejtett intravénás népesség jelenti, ebben a fogyasztói körben legmagasabb a használat során terjedő fertőzőbetegségek (HIV, HBV, HCV) előfordulásának veszélye és annak tartós látenciába maradása.

Az ENSZ és EU ajánlásainak megfelelően a nemzetközi és hazai szűrőrendszerek különösen nagy figyelmet szentelnek az intravénás drogfogyasztók kontrolljának, a 90-e években drasztikusan megszaporodott HIV előfordulások miatt. A friss kutatatási adatok arról

[6] Országos Epidemiológiai Központinformációs tájékoztatója EPINFO 2009/45, 47. szám
[7] Nemzeti Drog Fókuszpont 2009. évi jelentése az EMCDDA számára

tanúskodnak, hogy a megelőző intézkedések (szűrés, tű-csereprogram, felvilágosító kampány) hatására a HIV terjedést sikerült megállítani, néhány balti állam Oroszország és Ukrajna statisztikai mutatói továbbra is aggodalomra adnak okot.[8]

Hazánkban a vizsgálatok tanúsága szerint az intravénás fogyasztók között nem jellemző a HIV fertőzöttség, sokkal reálisabb veszélyt hordoz előfordulásának gyakorisága miatt a Hepatitisz C. A regisztrált fertőzöttek kb. 30%-a bizonyul pozitívnak, függve a fecskendőhasználati szokásoktól, a fecskendő típusától stb.
A kétrészes fecskendőt használóknál, illetve az egyrészes fecskendőt receptíven megosztva, tisztítatlanul használva ez akár a kétszeresét is elérheti. [9]

Bűnügyi szempontból ugyancsak problematikus a fogyasztói/terjesztői arányok és adatok felmérése. A bűnügyi statisztika éves szinten 3-6000 bűncselekményt regisztrál, utóbbi három év átlagát tekintve kb. 5000 elkövetővel.

Tekintettel arra, hogy a kábítószer bűnözés olyan jogsértés, ahol a fogyasztás és terjesztés egyaránt büntetendő magatartás, az ismerté vált elkövetők száma magába foglalja a büntetőeljárás jogi szempontból regisztrált kábítószer-élvezőket kb. 80-85 % részesedést képezve. A valódi rendszeres fogyasztók száma, még a legóvatosabb becslések szerint is ennek öt-tizenkétszerese, 50-80 ezer fogyasztóval kalkulálva.

A hivatásos állomány körében előforduló kábítószer-fogyasztás

Speciális problémát jelent a büntetés-végrehajtási, rendvédelmi, illetve honvédségi objektumokban, illetve ezen szervek hivatásos állománya körében előforduló kábítószer-fogyasztás. Nem szükséges külön részletezni a kábítószer befolyás alatt álló békefenntartó katona - utalva a válsággócpontok Afganisztán, Balkán, Közel-Kelet stb. kiemelt fertőzöttségére - a veszélyes bűnözőket őrző, kísérő fegyőr, a személyi szabadságot korlátozó intézkedést foganatosító vagy tömegoszlató rendőr milyen mértékű biztonsági kockázatot jelent.

A felvételi pályaalkalmassági eljárás, illetve a szolgálatra vezénylés során való kontroll szükségességét jól igazolja egy 2006-os honvédségi szűrővizsgálat eredményeit bemutató 2007-es publikáció.[10] Az alkalmassági vizsgán 76, hatósági ellenőrzés során 33, preventív vizsgálat során 17 személy esetében mutattak ki kábítószer-fogyasztást. A szűrés tanúsága számos tapasztalattal járt egyrészt a Magyar Honvédség komplex szűrővizsgálati rendszere, másrészt a prevenciós stratégia vonatkozásában.

A Rendőrség 2005-ben kidolgozott drogstratégiájának ugyancsak részét képezte a hivatásos állomány tagjainak kábítószer-használat vonatkozású szűrése, ellenőrzése. Ennek a szükséges jogi, szervezeti és anyagi feltételeit a HM által kidolgozott és eredményesen alkalmazott tematika ismeretében biztosítani kell.

[8] EMCDDA Annual Report 2007.
[9] Nemzeti Drog Fókuszpont 2009. évi jelentése az EMCDDA számára
[10] Jelentés a magyarországi kábítószerhelyzetről Szociális és Munkaügyi Minisztérium 2007

A kábítószerfajták fogyasztás szerinti megoszlása

Az egyes kábítószerfajták fogyasztás szerinti megoszlása az elmúlt évek adatai alapján jelentős változást nem mutat, az úgynevezett „discodrogok", az amfetamin, ecstasy és kannabisz-származékok dominenciája érvényesül a hazai fogyasztók körében is.

Mind bűnügyi, mind egészségügyi szempontból jelentős tényező a függőség kialakulásának mértéke, a kábítószer-adagolás miatti halálesetek oka és tendenciája, a kábítószer és kábító hatású anyagok használata miatt bekövetkezett átmeneti vagy végleges egészségügyi károsodás.

Éves viszonylatban 400 fő körüli a drogfogyasztással közvetlenül összefüggő elhalálozás. Továbbvizsgálva a megoszlást, a heroin túladagolása miatt elhunytak száma 20 körüli, az esetek mögötti ok általában a beszerzési források, csatornák módosulása, kevésbé hígított termékek piacra kerülése vagy a közelmúltban lezajlott tragédiáknál szennyezett adalék felhasználása volt. Más drogok fogyasztásából fakadó elhalálozások további 5-10 esetet jelentenek. Az egyéb kábító hatású anyagokkal (gyógyszerek, szerves oldószerek) összefüggő halálesetek száma jelenti a nagyobb hányadot, 350 körülit.

Fő ellenség továbbra is több vonatkozásban a heroin, volt azonban már halál okozója egyéb ópiát, illetve a kokain is. Egyes vegyi szakértői vélemények rámutatnak arra, hogy a média által „lágydrogként" jellemzett marihuána cannabis tartalma növekvő koncentrációt mutat, akár 12% THC-t is elérve erőteljesebb függőséget, jelentősebb személyiségtorzulást okoz.[11] Ezen túlmenően egyéb egészségkárosító hatásokra hívják fel kutatók a figyelmet, többek között a súlyos és visszafordíthatatlan légzésfunkció károsodásra.

A kábítószer tiltólista kijátszása állandó kihívást jelent a nemzetközi szervezett bűnözés által alkalmazott vegyészeknek. Évente jelenik meg új hatóanyag a piacon, hónapokba, évekbe kerül, míg jogilag is kábítószernek minősítik. Igen jellemző példa volt az mcpp ezredfordulót követő megjelenése, melyből hazánkban 2005-ben többet foglaltak le (80 ezer db.) mint egész Európában.

Mindenképpen említést érdemel a kábítószerek élettani vonatkozása a kábítószer hatása alatt elkövetett bűncselekmények viszonylatában. A nyomozati adatok szerint mind nagyobb számú (évi 3-4000) bűncselekményt követnek el kábítószer hatása alatt, ezek jellemzően erőszakos vagyon elleni, erőszakos nemi erkölcs elleni jogsértések vagy a közlekedés biztonságát veszélyeztető delictumok.

Részkövetkeztetésként elmondható, hogy az orvosi és kriminalisztikai ismeretek komplex alkalmazásának kiváló példája volt a rendőrség drogstratégiájának 2005-ös kidolgozása, ahol a munkacsoportba a bűnmegelőzés, bűnüldözés, bűnelemzés szakemberei mellé a bűnügyi (igazságügyi) orvostan képviselőit is bevonták. Javaslatukra került be a stratégiába a kábítószer túladagolások következtében bekövetkezett egészségkárosodások, halálesetek szakértői információinak felderítési célú visszacsatolásának szükségessége és lehetősége.

Ugyancsak ebben a munkacsoportban fogalmazódott meg ajánlás a vegyi-, toxikológiai szakértői véleményeknek a Robotzsaru Integrált Ügyviteli és Ügyfeldolgozó Rendszerbe

[11] Kábítószer-és Kábítószer-függőség Európai Megfigyelőközpontja EMCDDA 2004. évi jelentése

történő digitalizált feldolgozására, mely további lehetőséget biztosít az ügysorozatok, terjesztői hálózatok feltárására, személyi és tárgyi összefüggéseik bizonyítására.

Hasonló megközelítést tükröz a ZMNE Katonai Műszaki Doktori Iskoláján készített PhD. értekezés egyik kutatási szempontja, amelynek szerzője - több tudományos kérdés között - azt vizsgálta, hogy a PTE ÁOK Igazságügyi Orvostani Intézete, valamint Laboratóriumi Medicina Intézete által az országban egyedülállóként bevezetett integrált extrakciós-analitikus rendszer (TOX.I.S.) - a szakértői funkción kívül - milyen további bűnmegelőzési, felderítési lehetőségeket hordoz.[12]

Az eltelt csaknem öt év igazolta a kezdeményezés szükségességét és az együttműködés új területei bontakoztak ki, kábítószerszondák alkalmazása és lehetőség szerinti egységesítése, az állomány munkaegészségi szűrése a kábítószer hatása alatt elkövetett bűncselekmények vizsgálata stb.

A korábban leírtak alapján látható probléma a kábítószer élvezők számának lehető legpontosabb meghatározása, melynek bűnügyi és egészségügyi vonatkozásai egyformán lényegesek.

A megválaszolandó kérdés az, hogy a rendőrségi eljárások és az egészségügyi szervek gyógyító tevékenysége során látókörbe kerülő kábítószer-fogyasztók azonosak-e, illetve mekkora mértékű a két halmaz közötti átfedés?

Tudományos újdonságként lehet beszámolni arról az együttműködésről, mely az ÁNTSZ szervezeti keretei között működő Nemzeti Drog Fókuszpont és az IRM-ORFK között jött létre a fenti probléma tisztázására, a személyiségi jogok, adatvédelmi szabályok szigorú megtartása mellett, statisztikai adatokra építve. A kutatás célja annak meghatározása, hogy mekkora azonosság mutatható ki a büntetőeljárás és az egészségi kezelés alá került fogyasztók körére, az esetekben szereplők anonimizálásával.

Az illegális hulladékkereskedelem egészségbiztonsági kockázatai

Egy más típusú bűncselekményfajta egészségbiztonsági veszélyeire is felhívnánk a figyelmet, ez pedig az illegális hulladékkereskedelem, az ipari, kommunális és élelmiszeripari nyersanyagok, intermedierek vagy végtermékek vonatkozásában.

A korábbi területekkel ellentétben látszólag nincs szoros, közvetlen kapcsolat a nemzetközi és honos szervezett bűnözéssel. A valóság azonban egészen más. Az illegális hulladékkereskedelem a XXI. század talán legbiztosabb hosszútávú üzlete, a szervezett bűnözés egyik legjövedelmezőbb tevékenységi formája, melyet egyrészt a kapzsiság, másrészt a korrupció, közömbösség táplál.

A fejlett jóléti társadalmak működése következtében egyre nagyobb mennyiségű hulladék keletkezik, melynek gyűjtésére, tárolására, feldolgozására vagy újrahasznosítására mind szigorúbb szabályokat, szabványokat hoznak.[13]

[12] Benkő András: Paradigmaváltás a kábítószerek biológiai mátrixból történő kimutathatóságában PhD. értekezés, ZMNE KMDI-2010

[13] Bázeli Egyezmény 1989, 259/93/EGK rendelet

Ezen szabályoknak való megfelelés horribilis költségeket ró az államokra, így megpróbálják megkeresni az „olcsóbb megoldásokat”: lakatlan területekre való lerakás, bányagödrökbe, építkezésekbe való beépítés, tengerekbe, tavakba, folyóvizekbe történő beöntés, felgyújtás vagy éppen szegényebb, kisebb ellenőrzési apparátussal rendelkező, esetleg korruptabb országokba történő elszállítás.

Ekkor jönnek képbe a bűnszervezetek, amelyek hazai és nemzetközi kapcsolataik felhasználásával a tranzakciókat lebonyolítják (német hulladékbálák megjelenése Csehországban 2006, Magyarországon 2007 vagy éppen a nápolyi hulladék nemzetközivé vált problémája 2008).
Itt is megfigyelhető a Kelet-Nyugat irányú, a centrumból a periféria felé történő illegális kereskedelem, csak a szexuális célú emberkereskedelemmel ellentétes irányban.

Míg az ipari hulladékok (műanyagok, gumiabroncsok, vegyi anyagok, nukleáris anyagok) időzített környezeti bombaként ketyegnek körülöttünk, az élelmiszerek azonnali hatásúak. A globalitás egyik negatív hatásaként a világ bármely fertőzött térségéből a hazai pultokra, piacokra kerülhetnek egészségre ártalmas élelmiszerek, hiszen a bűnözésnek köszönhetően sem a származási hely, sem a minőség, sem pedig a szavatossági idő valódiságában nem bízhatunk. Erre az elmúlt három év külföldi (kínai melamin, ukrán vodka, cigaretta) és hazai és élelmiszerbotrányai (hús, tojás, tejpor, ételízesítő, paprika) egyértelmű igazolást adnak.

Összeköti e két ismertetett területet (kábítószer, illetve élelmiszer) a gyógyszerek, illetve gyógyszernek nem minősülő „gyógyhatású” készítmények illegális forgalmazása, melyre külön iparág épül. Az uniós és tagországi ellenőrzési rendszerek kijátszásával, valamint az Internet felhasználásával élénk kereskedelem folyik világszerte, sok esetben a nemzetközi bűnszervezetek közreműködésével, irányításával.

A globális fenyegetettséggel szemben a nemzetközi együttműködés, a kockázatelemzésre alapuló szigorú ellenőrzés és a jog általi megtorlás lehet az alkalmas válasz. Ebben a küzdelemben meghatározó szerepet kell betölteni az engedélyezésben, ellenőrzésben érintett állami egészségügyi hatóságoknak, az elmúlt évek tapasztalatai szerint munkamegosztásban a rendvédelmi és fogyasztóvédelmi szervekkel és szervezetekkel.

Illegális szervkereskedelem

Végezetül még egy fontos kockázati területre fókuszálnánk. Bár a hazai bűnügyi statisztikai adatok ilyen jellegű bűncselekmények megjelenését nem regisztrálták, a nemzetközi szervezett bűnözés vonatkozásában mindenképpen említést érdemel az illegális szervkereskedelem, szoros összefüggést mutatva az emberrablással, emberkereskedelemmel, illegális migrációval és az úgynevezett gyanús eltűnésekkel.

Hasonlóan az emberkereskedelem mechanizmusához, az egyik oldalon egy folyamatosan rendelkező hiány kielégítésére való törekvés, fizetőképes kereslet, míg a másik oldalon a szegénység, kiszolgáltatottság áll.

E két oldalt kapcsolják össze a szervezett bűnözést megjelenítő csoportok. Donortérségeknek a világ gazdasági-politikai válságzónái tekinthetők, mely nem feltétlen jelent hazánk vonatkozásában kontinensnyi távolságokat, már a közeli balkáni térségre is jellemző.
A probléma súlyosságát a közelmúltban megjelent néhány híradás egymást megerősítve igazolja.

Több európai országban az elmúlt évben jelent meg a Hágai Nemzetközi Törvényszék balkáni háborús bűnösök ügyét vizsgáló már nyugalmazott főügyészének, Carla del Ponte-nek a könyve „Vadászat - én és a háborús bűnösök" címmel. Ebben igazolja azokat a korábbi értesüléseket, hogy a háború „mellékszálaként" albán bűnszervezetek által irányított szerkereskedelem folyt a balkánon hadifoglyok felhasználásával.

Másfél éve Genfben ülésezett a WHO Végrehajtó Bizottsága, ahol már a módosítási javaslatokat integrálták bele a világszervezet májusi közgyűlésén jóváhagyásra előkészített határozattervezetbe, melynek tárgya éppen az emberi sejt-, szövet- és szerv transzplantációjával kapcsolatos jogi és kereskedelmi szabályozás.
2008 februárjában Bécsi Fórum néven folyt tanácskozás az ENSZ égisze alatt 116 ország delegáltjainak részvételével az emberkereskedelem elleni fellépés jogi, szervezeti és műveleti összehangolása érdekében. A megnyitó beszédet az ENSZ Kábítószer-ellenőrzési és Bűnmegelőzési Hivatalának (UNODC) vezetője tartotta, hangsúlyozva a szervezett bűnözés egyes megnyilvánulásainak (kábítószer-, ember- és szervkereskedelem) egymáshoz való szoros kapcsolódását.

ÉRTÉKELÉS, KÖVETKEZTETÉSEK

A kétpólusú világrendszer felbomlását követően új típusú biztonsági kockázatok detektálása és kezelése jelent komoly kihívást a nemzeti és nemzetközi biztonsági szerveknek. A veszélyforrások vizsgálatával készített értékelések arról tanúskodnak, hogy több évtizedes szembenállás megszűnésével sem lett sokkal biztonságosabb a világ, figyelembe véve a kialakult geopolitikai helyzetet és fenyegető tényezőket.

Az államok és általuk alkotott politikai-katonai tömbök klasszikus szembenállása helyett és mellett nem állami szereplők jelentek meg a nemzetközi biztonságpolitikai porondon, több országra, kontinensre kiterjedő hálózatokat létrehozva. Ez a folyamat az etnikai, valamint vallási alapokon nyugvó terrorizmus széleskörű elterjedéséhez vezetett, számos új válsággócot képezve a világban.

Ezzel párhuzamosan egy másik – ugyancsak nem hagyományosnak tekinthető – globális biztonsági kihívás a *nemzetközi szervezett bűnözés* széleskörű felerősödése is tapasztalható, melynek jelen szintre történt fejlődésében ugyancsak fontos szerepet játszott az ezredfordulóra kialakult új geopolitikai környezet.

Ez szintén egy aszimmetrikus küzdelmet mutat, ahol a jogállamok nemzeti és nemzetközi szervezetei állnak szemben magukat jogon kívülinek deklaráló, illetékességi határokon átnyúló, jelentős anyagi és szakértői hátterű bűnöző struktúrákkal.

Az új kihívásokkal szembeni hadviselésben – mint az emberiség történelmének valamennyi háborújában – fontos szerepet töltöttek be a különböző tudományok, köztük az orvostudomány. A hadtudományok és a vele kapcsolatban álló természet-, és műszaki tudományok gyümölcsöző kölcsönhatást fejtettek ki egymás területeire. Publikációnk megjelentetésének alapvető célja annak bemutatása, hogy milyen feladatot tölthet be a modern orvostudomány a nemzetközi szervezett bűnözés elleni küzdelemben, rámutatva a bűnszervezetek tevékenységének rendkívül veszélyes egészségbiztonsági aspektusaira.

A tanulmány készítése kettős célt szolgált. Egyrészt mind szélesebb körben megvizsgálni a nemzetközi és honos szervezett bűnözés tevékenységének közegészségügyi, egészségbiztonsági köz- és nemzetbiztonsági kockázatait.

Ennek során áttekintettük a prostitúciós tevékenységhez kapcsolódó veszélytényezőket, kitérve a nemzetközi emberkereskedelemhez való közvetlen kapcsolódásra. Utaltunk a probléma jogi kereteire, bemutatva az 1999. évi LXXV. törvény megalkotását megelőző viszonyokat, a szabályozás célját és hatályba lépése óta kialakult viszonyokat.
A leírtak alapján indokoltnak látjuk a probléma jogi, bűnügyi és egészségügyi vonatkozásainak aktuális felülvizsgálatát.

Részletesen megvizsgáltuk a kábítószerrel összefüggő bűncselekmények jelentette biztonsági kockázatokat, kitérve a hazai terjesztésben és fogyasztásban elterjedt kábítószerfajták jellemzőire. Utaltunk a hazai kábítószerélvezők körében favorizált, a média által bagatelizált marihuána kannabisz koncentrációjának veszélyes mértékű növekedésére, egyes - tiltólistán még nem szereplő - kábító hatású készítmények időszakos felbukkanására.

Az orvostudomány szervezett bűnözés elleni küzdelemben való alkalmazásának egyik fontos bizonyítékaként számoltunk be a rendőrség drogstratégiájának kidolgozását végző munkacsoport 2005-ös tevékenységéről. Ismertettük, hogyan ágyazódtak be az orvosi, élettani ismeretek a tervezetbe, melyet végül a 17/2006. (XI.24.) ORFK utasítás tett belső normává. Bemutattuk, hogy a belső jogszabály hatályba lépése óta milyen új területeken bontakozott ki az együttműködés további igénye és lehetősége.

Kitértünk a kábítószer-fogyasztás katonai és rendvédelmi szerveket érintő kockázati tényezőire, a prevenció és szűrés kérdéskörére, kiemelt veszélyforrásként vizsgálva a békefenntartó missziókban tevékenykedő állomány többszintű fenyegetettségét.

Áttekintettük a kábítószer-fogyasztás és a szerhasználattal összefüggő fertőzőbetegségek hazai helyzetét, abból meghatározható tendenciákat, melyet az egészségügyi rendszernek a jövőben kezelni kell.
Ismertettük a kábítószer fogyasztók számának bűnügyi és egészségügyi szempontú meghatározásának szükségességét és módszertanát, kitértünk a két megközelítést szinkronizáló tudományos kutatásra.

Kitértünk a globalizáció környezetvédelemmel és élelmezésbiztonsággal kapcsolatos vonatkozásaira. Utaltunk a veszélyes hulladékok kezelésével kapcsolatos nemzetközi szabályozásra, a bűnszervezetek ezzel összefüggő tevékenységére. Fel kívántuk hívni a figyelmet arra, hogy egyrészről a szigorú szabályozás, másrészről a növekvő hulladékmennyiség és költséges megsemmisítés a nemzetközi bűnszervezetek egyik legjövedelmezőbb üzletágává teszi az illegális hulladékkereskedelmet, melynek környezeti-egészségügyi hatásai beláthatatlanok.

Végezetül – bár a hazai adatok a veszély mértékét szerencsére nem igazolják- rámutattunk a nemzetközi szervezett bűnözés egy viszonylag új területére, a szervkereskedelemre, mely a nem is távol lévő balkáni térségben is előfordul. A probléma vizsgálatánál kitértünk arra, hogy ezt a bűncselekményt is komplexen szükséges kezelni, szoros összefüggésben kapcsolódó más bűncselekményekkel és gyanús eltűnési ügyekkel.

A tanulmány másik célja annak alátámasztása, hogy az EU jelenlegi fenyegetettség elemző szempontrendszerét a fentiek alapján célszerű és indokolt kiegészíteni egy önálló vizsgálati területtel a szervezett bűnözés egészségbiztonsági hatásainak vizsgálatával, mely önmagában, de a többi már értékelt területekre gyakorolt hatásával mindenképpen meghatározó jelentőségű.

Az ENSZ és az EU keretében folyó nemzetközi akcióprogramok igazolják a feldolgozott téma fontosságát és aktualitását, melyet orvosi és kriminológiai megközelítésben egyaránt vizsgáltunk. A két látszólag távolálló terület képviselőinek közös tanulmánya jól illusztrálja, hogy a tudomány hogyan képes összehozni különböző szakmai szerveket, melynek fórumát jelen esetben a ZMNE Doktori Iskolája biztosította.

Felhasznált irodalom

(1) The Hague Programme (2005/C 53/01)
http://eur-lex.europa.eu/LexUriserv.do?uri=OJ:C:2005:053:0001:0014:EN:PDF (2010-04-10)

(2) Action Plan implementing the Hague Programme (2005/C 198/01)
http://eur-lex.europa.eu/LexUriserv.do?uri=OJ:C:2005:198:0001:0022:EN:PDF (2010-04-10)

(3) Dr. Istvanovszki L.- Kenedli T.: Új értékelési módszerek alkalmazása a szervezett bűnözésre (Magyar Rendészet 2007/1-2)

(4) Jelentés a korábbi évek bűnügyi helyzetképéről és végrehajtott intézkedésekről Országos Bűnmegelőzési Bizottság tanulmánya 2009.
http:www.bunmegelozes.hu/index.html?pind=1719lang (2010-05-30)

(5) Reports on the globál AIDS epidemic 2008
data.unaids.org/./GlobalReport/2008/jc1511_gr08_executivesummary_en.pdf (2010. 05. 30)

(6) Dr. Csohán-Lendvai-Fogarassy HIV/AIDS Magyarországon 2009
www.oek.hu/oekfile.pl?fid=2621PDF (2010-04-10)

(7) EPINFO 2009 45, 47. száma
www.oek.hu/00300/00398/00370/pdf/epinfo_EPA00398_2009_45.pdf (2010-04-10)

(8) Nemzeti Drog Fókuszpont 2009.évi jelentése az EMCDA számára
www.drogfokuszpont.hu/ éves jelentések/ 2009 (2010-05-30)

(8) EMCDDA Annual Report 2007.
www.emcdda.eu_annual report 2007 pdf. (2010-05-30)

(9) Jelentés a magyarországi kábítószerhelyzetről 2007

Szociális és Munkaügyi Minisztérium. Szerkesztő: Dr. Felvinczi Katalin, Nyírády Adrienn

(10) EMCDDA Annual Report 2004

(11) Benkő András: Paradigmaváltás a kábítószerek biológiai mátrixból történő kimutathatóságában PhD. értekezés ZMNE KMDI 2010

(12) Bázeli Egyezmény A veszélyes hulladékok országhatárokat átlépő szállításának ellenőrzéséről és ártalmatlanításáról (EU Hivatalos lapja 1993.02.16) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:11:18 (2010-05-30)

(13) 259/93 EGK tanácsának rendelete az Európai Közösségen belüli, az oda irányuló és az onnan kifelé történő hulladékszállítás felügyeletéről és ellenőrzéséről (1993.02.01) http://eur.lex.europa.eu/LexUriServ/LexUriserv.do?uri...1993R0259

(14) ENSZ Palermói Egyezmény a nemzetközi szervezett bűnözés elleni küzdelemről (2000.december 14.) kihirdette a 2006. évi CI. tv., 9. kiegészítő jegyzőkönyve az emberkereskedelem visszaszorításáról a 2006. évi CII törvénnyel kihirdetve. www. complex.hu/jr/gen/hjegy_doc.cgi?docid (2010-05-30)

(15) A szervezett bűnözés, valamint az azzal összefüggő egyes jelenségek elleni fellépés szabályairól szóló 1999. évi LXXV. törvény és módosításai http://net.jogtar.hu./jr/gen/hjegy_doc.cgi?docid (2010-05-30)

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Potóczki György
vamsped@chello.hu

ÁTTEKINTÉS A KRITIKUS INFRASTRUKTÚRA VÉDELEM JELEN HELYZETÉRŐL, A TOVÁBBLÉPÉST NEHEZÍTŐ TÉNYEZŐK ELEMZÉSE ÚTJÁN

Absztrakt

Ez a cikk áttekintő, problémaelemző célokat szolgál egy olyan kutatási munka kezdeti szakaszában, amely a kritikus infrastruktúra egy speciális részterületének feltárását tűzi ki célul. Elemzésre kerülnek a kritikus infrastruktúra védelem fejlesztése szempontjából lényeges témakörök. Az aktuális kihívások és kockázatok környezetében nem lehetünk elégedettek a megelőzés/védekezés jelen helyzetével. Az áttekintett szempontok (fenyegetettség, stratégiák, definíciók, azonosítás, tulajdonviszonyok, adatbázisok, jogalkotás, szervezeti kérdések, finanszírozás) egyike alapján sem megnyugtató a helyzet. A rendkívül szerteágazó, szövevényes, sokszor rajtunk kívülálló eseményektől is függő feladatsor miatt aligha várhatóak gyors és mindenre kiterjedő megoldások. A védekezési mechanizmus kiépülését egy-egy váratlan, nem kívánatos esemény jelentősen felgyorsíthatja. A döntés-előkészítés sokszereplős, részérdekektől erősen tagolt mind belföldi, mind nemzetközi vonatkozásban. A kutatási terület nyitott, az előrelépés szükségszerű, a megoldás az érintett nemzetközi, állami szereplők, a tulajdonosi-üzemeltetői körök és a szakirányú kutatók kezében van.

This article serves surveying, problem analysing goals in the initial phase of a research work aimed at exploring a special field of critical infrastructure. Subject areas relevant in terms of development of critical infrastructure protection will be analysed. In the environment of current challenges and risks we cannot be satisfied with the present situation of prevention/protection. Based on neither of the aspects surveyed (threats, strategies, definitions, identification, ownership relations, databases, law-making, organisation questions, financing) is the situation reassuring. Due to the highly far-reaching, complicated set of tasks often depending on events beyond our control, fast solutions covering all areas can be hardly expected. Development of the protection mechanism might be significantly accelerated by unexpected, undesirable events. Preparation of decision is a process involving several participants, highly structured by partial interests both in terms of domestic and international issues. The research field is open; progress is necessary; the solution is in the hands of the concerned international state players, owner/operator circles and researchers of the specific field.

Kulcsszavak: *kritikus infrastruktúra, kritikus infrastruktúra azonosítás, védelmi stratégia, társadalmi kapcsolat, szabályozás ~ critical infrastructure, identification of critical infrastructure, defensive strategy, social contact, regulation*

BEVEZETÉS

A kritikus infrastruktúra (továbbiakban: KI) védelemnek, vagy az ezzel kapcsolatos kutatásoknak nincs hosszú előtörténete[1], ugyanakkor már több elemzés, értékelés, jogi intézkedés, szakmai állásfoglalás létezik belföldi, illetve nemzetközi területen egyaránt. (A huszadik század végén az USA technikai értelemben, majd 1996-tól biztonságpolitikai szempontok szerint foglalkozott vele.)

A KI, mint komplex feladat a 2001. szeptember 11-i terrortámadás után felerősödött: bárki számára nyilvánvaló vált a fenyegetettség. Több ország, s nemzetközi fórum is ekkor ébredt rá a igazán a cselekvés múlhatatlan szükségességére.

A XXI. század elején megfigyelhető, hogy a KI kutatás néhány részterületen (pl. a kritikus információs infrastruktúra) sokkal intenzívebb, más szektoriális területeken azonban még bőven vannak feltáratlan „fehér foltok".

Álláspontom szerint az eddigi eredményeket, gyakorlati hasznosíthatóságát illetően nem lehetünk elégedettek. Miért? Mert a meglévő és eltérő formában újratermelődő kockázatok sokasága közepette nincs mindenre kiterjedő biztos védelem, stabil biztonságérzet. Abszolút biztonság nem létezik. Még azt is nehéz eldönteni, hogy a természeti, vagy a civilizációs eredetű kockázatok káros hatásai elleni prevenciós védekezés lenne-e könnyebb, vagy mely területen érhető el relatíve kisebb ráfordítással kecsegtetőbb eredmény. A KI védelmet napjainkban egyesek felesleges „béke időbeni" aggodalmaskodásnak tartják. Nem ismerik fel, hogy a KI védelemre, megelőzésre-felkészülésre fordítandó anyagi erőforrásoknál sokkal nagyobb összegű lenne/lehetne a bekövetkező pusztítás, a következmények kezelése-elhárítása.

A kockázatok társadalmi szintű felismertsége még nincs azon kényszerítő szinten, amelynél a döntéshozók súlyának megfelelően és egységesen kezelnék a KI biztonság kérdését. A védekezés fontosságának felismerése korrelál az aktualitásokkal, a mérvadó politikai-, gazdasági-, vagy média figyelem általában egy-egy konkrétan bekövetkezett esemény kapcsán (esetleg azt követően) jelenik meg. A kockázat életünk folyamatos része, annak érzete viszont nem állandó, a felkészülési-megelőzési hajlandóság és intenzitás is ennek megfelelően hullámzik.

Jelen cikkben (a vonatkozó joganyag, az elérhető releváns szakirodalom és saját gondolataim segítségével) választ keresek arra: Milyen állapotban van a KI védelem 2010 tavaszán? Milyen szakirányú továbbfejlesztési lehetőségeink vannak? Melyek a gyorsabb léptékű, gyakorlatiasabb előrehaladást gátló tényezők?

[1] Szerzői megjegyzés: A KI témakörével történő foglalkozás nem nagyon régi keletű. Bővebben lásd Précsényi Zoltán-Solymosi József: „Kritikus infrastruktúrák azonosítása: Körkép az EU-ban és az USA-ban tapasztalható nehézségekről" c. tudományos közleményének bevezető részében. Hadmérnök III. Évfolyam 1. szám 2008. március 60. oldal

A KI, mint kockázati tényező a permanens változás folyamatában van és az azt elviselő társadalmi tűrő- és reagáló képesség is változik. A KI kutatásnak e két tényező egymáshoz viszonyított változását lenne célszerű kutatnia az idő függvényében.

A KRITIKUS INFRASTRUKTÚRA VÉDELEM JELEN HELYZETE, A TOVÁBBLÉPÉST NEHEZÍTŐ TÉNYEZŐK ELEMZÉSE ÚTJÁN

1. Társadalmi-gazdasági beágyazottság, fenyegetettség

A KI fogalmából következnie kell a társadalmi-gazdasági beágyazódottságnak is, hiszen napi életünk és belátható jövőképünk is nagymértékben múlik e területen. Az ipari- és mezőgazdasági termelés, a szolgáltatások, a kereskedelem, a közigazgatás és az alapvető állami funkciók területein működő infrastruktúrák a normál társadalmi életvitel biztosítékait jelentik.

A 94/1998. (XII. 29) OGY határozat más biztonság- és a védelempolitikai alapelvek között kimondja:

„A Magyar Köztársaság a biztonságot átfogó módon értelmezi, amely a hagyományos politikai és katonai tényezőkön túl magába foglalja a széles értelemben vett biztonság egyéb - gazdasági és pénzügyi, emberi jogi és kisebbségi, információs és technológiai, környezeti, valamint nemzetközi jogi - dimenzióit is." [1] A dokumentum a továbbiakban hangsúlyozza: *„Növekvő kockázatot jelentenek az eltérő társadalmi fejlődésből fakadó, országok és csoportok közötti, átmeneti vagy tartós ellentétek, a gazdasági, pénzügyi és társadalmi válságok, az etnikai és vallási feszültségek, a terrorizmus, a szervezett bűnözés, az illegális kábítószer- és fegyverkereskedelem, a demográfiai feszültségek, a tömeges migráció és a nagyfokú környezeti ártalmak. Fokozódó kihívást és veszélyt jelent a tömegpusztító fegyverek és azok hordozóeszközeinek elterjedése, valamint az információs rendszerek elleni támadások lehetősége. Emellett az államok közötti feszültségek, illetve államokon belüli fegyveres konfliktusok ma is jelen vannak Európában. Régiónkban sajátos veszélyforrásként jelentkezik az átalakulásból fakadó instabilitás és kiszámíthatatlanság, a demokratizálódási folyamatok törékenysége."* [2]

Legfőbb jogszabályalkotó szervünk hivatkozott határozatából egyértelműen kitűnik, hogy melyek a biztonság hivatalos dimenziói, a növekvő kockázatok, s milyen sok területen van kétoldalú kapcsolat. Álláspontom szerint az Országgyűlési határozatban meg kellett volna jelennie a KI-nek, mint fogalomnak, vagy legalább megnevezésnek, hiszen a teljes szövegkörnyezetből már 1998-ban is következhetett volna: a biztonság- és védelempolitika egyik elemi előfeltétele a KI objektumok megóvása.

A KI a társadalom egyik létfeltételeként is értelmezhető, mert egyes elemek hiánya, vagy az azokból eredő dominószerű következmények alapvető működési zavarokat, ellehetetlenülést is eredményezhetnek széles rétegek számára. A több irányból, eltérő időpontokban és néha löketszerűen érkező változások biztonsági kockázatú összeérése, egymást erősítő kumulatív hatása a társadalomban fokozott veszélyérzetet generálhat.

A társadalmi-gazdasági változások kölcsönösek, egymást generáló hatásúak. Az utóbbi ötven évet tekintve is elementáris változások történtek világszerte. Politikai rendszerek, szövetségek, gazdasági formációk szűntek meg, újak jöttek létre. A világméretű globalizáció,

az ipari munkamegosztás, a mezőgazdaság szakosítása, új – korábban nem ismert - termékek és szolgáltatások özönének létrejötte, a standardizált kereskedelmi- és pénzügyi folyamatok terjedése nem maradt társadalmi hatások nélkül. A változás inkább a centrum-periféria viszony ismert közgazdasági elmélete szerinti helyzetet eredményezte, az ebből következő társadalmi mozgásformákat generálta, s kevésbé hatott a nivelláció irányába. A világ energiakészletének alakulása, a globális felmelegedés, az űrkutatás, az emberiség létszámbeli növekedése, a gazdasági egyenlőtlenségek felismerése új társadalmi mozgástereket nyitott meg. A változó társadalom és gazdaság új kockázatok megjelenését, mások megszűnését idézi elő. Álláspontom szerint a mindenkori kockázati állapotoknak és a társadalmi tűrő-, illetve reagáló képesség változásainak összhangban kellene működnie. Sajnos e téren nem megfelelő a harmonizáció, illetve e három fontos tényező együttes kezelésének részleges hiánya tapasztalható. Csak megemlítem, hogy mind a kockázatok, mind a társadalmi tűrő-, illetve reagáló képességek is értelmezendőek lennének közösségi (EU), nemzeti (ország), illetve regionális szinteken.

A lakosság „hozzáállásán" közvetlenül is érzékelhető, hogy mit jelenthetne pl. egyes közüzemi szolgáltatások kiesése, vagy egy nem kívánatos nagy horderejű természeti jelenség, esetleg valamely komoly társadalmi konfliktushelyzet következménye. Alapvető ellátási rendszerek órákon belül működésképtelenné válhatnak (élelmiszer disztribúció, közlekedési hálózatok, fűtőanyag ellátás, stb.).

A társadalom és a KI között tehát szoros korreláció van. Ellenkező esetben utóbbi fogalomra vagy nem lenne szükség, vagy szerepe, közérdekű jellege minimálissá válna.

Társadalmi szempontból nem is elsősorban a KI fogalomrendszerhez tartozó infrastrukturális létesítmények, rendszerek, hálózatok védelme az igazán fontos, hanem az általuk előállított produktum – termék, szolgáltatás, stb. - gördülékeny és folyamatos biztosítása (persze érthetően az utóbbi feltételezi az előbbit).

A KI biztonsági kockázatainak követése, a fenyegetettségi jellemzők megértése és „lereagálása" nagyon fontos. Az ezzel kapcsolatos kérdések megfelelő kezelése

- hazánkban azért jelent gondot, mert a KI nem tartozik a politikai/gazdasági prioritások közé és védelem ügye sok látens, megoldatlan problémával küzd. Fő célnak tartanám, hogy a vezetés mindig legyen képes biztonsági szempontból kezelni a társadalmi reagálást.

- nemzetközi értelemben (EU szinten) sem történik súlyának megfelelően, hiszen inkább deklarációk és követendő eljárási formák születnek elméleti síkon. Az gyakorlati megvalósítás már lassú, érdekszövevényekkel tagolt, nehezen átlátható. Az egyeztetés évekig húzódik, a pusztítás percek alatt bekövetkezhet.

A KI védelem minden államapparátus múlhatatlan és vitathatatlan alapfeladata, de a kölcsönhatások, a hálózatok, az összetett folyamatok és a természeti- és társadalmi determinánsok miatt nem mellőzhetőek a nemzetközi szintű együttgondolkodás szempontjai sem.

2. Stratégiák

A 2003 decemberében az Európa Tanács brüsszeli ülésén elfogadott, „Biztonságosabb Európa egy jobb világban" címet viselő Európai Biztonsági Stratégia[2] elsősorban azt célozza, hogy az Unió a világ egyik erőcentrumaként jelenhessen meg. A célok eléréséhez szükséges az egységes biztonság- és védelempolitika. Az Európai Biztonsági Stratégia végrehajtásáról szóló jelentés „A biztonság megteremtése a változó világban" címmel olvasható[3]. Ebben címzetten csak a közlekedési, kommunikációs és energiaellátási infrastruktúrát említik, ideértve az internetet is, de foglalkoznak pl. az éghajlatváltozással és a biztonság-fejlesztés kapcsolatrendszerrel is.

A hazai tárgybani stratégiákat lényegében a 2073/2004. (IV. 15.)[4], valamint az 1009/2009. (I. 30.)[5] Korm. határozatok jelenítik meg.

Álláspontom szerint a mai védelmi rendszerek nem nélkülözhetnék a stratégiai tervezést. Ezt a a teljes megoldáshoz vezető „lépcsőnek" kell tekintenem, amely magában foglalná: a teljes víziót, a stratégiát, a tervezést (időtávok rendre: 20, 5, 1-2 év), az alprogramokat és a részterületekre vonatkozó rövidtávú projekteket. A ilyen felépítés nemcsak rendszertechnikai szempontból lenne követendő, hanem azért is, mert a megvalósítás finanszírozása is logikus tagolást, időütemezést követelne meg.

3. Definíciók, kritériumok, értelmezési problémák

Az infrastruktúra értelmezése alig igényel köznapi magyarázatot, a létező definíciók mégis eltérőek. A régebbi kiadású idegen szavak és kifejezések szótára [3] szerint az infrastruktúra: *„a gazdaság működésének üzemen kívüli feltételeit biztosító álló- és forgóeszközök; lakásállomány és a legkülönfélébb szolgáltatások (művelődésügy, közlekedés, közművek, hírközlés, egészségügy, kereskedelem, stb.) állóeszközei, ill. ezek hálózata"*[6]. E megközelítés felett már eljárt az idő, hiszen pl. csak álló- és forgóeszközökről tesz említést. Más definíció szerint infrastruktúra: *„minden olyan berendezés és hálózat, amely a szállításhoz és hírközléshez szükséges, azaz szárazföldi (közúti, vasúti) szállítási, belvízi szállítási (folyók, csatornák), tengeri szállítási (kikötők), légi fuvarozási (repülőterek), vízelosztási, energiaelosztási (villanyáram, olaj, gáz) és távközlési (telefon, rádió, televízió, telematika stb.) hálózatok, beleértve a műholdakat."* [4] Ez kifejezetten közlekedés centrikus felfogás. A Magyar Larousse Enciklopédikus szótár meghatározása szerint infrastruktúra: *„...a társadalmi, gazdasági újratermelés zavartalanságát biztosító háttér...."*[5][7]

---

[2] Biztonságos Európa egy jobb világban. Európai biztonsági stratégia.
http://www.consilium.europa.eu/uedocs/cmsUpload/031208ESSIIHU.pdf
Letöltés: 2010. május 6.

[3] Lásd: Brüsszel 2008. december 11. S407/08.
http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/HU/reports/104644.pdf
Letöltés: 2010. május 6.

[4] A részleteket lásd: 2073/2004. (IV. 15.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról.
http://www.kbh.gov.hu/index.php?id=2073_2004_kormhat
Letöltés: 2010. május 6.

[5] A részleteket lásd: Nemzeti Katonai Stratégia 2009.02.05.
http://www.hm.gov.hu/miniszterium/nemzeti_katonai_strategia_-_kormanyhatarozat
Letöltés: 2010. május 6.

[6] Lásd [3] szakirodalmi hivatkozásnál 369 p.

[7] Lásd [5] szakirodalmi hivatkozásnál 363 p.

Az infrastruktúra fogalmát eltérő jelentéstartalommal értelmezik. Van energia-, közlekedés-, telekommunikációs, környezetvédelmi, oktatási, mezőgazdasági, katonai, vagy éppen humán, stb. infrastruktúra. Utóbbihoz tartozhat pl. a szociális, munkaügyi, az egészségügyi, közművelődési intézmények hálózata, stb. Van olyan meghatározás, amely szerint az infrastruktúra fizikai építmények, berendezések összessége, amely álláspontom szerint szintén hiányos, szemléletében túlhaladott. Ma már evidensnek tartunk olyan infrastruktúrákat (pl. mobiltelefon, GPS szolgáltatás, internetes kereskedelem) is, amelyek pár éve még nem léteztek. Gazdasági fejlődésünk extenzív szakaszaiban fontos, intenzív szakaszaiban már meghatározó az infrastruktúra. Alacsony fejlettség, rossz összetétel esetén bizonyítottan negatív tényezőként hat, magas fejlettségnél viszont multiplikátorként működik, dominál a versenyképesség alakulásában.[8] A különböző meghatározások áttekintése után – álláspontom szerint - nem került igazán birtokunkba az infrastruktúra hibátlan, mai viszonyaink között is helytálló definíciója.

A KI-nak jelenleg nincs - nemzetközi és hazai szinten, a mértékadó szakmai közvélemény által - általánosan elfogadott, szintetizált definíciója. További gond, hogy még a kritikusság fogalma is meglehetősen tisztázatlan, amely önmagában is függvénye lehet a veszélyeztetettségnek, az időnek, a technikai fejlődésnek, a hálózati jellemzőknek és a gazdaság aktuális helyzetének. Ez azonban nem jelenti azt, hogy nincsenek kísérletek, reményteljes próbálkozások és azt sem, hogy több ország, vagy több kutató ne tekintene egy-egy megoldásra tökéletesként. Tekintsünk néhány szakirodalmi példát is, nyilván a teljesség igénye nélkül:

A 2080/2008.(VI. 30.) Korm. határozat [6] 1. sz. mellékletének 3.2. pontja szerint: *„Kritikus infrastruktúrák alatt olyan egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.”*

A definíció szabatosan összefoglalja a figyelembeveendő szempontokat, azonban álláspontom szerint nem kerülhető meg a nemzetközi kapcsolatokra, jelenségekre történő utalás és talán a veszélyhelyzeteket generáló kockázatok ok-okozati megjelenítése sem.

Az egyik tudományos közleményben olvasható:

„Az infrastruktúra rendszerek méretének és komplexitásának növekedésével, azok védelme is egyre nagyobb szervezettséget igényel. Az infrastruktúra védelem feladat éppen ezért nem lehet a teljes rendszer minden egyes elemének védelme… Ennek nyomán született meg a KI fogalma, és az infrastruktúrák közül jelenleg ezen fogalomkörbe tartozó rendszerek védelmét tekinti stratégiai fontosságúnak az egyes országok vezetése. …… A holland kormány kezdeményezésére a következő definíciót alkották meg: Kritikusnak tekintendők azok az infrastruktúrák, amelyek leállása vagy súlyos sérülése nemzeti szintű károkhoz vezethet.” [7]
A német definíció szerint *„kritikus infrastruktúrák szervezetek és intézmények, amelyek létfontosságúak a népjólét számára, és amelyek leállása vagy kimaradása hosszú távon az*

[8] A fogalmat, a felosztási rendszereket lásd bővebben: Dr. Abonyiné Dr. Palotás Jolán: Infrastruktúra című művében. ISBN 978-963-9310-77-3 Dialóg campus kiadó. 2003 Budapest-Pécs http://www.dialogkiado.hu/index.php?page=kiadvany_reszletes&kid=201.
Letöltés: 2009. november 8.

ellátás zavarait eredményezheti és/vagy más drámai következménye van a lakosság széles rétegei számára." [8]

Az USA szempontjai szerint a KI értelmezése időről-időre új dimenziókkal bővül és az sem állandó, hogy egy-egy elem mikor válik kritikussá.

Érdekes, hogy ezt megelőzően az Európai Bizottság 2004. október 20-i *„A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben"* címmel kiadott Közleményében – többek között – meghatározást is adott a KI fogalmára.[9]

A kritikus infrastruktúra egységes fogalmi definíciójának hiányát a ZMNE egyik egyetemi jegyzete is nagyszerűen bemutatja. [9] Érdekes tanulmányozni egy világszerte közel 45 ezer főt foglalkoztató amerikai civil szervezet[10] nézetrendszerét, amely – többek között- a KI körébe tartozó árutovábbítást, az energia- és vízszolgáltatást, az élelmiszerellátó rendszerek biztonságát, a közegészségügyet, a vészhelyzeti szolgáltatásokat, a kommunikációt és az adatszolgáltatásokat tekinti feladatkörének.[11] Az általam elemzett probléma aktualitását aláhúzza a következő megállapítás: *„A kritikus infrastruktúra védelmének területén az egyik legsúlyosabb kihívást a közös terminológia hiánya jelenti. Túl sok ember használ túl sok rosszul definiált kifejezést…."* [10]

Álláspontom szerint a KI védelem:

- vizsgálatát, rendszeralkotását megelőzően el kell/ene/ végezni a fogalmak tisztázását, egységes értelmezését, a fenyegetettség rendszerezését, meg kell oldani a változások követését. Ez azonban – a témakör rendkívüli bonyolultsága, nemzetközi kihatásai miatt - nem lehet néhány személy, vagy kutatócsoport elszigetelt feladata,
- nem vállalhatja fel sem a – fogalmi körön kívüli - kisebb kihatású zavarok elhárítását, sem a fenyegetettségi, kockázati jellemzők teljes körének kezelését.

A KI-hoz tartozás kritériumrendszerét a fenyegetettség mértéke, a rendszerben betöltött hely és fontosság, valamint a közvetlen és közvetett következmények kiterjedtsége determinálhatja elsősorban. Ez a gondolat már átvezet az azonosítás témaköréhez.

4. Azonosítás, KI szektorok, kölcsönös függőségek

A KI biztonságos működéséhez fűződő érdekek egyetemlegesek, tértől, időtől, politikai, vallási és társadalmi-gazdasági berendezkedéstől, történelmi hagyományoktól szinte függetlenül jelentkeznek. Napjainkban az adott körbe tartozó infrastruktúrák azonosítása, a róluk alakuló megítélés és besorolás viszont – álláspontom szerint és érdekes módon – pontosan az előbbi tényezők különböző súlyozott átlaga által determinált.

[9] Lásd bővebben: Commission of the European Communities: Communication from the Comission to the Council and European Parliament – Critical Infrastructure Protection int he fight against terrorism, Brussels, http://ec.europa.eu/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf 2009.
Letöltés: 2009. november 9.
[10] Nevezetesen: Science Applications International Corporation /SAIC/ Lásd: http://www.saic.com
Letöltés: 2010. május 3.
[11] Bővebb információk angol nyelven a http://www.saic.com/critical-infrastructure/ oldalon érhetőek el.
Letöltés: 2010. május 3.

A lehetséges, vagy elvileg szóba jöhető teljes KI azonosítási halmazon belüli különféle csoportképző ismérvek nyilvánvalóan eltérő eredményre vezethetnek és – mint látjuk – vezetnek is. Lehetséges-e, hogy ez a kimondatlan oka annak, hogy nem létezik általánosan elfogadott egyetlen fogalmi meghatározás és ágazati besorolás sem?

A KI szektorokat más összetételben azonosítja pl. az USA, KANADA, az EU, illetve ez utóbbi néhány tagországa is. A KI azonosítás folyamatáról és védelméről alapos áttekintést nyújt a „Hadmérnök" c. on-line tudományos kiadvány egyik, még 2007-ben készült szakcikke.[11]

Az eltérő megítélés, azonosítás szemléltetésére bemutatok egy táblázatot (lásd 1. sz. táblázat), amely néhány ország saját szempontok szerinti KI besorolását tartalmazza:

Ország **Szektor**	**A**	**CAN**	**CH**	**DE**	**F**	**FIN**	**I**	**NL**	**NO**	**SE**	**UK**	**USA**	**Σ.**
Légi irányítási rendszer										✓			1
Bank, pénzügyi szolgáltatások	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	14
Kormányzati szolgáltatások		✓		✓		✓	✓	✓	✓	✓	✓	✓	11
Polgári védelem			✓				✓						2
Kommunikáció /ICT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	14
Gát												✓	1
Felsőoktatás												✓	1
Energia/ villamos e.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	14
Veszélyhelyzeti szolgálatok	✓	✓	✓	✓		✓			✓		✓	✓	10
Élelmiszer/ Mezőgazd.		✓		✓		✓		✓			✓	✓	7
Veszélyes anyagok/RBV		✓									✓	✓	3
Egészségügy	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	12
(Védelmi) ipar/gyártás		✓	✓		✓	✓						✓	6
Távközlés/ Média	✓	✓	✓			✓		✓		✓	✓		8
Biztosítás				✓								✓	3
Ig.szolgáltatás/ büntetés-végrehajtás				✓				✓			✓	✓	5
Honvédelem/ Honvédelmi létesítmények	✓			✓				✓	✓				5
Nemzeti jelentőségű értékek		✓										✓	3
Atomerőmű					✓							✓	2

Kőolaj és földgáz ellátás		✓		✓			✓	✓	✓		✓	✓	9
Rendőrség	✓	✓				✓			✓		✓		6
Posta	✓											✓	2
Közigazgatás	✓		✓	✓		✓	✓	✓			✓	✓	8
Közrend/ biztonság					✓			✓			✓		3
Szennyvíz/ hulladék kezelés		✓							✓		✓		4
Szociális háló	✓					✓			✓				4
Közlekedés/ elosztás	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	13
Közművek	✓								✓				3
Ivóvíz szolgáltatás	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	12
Árvíz védekezés.								✓					1
ÖSSZESEN	14	16	11	14	9	14	10	15	14	6	17	20	

1. sz. táblázat. Egyes országok KI szektor megítélése
Forrás: NFGM KI Védelmi Nemzeti Program Konzultációs Fórum háttérismertető Budapest, 2009. március 2. 77 oldal, pp 44-45.

Az EU Tanács 2008. december 8-án fogadta el az európai KI-k azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelvet. Szakmai körökben közismert és most aktuális, hogy az EU - az EPCIP és az említett irányelv alapján - 2011. január 12-ig kérné az európai körbe tartozó KI elemek azonosítását a tagországoktól. A KI üzemeltetők azonban nem egységesek és nem rendelkeznek azonos tapasztalatokkal. Ezért nem nélkülözhető az ágazati sajátosságok és a (közösségi, nemzeti, regionális) intézkedések figyelembevétele, valamint adott esetben a KI-k tulajdonosai/üzemeltetői között már létrejött, határokon átnyúló kölcsönös segítségnyújtási megállapodások ismerete sem.

A 2011. januári határidő tekintetében egyszerűsítheti a helyzetet, hogy az irányelv hatálya jelenleg kizárólag csak a közlekedési és energia szektorra terjed ki. Itt viszonylag egyszerű a releváns (mint villamos energia, kőolaj, földgáz, valamint a csővezetékes továbbítást kivéve a többi közlekedési alágazat /közút, vasút, légi, vízi, tengerhajózás és kikötők/) szektorok azonosítása. Az irányelvben szerepel, hogy a hatálybalépésétől számított 3 év múlva kell felülvizsgálni és dönteni arról: szükséges-e más ágazatokat is bevonni az irányelv hatálya alá. Az IKT szektornak bővítményként kell majd prioritást adni.

Hazánkban komolyan felmerülnek a következő kérdések: Szükség van-e jogszabályi háttérre a kijelöléshez, azonosításhoz? (Álláspontom szerint igen: de ez esetben jelzem, hogy ilyen jogszabály ismereteim szerint jelenleg nincs!) Elegendőek lesznek-e az EU által biztosított támpontok a hatékony döntésre? Probléma, hogy az EU rendelkezik az európai KI körbe tartozó üzemeltetési kötelezettségekről és biztonsági tervről, de az üzemeltetési tartalomról már csak körvonalaiban tesz említést. Lehetséges, hogy ez utóbbi már nemzetközi harmonizáció nélküli hazai kompetencia? Eldöntendő, hogy az azonosítás egyértelműen

közigazgatási feladatnak minősíthető-e, vagy sem? (Álláspontom szerint igen, hiszen a közigazgatás szerves részeként tekintek a KI védelemben fontos szerepet betöltő civil-, rendészeti-, illetve honvédelmi típusú igazgatási feladatokra és csak ezek után értelmezendőek a fizikai, kémiai, matematikai, közgazdasági, stb. megfontolások). Van-e jogorvoslat a kijelölés, azonosítás ellen? Alkalmazni fogjuk-e az állami és a piaci szféra együttműködésének valamelyik nemzetközileg ismert típusváltozatát hazánkban a KI védelem területén? Milyen két-, vagy többoldalú nemzetközi egyeztetési problémák merülhetnek fel a hatásmechanizmusok (kiterjedtség, súlyosság, időbeni hatás) megítélését, vagy az interdependencia (azonosított kapcsolati összefüggés) szintjét illetően (tekintettel arra, hogy az európai KI körbe tartozás kritériuma a több ország általi érintettség)?

Természetesen át kell tekinteni a nyilvánvaló kapcsolódásokat nemzeti politikánk más szintjein is (például Nemzeti Környezetvédelmi Program, Nemzeti Éghajlatváltozási Stratégia, Országos Területfejlesztési Koncepció, energia-, agrár- és közlekedéspolitika). Álláspontom szerint további igényként jelenhet meg az egyes stratégiák – jelenleg hiányos – harmonizációja, vagy pl. a Nemzeti Éghajlatváltozási Stratégia és az energiapolitika közötti ellentmondások feloldása.

5. Tulajdonviszonyok szerepe

A tulajdonviszonyokkal kapcsolatos alapvetésem az, hogy az Alkotmány nem tesz különbséget tulajdonformák között. Ebből levezethető a tulajdonviszonyok hatása a biztonsági kérdésekre, arra, hogy a biztonság nem alapvetően a tulajdonviszonyokon, sokkal inkább a jogi szabályozáson múlik. A KI védelem ügyét semmiképpen nem korlátozhatják lényegesen, vagy gátló módon a tulajdonviszonyokból származó egyedi magán, vagy cég szempontok,

- hiszen ez esetben aligha lenne megengedhető, hogy pl. közüzemi szolgáltatók magánkézben legyenek,
- mert a KI védelemhez tartozó jogok, de különösen a kötelezettségek messze túlnyúlnak egy-egy tulajdonos, vagy cégcsoport érdekkörén, gondolkodási horizontján,
- ezért a magasabb szintű közös érdekek feltétlen érvényesülését – szükség esetére - jogi úton is garantálni kell.

A privatizáció okán a KI védelem területén korábban meglévő közvetlen állami befolyás alaposan meggyengült, a közvetett hatás nagyobb jelentőséget kapott. A magánosítás bőven érintett KI fogalomkörbe tartozó elemeket is, így akarva-akaratlanul közös felelősségi rendszer keletkezett a közigazgatási és az üzleti szféra között, amely sok ellentmondást is hordoz.

A KI védelmi feladatokat koordináltan kell végezni úgy, hogy közigazgatás illetékes szervei fokozatosan igényeljék /szükség esetén kötelező jelleggel írják elő/ minden KI üzemeltetőtől a részletes elemzést, a feladatok-hatáskörök-felelősségi rendszerek pontosítását.

6. Adatbázisok

Terjedelmi okok miatt csak jelzésszerűen foglalkozom a KI körbe tartozó adatbázisokkal. Az informatikai eredetű kockázatok elérhetnek olyan adatbázist, amely adott KI-t veszélyeztethetnek. A veszélyeztetett adatbázisokat álláspontom szerint hozzá kell rendelni a

KI azonosítás szerinti tételes ágazati, alágazati besoroláshoz és külön figyelmet kell fordítani a folyamat-, illetve a rendszerfelügyelet elektronikus rendszereire. Ez azt jelenti, hogy a közösségi (EU), a nemzeti, illetve az ágazati elemek azonosításával célszerű párhuzamosan végezni a védelemre szoruló adatbázisok kijelölését, tulajdonságai elemzését, belső- és külső összefüggéseinek feltárását. A feladat hangsúlyos, hiszen rohamléptekben fejlődik az e-közigazgatás (adó-, vám-, önkormányzatok, stb.), a KI ágazatokban is bővülnek az elektronikus termelésirányítói rendszerek, s szinte minden meghatározó szektor (közüzemek, energiaszolgáltatók, pénzügy, posta, közlekedési rendszerek, logisztikai disztribúció, környezetvédelem, vízügy, egészségügy, közbiztonsági és védelmi szervek, stb.) növekvő internetes- és mobil forgalmazást végez. Az adatbázisoknak a KI-ben betöltött szerepéről színvonalas áttekintő értékelés jelent meg a Hadmérnök c. on-line tudományos kiadvány egyik számában. [12] A cikkben vitatnám azt a megállapítást, hogy pl. az adatbázisok nem játszanak jelentős szerepet a postai szolgáltatások esetében. Hangsúlyozom, hogy a KI adatbázisok csak a szakképzett kezelő személyzettel, speciális szoftverekkel alkalmazhatóak rendeltetésszerűen.

7. Szabályozási, jogalkotási körkép

Álláspontom szerint a jogszabályi környezetnek követnie kell a bekövetkező változásokat (a gazdaság az alap, a jog a felépítmény). Nagy kérdés azonban, hogy a jelen válságkörülmények közepette képes-e a nemzetgazdaság a biztonságpolitikai célokhoz nélkülözhetetlen pénzügyi feltételeket biztosítani, s milyen együttműködési hajlandóságot mutatnak az érintett tulajdonosi körök.

Deklarált cél a 114/2008. EK irányelv hazai jogharmonizációja, ezért a nemzeti szabályozási javaslat összeállítása céljából a 2080/2008. (VI. 30.) Korm. határozat elrendelte ágazati konzultációk lefolytatását a hazai infrastruktúrák üzemeltetőivel és tulajdonosaival.[12] Ez lényegében megtörtént, a résztvevők által kérdőívek is kitöltésre kerültek. A tapasztalatok feldolgozása útján 2009 októberére elkészült egy szabályozási koncepció, amelyben törvényi szabályozásra is született javaslat.

A koncepció kidolgozása során alapfeladat volt az, hogy *„tekintettel kell lenni a létfontosságú infrastruktúra elemek közötti összefüggésekre, a nemzeti intézkedések végrehajtását biztosító intézményrendszerre, az üzemeltetők és tulajdonosok alkotmányos kötelezettségeire, az infrastruktúra honvédelmi célú felkészítésének és fejlesztésének állami feladataira, a honvédelem szempontjából fontos, kritikus infrastruktúra védelmére vonatkozó követelményekre valamint az európai jogharmonizációs feladatok végrehajtására és a NATO szövetségesi kötelezettségek érvényesülésére."* [13]

A szakmapolitikai egyeztetésen azonban vitás kérdések, kifogások merültek fel, amelyek következtében már nem került sor – a jogszabállyá válás következő lépcsőfokát jelentő – közigazgatási egyeztetésre. A közeljövő tárgybani eseménysora – jelen cikk írásának időpontjában - a 2010. áprilisi országgyűlési választásokat követő új kormányzati munkamegosztási rend kialakításának időigénye miatt nehezen prognosztizálható, de az EU által a tagországok számára adott implementációs határidő (2011. január 12) már nagyon közelinek tűnik. Ez lényegében az európai KI körébe tartozó azonosítást és nemzeti jogszabályalkotást tenne szükségessé. A nemzetközi koordinációt kissé nehezítheti hazánk

[12] Lásd a Nemzeti Fejlesztési és Gazdasági Minisztérium a KI Nemzeti Védelmi Program Konzultációs Fórumára (Budapest, 2009. március 2) kiadott háttérismertető anyagot, amely összefoglalja a téma kezelésének helyzetét.

földrajzi, geopolitikai helyzete is, hiszen a szomszédaink között egyaránt találhatóak más-más fejlettségű és elkötelezettségű partnerek, valamint EU, NATO, schengeni övezeti tagországok is.

A döntés-előkészítőkre több problémás kérdés megválaszolása vár.[13] A jogalkotás tekintetében – jelen cikk írásának időpontjában – az valószínűsíthető, hogy bizonyos együttműködési kötelezettségeket előíró, taxatív felsorolásokat nem tartalmazó, ún. keretjellegű hazai jogszabálytervezet készül. Várhatóan nem lesz a válságkörülményeket kategorizáló tételes lebontás, sokkal inkább számíthatunk értelmező rendelkezésekre, fogalmi tisztázásokra, az üzemeltetési jogok és kötelezettségek kimunkálására, a kapcsolattartás módozatainak kijelölésére és jövőbeni funkcionális utalásokra.

A KI legfontosabb Európai Uniós, illetve magyar jogi- és egyéb szabályozásai a következők:

- EPCIP Green Paper (COM (2005) 576 final) /Zöld könyv/
- EPCIP – European Program for Critical Infrastructure Protection (COM(2006) 786 final – 2006.12.12) /A KI európai védelmi programja/
- EPCIP része a CIWIN - Critical Infrastructure Warning Information Network /A KI figyelmeztető információs hálózata/
- 114/2008 EK Irányelv az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről 2008.12.08.
- 94/1998 (XII. 29.) OGY határozat a Magyar Köztársaság biztonság és védelempolitikájának alapelveiről
- 2236/2003 (X. 1.) Korm. határozat a Magyar Honvédség 2004-2013 közötti időszakra vonatkozó átalakításának és új szervezeti struktúrájának kialakításáról
- 180/2003. (XI. 5.) Korm. Rendelet a Nemzeti Biztonsági Felügyelet részletes feladatairól és működési rendjéről, valamint az iparbiztonsági ellenőrzések részletes szabályairól
- 2073/2004 (IV. 15.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról
- 2004. évi CV. Törvény a honvédelemről és a Magyar Honvédségről
- 2112/2004 (V. 7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól
- 24/2004. (VIII. 16.) IHM rendelet a védelmi feladatokban részt vevő elektronikus hírközlési, illetve postai szolgáltatók kijelöléséről és felkészülési feladataik meghatározásáról
- 27/2004. (X.6.) IHM sz. rendelet az informatikai és elektronikus hírközlési, továbbá postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségéről
- 2151/2005 (VII. 27.) Korm. határozat a Terrorizmus Elleni Akcióterv felülvizsgálatáról
- 195/2005. (IX.22.) Korm. sz. rendelet az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességeiről és egységes használatáról

[13] Szerző megjegyzése: Több felvetett probléma mellett itt hívnám fel ismét a figyelmet a jelen cikk 4. pontjának utolsó előtti bekezdésében foglalt kérdésekre adandó válaszok fontosságára. A jogszabályi előkészítés egyéb szempontjaira, illetve az állami szerepvállalásra a 8. pontban is ki fogok térni.

- 276/2006 (XII.23.) Korm. sz. rendelet a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala létrehozásáról, feladatairól és hatásköréről
- 2046/2007 (III. 19.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól szóló 2112/2004 (V. 7.) Korm. Határozat módosításáról
- 1/2007 (III. 29.) Kormányzati Koordinációs Bizottság határozat
- 84/2007. (IV. 25.) Korm. Rendelet a Központi Elektronikus Szolgáltató Rendszer és a kapcsolódó rendszerek biztonsági követelményeiről
- 81/2008 (IV. 4.) Korm. Rendelet a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala létrehozásáról, feladatairól és hatásköréről szóló 276/2006 (XII. 23.) Korm. Rendelet módosításáról
- 2080/2008 (VI. 30.) Korm. Határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

8. Szervezeti kérdések, koordináció

A védtelen a magyar infrastruktúra c. cikkben[14] arról olvashatunk, hogy „digitális Mohács fenyegeti Magyarországot" és „A legnagyobb gond a védekezést irányító szervezet teljes hiánya…". Vajon miért érezhetik ezt így az elektronikus hadviseléssel foglalkozó szakértők, amikor hazánkban létezik KKB (Kormányzati Koordinációs Bizottság) és alárendelt szervei, van címzetten delegált jogszabály előkészítési felelősség, ágazati egyeztetés, stb.? E gondolatok is rávilágítanak arra, hogy a veszélyhelyzeti megelőzés/felkészülés jelen szintjével nem lehetünk elégedettek.

Kinek a feladata és felelőssége a szolgáltatások, termékek és eljárások védelme a magántulajdonban lévő kritikus szektoron belül? Nyilván elsősorban a tulajdonosoké, vagy üzemeltetőké. Azonban az általuk esetleg elkövetett felelőtlenség okozta hatások messze meghaladhatják működési körüket, kompetenciáikat! Megkövetelhető-e tőlük a kellő szakértelem, a kívülállók szempontjainak figyelembevétele, a biztonsági tervek elvárt szintű (gyakorlatban könnyen értelmezhető, és végrehajtható) kidolgozottsága és aktuális jellege? Elkülöníthetőek-e a természeti, illetve a civilizációs okokból fennálló veszélyhelyzet megelőzési/kezelési funkciók és felelősségek? Válaszaim: Igen!

Mi az állam szerepe a KI védelem munkamegosztásában? Elfogadható lenne-e, hogy az állami szerep csak a követelmények végrehajtásának felügyeletére korlátozódjék jogszabályi felhatalmazással? Álláspontom szerint a megelőzési/felkészülési időszakban – többek között - a következő állami szerepvállalások lennének célszerűnek:

- stratégia alkotás, államigazgatási koordináció az érintett szervek között,
- központi védelmi irányító szervezet, apparátus működtetése,
- KI azonosítási feladatok ellátása,
- elemzési módszerek kiválasztása, fejlesztése,
- veszélyhelyzeti, folytonossági (üzemeltetői-biztonsági) tervek felügyelete, azok készítési kötelezettségének kiterjesztése minden KI szektor üzemeltetőre, de még az érintett állami szervekre is,
- szimulációs gyakorlatok szervezése,
- elvárt biztonsági követelményszint meghatározása, kockázati prioritások felállítása,

[14] Lásd részletesebben: Tóth Balázs: Védtelen a magyar infrastruktúra, 2009. szeptember 20. http://index.hu/tech/2009/09/20/vedtelen_a_magyar_infrastrukt%c3%bara/
Letöltés: 2010. május 9.

- nemzetközi együttműködés bővítése két- és többoldalú szinteken (nemzetközi összekötők, információcsere működtetése),
- vészhelyzeti tömegtájékoztatás koordinációja, hírközlési funkciók kézbentartása,
- az EU források hatékony felhasználásának elősegítése, pályázatkoordináció,
- a KI üzemeltetők segítése és ösztönzése, a partneri szintű együttműködés szervezése, különös tekintettel az interdependencia jelenségre.

A rendszer hatékony és garantált működéséhez – a fentieken túlmenően – szükség lenne arra, hogy a védelmi feladatok az érintett köz- és magánszférai szervezetekbe, tevékenységekbe napi szinten integrálódjanak, szervesen beépüljenek.

9. Védelemfinanszírozási szempontok

Az EU Bizottság a finanszírozás „örökzöld" kérdésével kapcsolatban elvárja, hogy a KI védelem okán meglévő kiadások ne gyakoroljanak különösen negatív hatást az adott alágazat versenyképességére. (Nem hanyagolható el az a közvetett hatás sem, amelyet a biztonság léte-, vagy hiánya okozhat a makrogazdasági mutatókban, az árfolyamokban, vagy egyéb piaci szegmensekben.) Komoly erőforrásokat kell biztosítani a szükségletek azonosítására és közös műszaki szabványok kidolgozására. Információim szerint a Bizottság támogatna olyan ágazatspecifikus tanulmányokat, melyek az adott infrastruktúrák biztonsága növelésének az ágazatra gyakorolt esetleges pénzügyi hatásait vizsgálná. Álláspontom szerint szükség lenne célzott kutatások megkezdésére mindazon magyar területen lévő szektorok/alágazatok tekintetében is, amelyek közösségi, vagy nemzeti szinten KI körbe tartozónak minősülnek.

A finanszírozás szempontjából sem érdektelen az állami és a tulajdonosi funkciók elkülönítése. Az anyagi erőforrások szűkössége miatt biztosra vehető, hogy a KI üzemeltetők nem lesznek (lehetnek) képesek teljes körű biztonságra törekedni, így közöttük is biztosítani kell olyan koordinációt, amely segíthet meghatározni a legszűkebb keresztmetszeteket, az elsősorban anyagi okokból redukált védekezési helyzet kulcsfontosságú pontjait, kihasználva szinergikus lehetőségeket is.

Álláspontom szerint meg kell oldani a következő helyzetet: A KI védelem pénzügyi-beruházási szempontból is értelmezhető úgy, hogy annak finanszírozása, pénzügyi megoldása egyértelműen a tulajdonosi/üzemeltető kör feladata, azonban szinte biztosra vehető, hogy az érintettek előbb-utóbb anyagi lehetőségeiket messze meghaladó probléma elé kerülnek. A KI védelmi feladatok ellátása azonban nyilvánvalóan nemcsak a tulajdonos/üzemeltető érdeke, hanem a társadalom szélesebb rétegeinek is. Ezért a finanszírozásánál megfontolandó lehetne az anyagi terhek szabályozott elvek szerinti megosztása. Ennek szabályozására is szükség lenne, hasonlóan mindazon további szempontokhoz, amelyek a KI hazai szabályozása tárgyában megjelent szakirodalomban is olvashatóak. [14] Érdemes lenne megvizsgálni: lehetséges és indokolt-e az igazolt KI finanszírozás valamilyen kedvezményezése a közgazdasági szabályozórendszer keretei között.

Van egyedi program, illetve EU Bizottság által évenként meghirdetett pénzügyi pályázati forrás lehetőség a KI védelemre fejlesztésére, a válságidőszaki biztonság fenntartására, vagy pl. az interdependencia elemzési módszereinek fejlesztésére is az IKT szektorban.[15]

[15] Részleteket lásd a Nemzeti Fejlesztési és Gazdasági Minisztérium honlapján
http://www.nfgm.gov.hu/feladataink/kulgazd/vedelem/egyediprg_biztonsag.html?query=kritikusinfrastrukt%C3%BAra
Letöltés: 2010. május 9.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

Jelen cikk néhány kiemelt szempont segítségével áttekintést adott a KI védelem jelenlegi helyzetéről, a továbblépést nehezítő egyes tényezők elemzése, bemutatása útján. Célom az volt, hogy egy folyamatban lévő, KI védelemmel kapcsolatos alágazati kutatómunka kezdetén felmérjem az aktuális állapotokat, bemutassak eredményeket, s felhívjam a figyelmet a még megoldásra váró problémák és eldöntendő kérdések sokaságára. Az elemzés alapján megállapítható: a KI védelem szerteágazó, szövevényes, sokszor rajtunk kívülálló eseményektől is függő jellege miatt aligha várhatóak gyors és mindenre kiterjedő megoldások. A döntés-előkészítő munka sokszereplős, részérdekektől erősen tagolt mind belföldi, mind nemzetközi vonatkozásban. A KI védelem ügye az elemzett szempontok (fenyegetettség, stratégiák, definíciók, azonosítás, tulajdonviszonyok, adatbázisok, jogalkotás, szervezeti kérdések, finanszírozás) egyikében sem tekinthető teljes körűen megoldottnak. Remélem, hogy javaslataim, észrevételeim – ha mégoly szerény mértékben is – közelebb vihetnek az életkörülményeink szempontjából fontos KI védelem ügyének megoldásához.

IRODALMI HIVATKOZÁSOK

[1] A Magyar Köztársaság biztonság- és védelempolitikai alapelveiről szóló 94/1998. (XII. 29) OGY. határozat 1. pont http://www.mkih.hu/torvenyek/o98h0094/o98h0094.htm Letöltés: 2010. május 3.

[2] A Magyar Köztársaság biztonság- és védelempolitikai alapelveiről szóló 94/1998. (XII. 29) OGY. határozat 2. pont http://www.mkih.hu/torvenyek/o98h0094/o98h0094.htm Letöltés: 2010. május 3.

[3] Bakos Ferenc: Idegen szavak és kifejezések szótára. Nyolcadik kiadás. Akadémiai Kiadó Budapest 1986. 949 oldal.

[4] Az Európa Lexikon részlet az Euro Infó Service kiadásában megjelent "Madari Ákos: E, mint Európa" c. könyvből. A könyv teljes szövege megtalálható az Európa Szerver oldalon. http://www.eutanfolyam.hu/index.php?mod=dinamikus&page=lexikon&b=i Letöltés: 2010. május 6.

[5] Magyar Larousse: Enciklopédikus szótár, H-M kötet ISBN 963-05-6421 Akadémiai Kiadó Budapest 1992. 1002 oldal.

[6] 2080/2008.(VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. http://www.otm.gov.hu/web/jog_terv.nsf/0/19659F03FD726909C12574C20034751C/$FILE/2080_2008_Korm-hat.pdf Letöltés: 2010. május 3.

[7] Mórotzné Cecei Katalin - Mórotz Attila: Klímaváltozás és a kritikus infrastruktúra. „Agro-21" Füzetek. ISSN 1218-5329 Kiadó: „Agro-21" kutatási programiroda. Budapest 2004. 36. szám 93 oldal, pp. 39.

[8] Mórotzné Cecei Katalin - Mórotz Attila: Klímaváltozás és a kritikus infrastruktúra. „Agro-21" Füzetek. ISSN 1218-5329 Kiadó: „Agro-21" kutatási programiroda. Budapest 2004. 36. szám 93 oldal, pp. 40.

[9] Dr. Kovács László: Kritikus információs infrastruktúrák. Egyetemi jegyzet. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest 2007. 206 oldal, pp. 21-30.

[10] Bukovics István – Vavrik Antal: Infrastruktúrák kockázata és biztonsága: kritikai problémaelemzés, Hadmérnök I. évfolyam 3. szám. 2006. december, pp. 32-40. http://www.hadmernok.hu/archivum/2006/3/2006_3_bukovics.pdf
Letöltés: 2010. május 6.

[11] Précsényi Zoltán - Solymosi József: Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé. Hadmérnök II. évfolyam 1. szám. 2007. március. http://www.hadmernok.hu/archivum/2007/1/2007_1_precsenyi.html
Letöltés: 2010. május 6.

[12] Munk Sándor – Fleiner Rita: Adatbázisok kritikus infrastruktúrákban. Hadmérnök IV. évfolyam 1. szám. 2009. március.
http://www.hadmernok.hu/2009_1_fleiner.php
Letöltés: 2010. május 9.

[13] Nemzeti Fejlesztési és Gazdasági Minisztérium: Kritikus Infrastruktúra Védelmi Nemzeti Program Konzultációs Fórum. Háttérismertető. Budapest, 2009. március 2. Szerkesztette: Baranyó Csaba 77 oldal, pp. 18.

[14] Mógor Judit - Földi László - Solymosi József: Lépések a kritikus infrastruktúra védelmének magyarországi szabályozása felé. Hadmérnök III. évfolyam 4. szám. 2008. december
http://www.hadmernok.hu/archivum/2008/4/2008_4_mogor.html
Letöltés: 2010. május 9.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Szabó Zsolt
szabo.zsolt@zmne.hu

A KECSKEMÉTI REPÜLŐBÁZIS TALAJ- ÉS VÍZSZENNYEZÉSÉNEK KÁRMENTESÍTÉSE, A MEGELŐZÉS ÚJ BIZTONSÁGTECHNIKAI MEGOLDÁSAI

Absztrakt

A cikk ismerteti a környezetszennyezés okát és mértékét, majd részletesen bemutatja a kármentesítés végrehajtásának módszereit, a munkálatok főbb adatait, valamint a megelőzés új biztonságtechnikai megoldásait. A kármentesítés tanúságai, valamint a telepítés problémái kerülnek ismertetésre.

In this paper the causes and extent of contamination will be shown. The remediation methods and the most important data of this process, as well as the new preventive safety solutions will be discussed. The conclusions and highlight the possible future problems will be determined.

Kulcsszavak: *környezetszennyezés, kármentesítés, biztonságtechnika ~ pollution, remediation, security*

BEVEZETŐ

„A föld védelme kiterjed a föld felszínére és a felszín alatti rétegeire, a talajra, a kőzetekre és az ásványokra, ezek természetes és átmeneti formáira és folyamataira. A föld védelme magában foglalja a talaj termőképessége, szerkezete, víz- és levegőháztartása, valamint élővilága védelmét is.” [1]

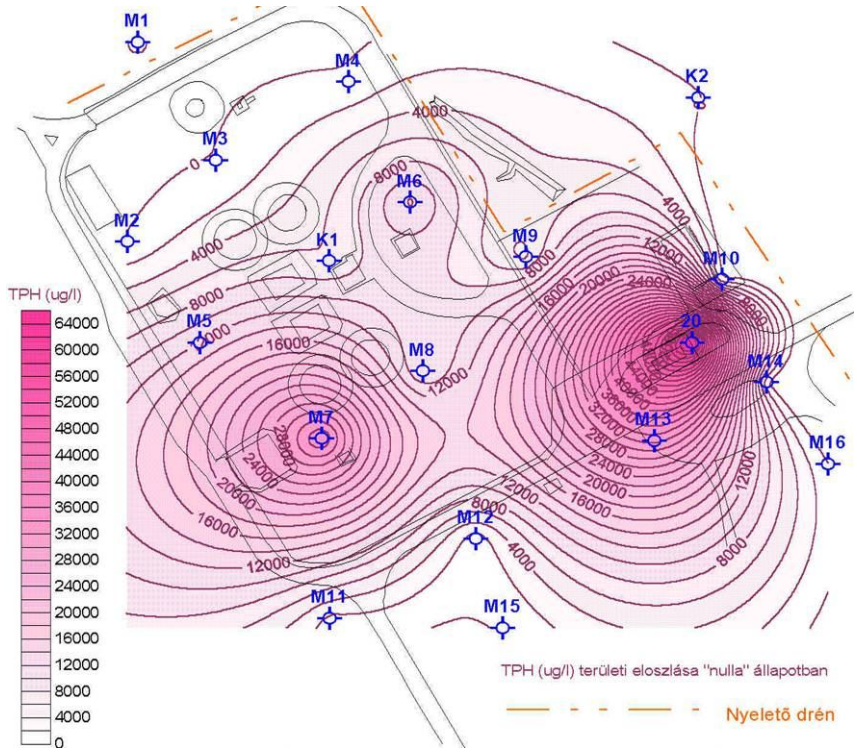
A talaj a földfelszín legfelső, termékeny rétege mely ökológiai és emberi tevékenységhez kötődő funkciókkal bír. A talaj megújuló képessége behatárolt. Leginkább az ökológiai funkciók sérülékenyek és védelemre szorulnak. Különféle anyagok talajba jutása szennyezést okozhat. A szennyeződés az, amikor a szennyezőanyag egy, az anyag minőségétől függő nagyságú koncentrációt meghalad. [2]

Egy repülőtér üzemeltetésének egyik legnagyobb kihívása a föld és a víz védelme. A nagy mennyiségben felhasznált hajtó- és kenőanyag tárolása, kezelése, a légijárművekbe történő feltöltése és/vagy leengedése a legújabb technológiák alkalmazását követeli meg.

A kecskeméti repülőtér hajtóanyag tároló és kiszolgáló rendszerét az ’50-es években alakították ki. Az akkori technológiának megfelelően a tároló tartályok és az azokat összekötő csővezeték rendszert a földbe ásták be. A tartályok szimpla falúak voltak, s a korrózió következtében szivárogni kezdtek. A ’90-es évek végére a talajszennyezés már olyan mértéket öltött, hogy elengedhetetlenné vált a környezeti károk felszámolása. A Honvédelmi Minisztérium megbízásából az ALTERRA Építőipari Kft. több, mint egy évig tartó tervezői és engedélyeztetési eljárást követően a 219/2004. (VII. 21.) korm. rendelet „A felszín alatti vizek védelméről” jogszabálynak megfelelően a kármentesítés két munkaterületen (üzemanyagkút és hajtóanyag telephely) 2001. május 02-án megkezdte. A munkálatok több lépcsőben 2008-ig tartottak.

Feladat a talaj és a talajvíz TPH[1] és BTEX[2] (2003-tól) tartalmának meghatározott szint alá (talaj esetében 30 mg/kg, talajvíz esetében 50 µg/l) csökkentése volt. [3]

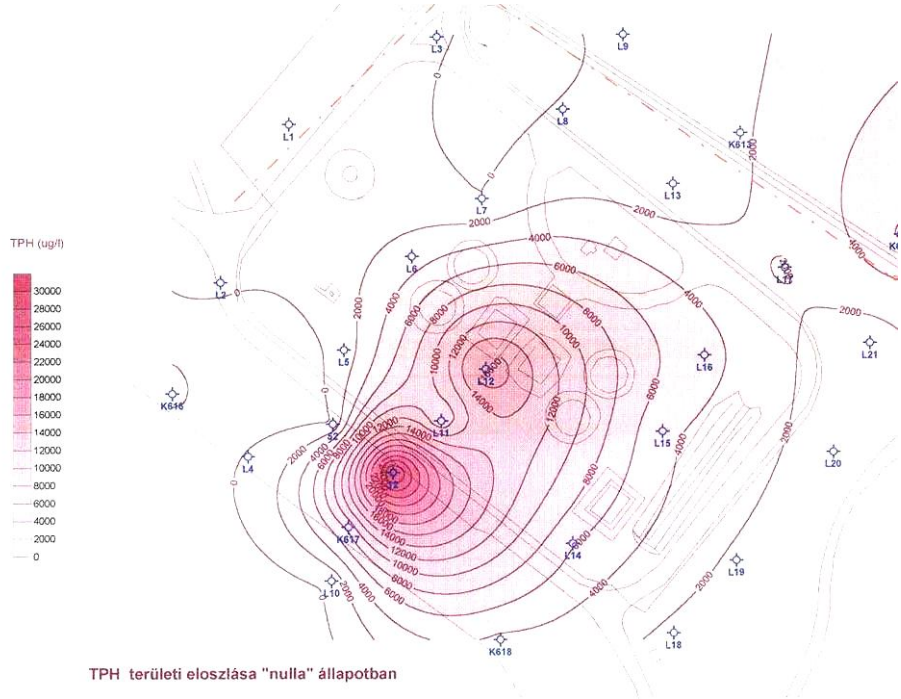
A kármentesítési munkálatokat a szennyezés mértékének megállapításával, s a szennyezett terület behatárolásával kezdték.



1. ábra. A talajvízszennyezés (TPH) kiterjedése az üzemanyagkút területén „0” állapotban.

[1] TPH - Total Petroleum Hydrocarbons - Összes Ásványolaj szénhidrogén
[2] BTEX – mozaikszó – benzol, toluol, etil, xilol

Az 1. ábra[3] a talajvízszennyezés (TPH) kiterjedését mutatja az üzemanyagkút területén „0” állapotban.



2. ábra. A talajvízszennyezés (TPH) kiterjedése a hajtóanyag telephely területén „0” állapotban.

A 2. ábra[4] a talajvízszennyezés (TPH) kiterjedését mutatja a hajtóanyag telephely területén „0” állapotban.

A KÁRMENTESÍTÉS VÉGREHAJTÁSA

A két munkaterületen a szennyezett talajvizet vákuum technológiával emelték ki.

A talajba 4, illetve 6 m mélyre vákuumcsápokat helyeztek el, mely kollektor csöveken keresztül juttatták a vizet a vákuum gyűjtőtartályba. A gyűjtőtartály biztonságos működését egy „alsó-felső szint érzékelő” automata irányította.

[3] ábra: ALTERRA Építőipari Kft
[4] ábra: ALTERRA Építőipari Kft



3. ábra. Vákuum csápok, gyűjtőtartály [fotó: Szabó Zsolt]

A gyűjtőtartályokból csőrendszeren keresztül központi víztisztító műbe (4. ábra) szivattyúzták a szennyezett talajvizet. A szennyező anyagot 4 lépésben távolították el a talajvízből.



4. ábra. Víztisztító mű [fotó: Szabó Zsolt]

Az első lépésben az illékony anyagokat kipárologtatták a vízből. A tartályban (5. ábra) a vizet keringtetik, s közé nagy nyomású levegő áramlik. A keletkező gázok elszívó ventillátoron keresztül biofilterbe áramlanak, ahol megtisztulnak. A tiszta levegő szelepen keresztül a szabadba távozik.



5. ábra. Illó szénhidrogéneket kiválasztó tartály [fotó: Szabó Zsolt]

A biztonságos üzemelés és a robbanásveszély elkerülésére a területet monitoring rendszer figyelte, s a megengedettnél magasabb koncentráció esetén az elektronika leállította volna a rendszer működését.

A második lépésként a levegővel dúsított víz iszapülepítő konténerbe (6. ábra) került. A fémoxidok és egyéb lebegő szennyeződések leültek a konténer aljára, melyet csővezetéken az iszapszikkasztóba (7. ábra) vezettek. Az iszap veszélyes hulladék, ezért azt elszállították és megsemmisítették.



6. ábra: Iszapülepítő
[fotó: Szabó Zsolt]



7. ábra: Iszapszikkasztó
[fotó: Szabó Zsolt]

A harmadik lépés többrétegű kavicsszűrő (8. ábra), majd a negyedik lépésként a víz kb. 5 tonna aktív szenet tartalmazó végfokozati szűrőbe (9. ábra) került.



8. ábra. Kavicsszűrő
[fotó: Szabó Zsolt]



9. ábra. Aktív szenes szűrő
[fotó: Szabó Zsolt]

A megtisztított vizet gyűjtőmedencében (10. ábra) tárolták, majd a laboratóriumi bevizsgálást követően a szennyezett terület határán a földbe visszanyelették.



10. ábra. Tisztított víz gyűjtőmedence [fotó: Szabó Zsolt]

A további talaj- és vízszennyezés elkerülése érdekében 2004-ben új üzemanyagkút és hajtóanyag telephely épült. A kitermelt szennyezett talajt a laktanya területén kialakított biodepóniában helyezték el.

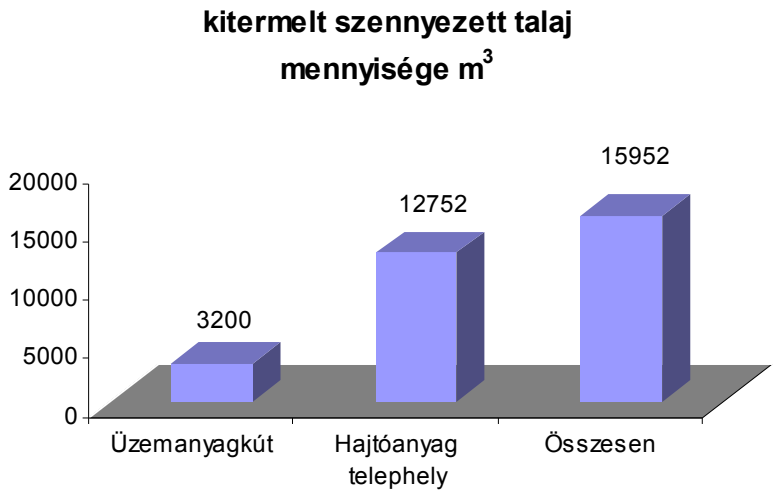
Az üzemanyagkút szennyezett talaját kitermelve egy talajvizes tó keletkezett, melyben a felúszó üzemanyag szennyeződést egy vízkiemelő zsompon (11. ábra) keresztül távolították el. A zsomp két rekeszből álló műtárgy. A befolyó szennyezett víz egy merülőfal alatt áramlik a második rekeszbe, így a felúszó szennyeződés az első rekeszből a tisztító nyíláson keresztül eltávolítható. A második rekeszben lévő talajvizet az eddig bemutatott víztisztító műbe továbbították.



11. ábra. Vízkiemelő zsomp [fotó: Szabó Zsolt]

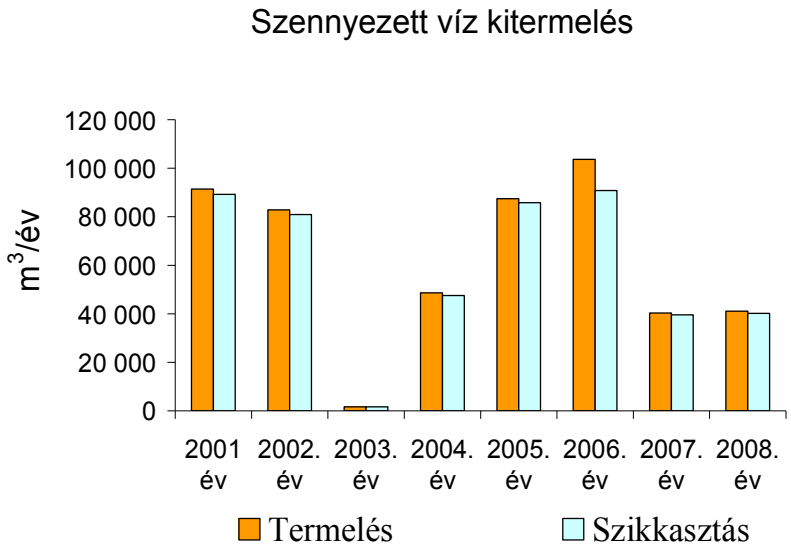
A KÁRMENTESÍTÉST BEMUTATÓ FŐBB ADATOK

A régi üzemanyagkút és a hajtóanyag telephely felszámolása során kiemelt és a biodepóniákba elszállított szennyezett talaj mennyiségét a 12. ábra mutatja.



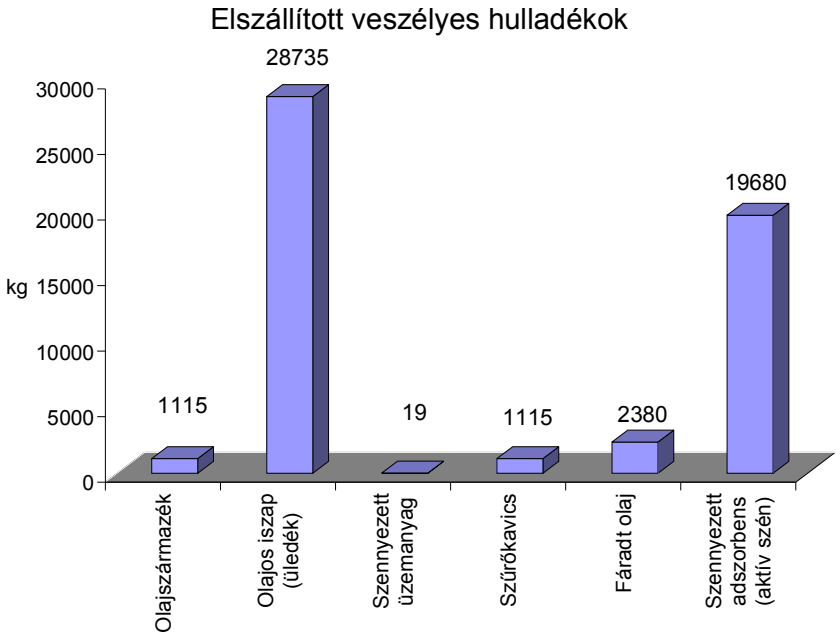
12. ábra.[5] A kitermelt szennyezett talaj mennyisége

[5] adat: ALTERRA Építőipari Kft, grafikon: Szabó Zsolt



13. ábra.[6] A kitermelt és megtisztított víz mennyisége

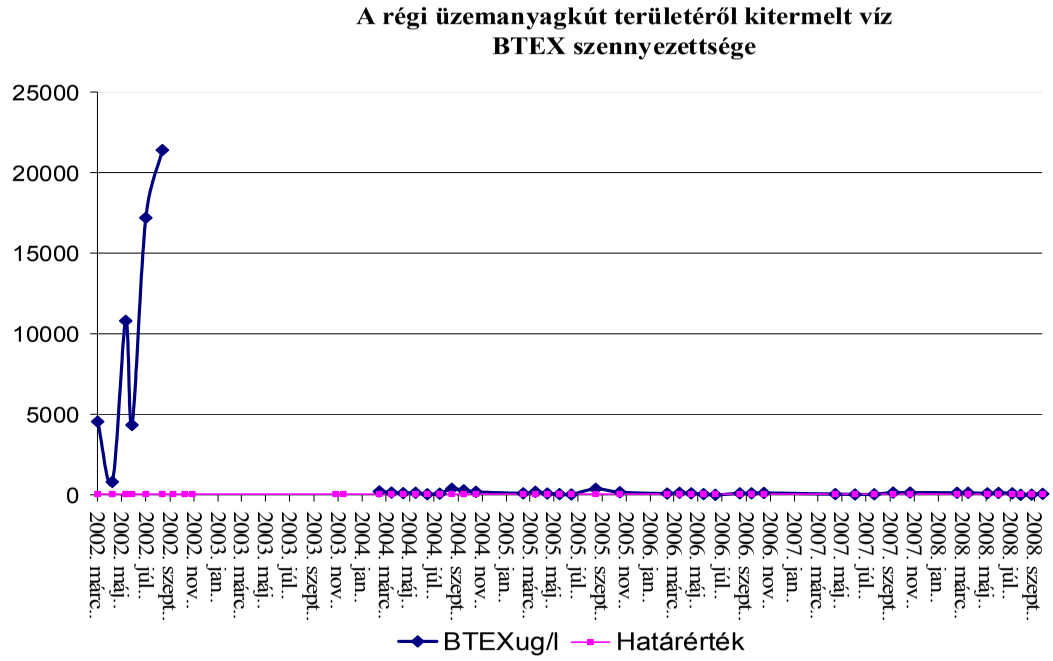
A 13. ábra a kármentesítés teljes ideje alatt kitermelt és megtisztított talajvíz mennyiséget ábrázolja. A munkálatok során mindösszesen 497 112 m^3 vizet nyertek ki, s 475 776m^3-t tisztítottak meg.



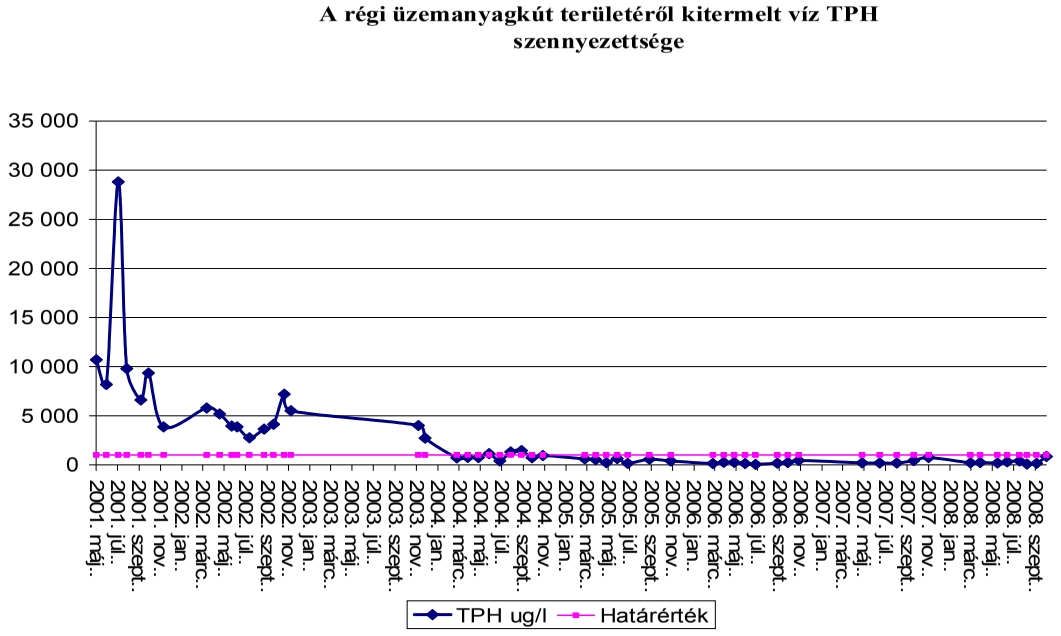
14. ábra.[7]Az elszállított veszélyes hulladékok mennyisége

[6] ábra: ALTERRA Építőipari Kft
[7] adat: ALTERRA Építőipari Kft, grafikon: Szabó Zsolt

A 14. ábra a mentesítés során keletkezett és megsemmisítésre elszállított veszélyes hulladékok mennyiségét ábrázolja.



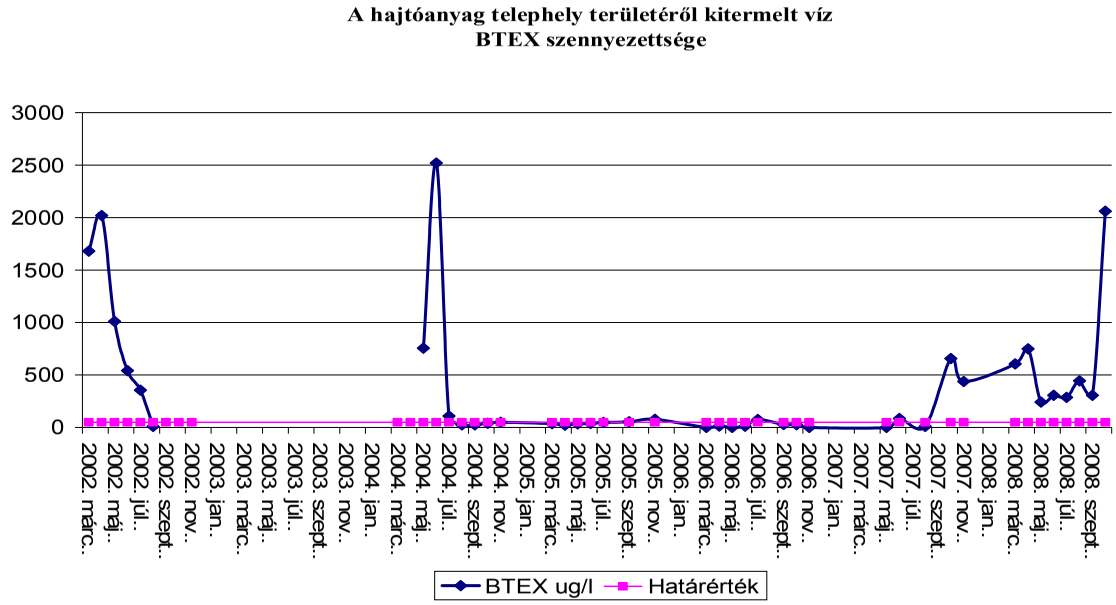
15. ábra.[8] A régi üzemanyagkútnál kitermelt víz BTEX szennyezettsége



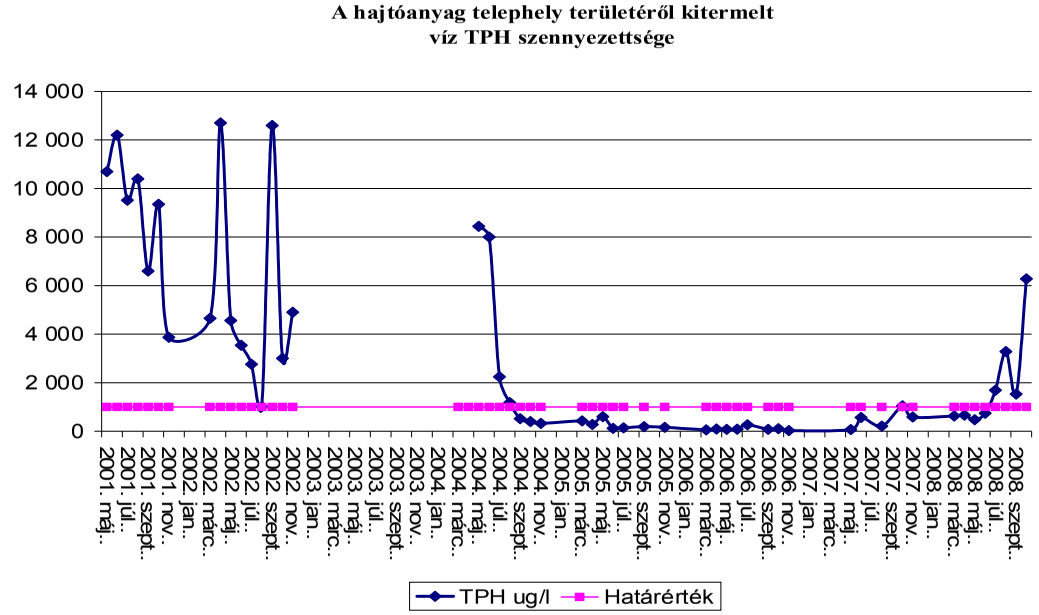
16. ábra.[9] A régi üzemanyagkútnál kitermelt víz TPH szennyezettsége

A 15. ábra a régi üzemanyagkút területéről kitermelt víz BTEX szennyezettségének, még a 16. ábra pedig a TPH szint alakulását mutatja. Jól látszik, hogy a munkálatok során mindkét szennyeződés szintjét rövid időn belül sikerült a megállapított határértékre csökkenteni

[8] ábra: ALTERRA Építőipari Kft
[9] ábra: ALTERRA Építőipari Kft



17. ábra.[10] A hajtóanyag telephelyen kitermelt víz BTEX szennyezettsége



18. ábra.[11] A hajtóanyag telephelyen kitermelt víz TPH szennyezettsége

A 17. és a 18. ábra a hajtóanyag telephely területéről kitermelt víz BTEX és TPH szennyezettségének alakulását mutatja. Látszik, hogy a határérték alá süllyedt szennyeződés értékek a munkálatok végére újra felugrottak.

[10] ábra: ALTERRA Építőipari Kft
[11] ábra: ALTERRA Építőipari Kft

A FÖLD ÉS A VÍZ VÉDELMÉNEK ÚJ BIZTONSÁGTECHNIKAI MEGOLDÁSAI

A laktanyába vasúti szállítással beérkező üzemanyagot egy vízzáró réteggel bevont területen fejtik le, mely tevékenység során esetleg szivárgó hajtóanyag nem kerül a talajba, hanem a csapadékkal keveredve egy gyűjtő csatornarendszeren keresztül ülepítő, leválasztó tározó rendszerbe folyik. Az ülepített szennyeződést megsemmisítésre elszállítják.

Az üzem- és hajtóanyag tárolása az újjáépített hajtóanyag tároló területén 50 m3-es, 200 m3-es és 1250 m3-es tartályokban történik.

Az üzemanyagot tartalmazó tartályok biztonsági felügyelete a Magyar Honvédségben alkalmazott monitoring rendszerrel történik. A repülőgép hajtóanyagot tartalmazó, nagy befogadó képességű tartályok biztonsági felügyeletét egy másik rendszer látja el.

A tartályokat dupla fallal látták el, s a két réteg között karbantartó, szerelőtér található. A külső és belső fal közötti rész levegőben jelenlévő üzemanyag koncentrációját egy jelző rendszer (19. ábra) figyeli. A megengedettnél magasabb koncentráció esetén, - mely a belső fal szivárgását feltételezi - riaszt, s egy automatikus szellőztető rendszert indít be (20. ábra). A rendszer a tároló két fala között addig nem engedi a világítás felkapcsolódását, míg a biztonságos szint alá nem süllyed a levegő káros anyag koncentrációja.



19. ábra. Üzemanyag koncentrációját figyelő szonda
[fotó: Szabó Zsolt]



20. ábra. Automatikus szellőztető rendszer
[fotó: Szabó Zsolt]

A hajtóanyag tartályok egy központi vezérlőre vannak bekötve, mely a tartályok állapot jellemzőit figyeli:

- a tartály töltöttségét, mely nagyban segíti a készletgazdálkodást;
- a hajtóanyag minimum és maximum szintjét, mely az esetleges túltöltést akadályozza;
- a tárolt anyag hőfokát.

A hajtóanyag telephelyen a szállító gépjárművek tartájait vízzáró réteggel ellátott területen, csepegésgátló töltő berendezéssel töltik fel.

Az új gépjármű üzemanyagtöltő állomás az eddig megszokottaknak megfelelően vízzáró réteggel ellátottak, s a szennyezett víz a gyűjtő rendszeren keresztül jut az ülepítő tartályba. Az üzemanyag tartályok dupla falúak, közüket fagyálló folyadékkal töltik fel. Szivárgás esetén a fagyálló folyadék puffer tartályában megnövekedik a szint, s a biztonsági rendszer jelez.

A repülőtéren a repülésről visszatérő repülőgépeket az indítási zónában töltik fel hajtóanyaggal és gázokkal. A zóna betonja is vízzáró réteggel van kezelve, ezáltal a töltés során lecsöpögő hajtó- és kenőanyag nem kerül a talajba. A beton enyhe lejtésének következtében a csapadékkal keveredő szennyeződés a gyűjtőárokba folyik (21. ábra), mely egy csatornarendszeren keresztül ülepítő tárolóba továbbítódik.



21. ábra. Vízgyűjtő árok [fotó: Szabó Zsolt]

A talaj és a víz szennyezésének megelőzése, illetve időbeni észlelése nem nélkülözi a hagyományos eszközök igénybevételét sem, ezért a repülőbázis területén monitoring kutakat (22. ábra) helyeztek el. [4]



22. ábra. Monitoring kút [fotó: Szabó Zsolt]

ÖSSZEFOGLALÁS

A környezet szennyezése sajnos véglegesen nem megszüntethető civilizációs ártalom, de törekedni kell bekövetkezésüknek minimalizálására. A modern biztonságtechnikai eszközök alkalmazása lehetővé teszik a környezetszennyezés megelőzését, a monitoring rendszer pedig az esetlegesen bekövetkező balesetek időbeni felfedését, a károk mentesítéssel történő elhárítását.

A kecskeméti repülőbázison stabil biztonsági rendszer került kialakításra, de a rendszernek van egy gyenge láncszeme. Az új helyre költöztetett és modern tartályokkal felszerelt hajtóanyag tároló és üzemanyag kút tartályai még az ’50-es években kiépített csővezeték rendszerhez kapcsolódnak. A további talajszennyezés elkerülése érdekében célszerű lenne egy következő ütemben ezek cseréje is.

FELHASZNÁLT IRODALOM

[1] 1995. évi LIII. törvény A környezet védelmének általános szabályairól

[2] Dr. Halász László-Dr. Földi László: Környezetvédelem II. ZMNE, Budapest, 2008.

[3] ALTERRA Építőipari Kft: MH 59. Szentgyörgyi Dezső Repülőbázis környezeti kármentesítése záródokumentáció

[4] Szabó Zsolt: A kecskeméti repülőbázis környezetvédelmi biztonságtechnikai megoldásai http://www.szrfk.hu/rtk/index.html

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Petró Tibor
petro.tibor@zmne.hu

A KÖZÚTI KÖZLEKEDÉS ÉS A BIZTONSÁG KAPCSOLATA AZ ALAGUTAKBAN

Absztrakt

Magyarországon a közúti közlekedés hálózata egy új elemmel bővült, miután a forgalom számára megnyitották az M6 autópályát Budapest-Pécs között. Az autópálya új műtárgyai közül az alagutak eddig nem tapasztalt kihívást jelentenek nem csak a közlekedők, hanem egy baleset következményeinek felszámolásában részt vevő mentőerők, illetve az üzemeltető számára is. Az európai tapasztalatok megismerésével, az Európai Unió szabályzóinak a magyar jogrendbe építésével, gyakorlatokkal azonban képesek lehetünk megfelelni e kihívásnak. A szerző célja a cikk megírásával, hogy az első ilyen létesítmény felavatása előtti gyakorlat eseményeinek leírásával bemutassa az autópálya-alagutak, mint a Magyarországon most megjelenő új közlekedési műtárgyak biztonsági rendszereit és összefoglalja az autópálya-alagutakban történő biztonságos közlekedés szabályait.

The road transportation network in Hungary has broadened with a new element, as the highway M6 has been opened between Budapest and Pecs. Tunnels, as new type of challenges has emerged from the structures of highways not only for drivers, but both for the operators and the disaster response forces. We will able to face this new challenge only with the knowledge of European experiences, building-in the regulations of the European Union into the Hungarian legislations and holding large-scale exercises to strengthen the practice. The aim of this paper was the security system's description of this new type of transportation structure by the detailed presentation of the first emergency exercise held just before the opening of the M6 highway tunnels, and to summarize the rules of safe traffic in highway-tunnels.

Kulcsszavak: *alagút gyakorlat, autópálya-alagutak biztonsága, katasztrófák alagutakban ~ tunnel, exercise, safety of highway tunnels, tunnel disasters*

Bevezető

Napjainkban, a felgyorsult világunkban egyre nagyobb igény van „A” pontból „B” pontba történő eljutás során a gyorsaságra, mely mellett fontos szempont, hogy az utazásunkat kényelmes körülmények között tehessük meg. Amennyiben nem szeretnénk a menetrend kötöttségei között utazni, akkor a közúti közlekedést kell választanunk. A közút azonban rengeteg veszélyt hordoz magában. Ahhoz, hogy a személyek, anyagok a leggyorsabban juthassanak el céljukhoz, szükség van a közlekedési infrastruktúra fejlesztésére.

A közúti közlekedés fejlesztése, ezen belül az autópálya fejlesztések minden kormány fejlesztési koncepciójában előkelő helyen szerepelnek. A legutóbbi autópálya beruházás keretében az M6/M60 autópálya 143,3 km-es szakaszát 2010. március 31.-n adta át a forgalomnak az akkori miniszterelnök, Bajnai Gordon. Az autópálya különlegességét hordozza, hogy Magyarországon először találkozhatunk alagútrendszerrel, mely a Szekszárd-Pécs közötti 81 km-es pályaszakaszon épített négy közúti közlekedési alagútból áll, amelyek természetesen megfelelnek a nemzetközi alagútbiztonsági előírásoknak. Magyarországon hasonló méretű, a közlekedést támogató alagút közúton még nem volt. Hazai vasúti közlekedés számára nem ismeretlen az alagútban történő közlekedés, hiszen pl. a Budapest-Esztergom vasúti vonalon találhatunk a közlekedést támogató alagutat.

Ha megvizsgáljuk a közúti közlekedés magyarországi fejlesztési elképzeléseit, több megvalósítandó új alagút tervét is megtalálhatjuk benne. Gondoljunk pl. az M0 északi szakaszának elgondolásaira. A tervezés egyik fő követelménye a biztonságra törekvés, azaz az üzemeltetés során a használat biztonságos legyen. A biztonság tartalmának meghatározása azonban időről változik. A múlt század elején akkor volt biztonságos egy alagút, ha abban a szembe jövők elfértek, a század közepén már tűzoltó erők tevékeny részvételét várták el az alagutat használók, míg napjainkban a korszerű biztonsági berendezések is részét kell, hogy képezzék egy-egy alagútnak.

Az alagútnak, mint műtárgynak a közlekedésben történő megjelenése kiemelt kockázatot jelent a közlekedésben részt vevők számára, legyen az autós, motoros, teherszállító, vagy csak utas egy autóbuszon. Ezt a kockázatot az út kezelőjének, jelen esetben a MAK Zrt. szakemberinek a minimális szintre kell csökkenteniük, melyet azonban megszüntetni nem lehet. Az alagút biztonsági berendezései, a lakosság ill. a közlekedők részére készített szóróanyagok, továbbá a rendőrség a közlekedési szabályok betartatásával a komolyabb balesetek megelőzését igyekeznek megakadályozni, míg a mentésben részt vevő szervek, mint eseménykövetők, a károk minimalizálásáért, a gyors kárfelszámolásért a felelősek. E képességük bemutatása történt 2010. 02. 23-án egy nagyszabású komplex gyakorlat keretei között az autópálya leghosszabb alagútjában.[1]

Alagutakban kialakuló katasztrófahelyzetek megelőzésének lehetőségei

A közelmúlt közlekedési balesetei ill. műszaki meghibásodásai alapján alagúttüzek komoly szerkezeti károkat, több esetben pedig tömeges halálesetet okoztak. A közlekedési veszélyhelyzetek kialakulásáért az emberi magatartás mintegy 90-95%-ban volt felelős, ugyanakkor az alagutakban kialakult tüzek esetén ez az arány már nem ilyen túlzó. A technikai meghibásodások (fék, ill. motortúlmelegedés, elektromos tűz) miatt kialakult veszélyhelyzetek száma alagúti tüzek esetén jóval magasabb. Ebben közrejátszik az alagutakban betartandó fokozott közlekedési szabályrendszer, mint pl. a csökkentett sebesség,

a külső körülményektől (időjárás) való mentesség. Ugyanakkor az elzárt térben kialakult alagúti balesetek és tüzek jóval nagyobb katasztrófahelyzetet idéznek elő, mint a nyílt pályás események. Egy-egy alagúttűzben a hőmérséklet könnyen elérheti az 1200 ^{o}C-ot, a sűrű, általában mérgező anyagokat tartalmazó füst nehezíti a mentési munkálatokat, a tűz időtartama jóval hosszabb, a baleset következményei így sokkal komolyabbak. Az alagutakban történt balesetek sajátossága lehet, hogy könnyen járhatnak tűzesetekkel, melyek esetenként olyan gyorsan terjednek, hogy a bent ragadtaknak esélyük sem marad a menekülésre a biztonsági berendezések nélkül.

Európa nagyobb alagút-katasztrófáinak bemutatása

Európában, főleg az Alpok területén, Franciaországban, Ausztriában, Olaszországban, sok kisebb-nagyobb alagúttal találkozhatunk, melyek közül szinte mindegyikben volt már baleset. Az elmúlt évtizedben azonban, több mint tíz nagyobb tűzesetből álló alagúttűz sorozat pusztított az anyagi javakban, emberéletekben.

A legnagyobb és legemlékezetesebb talán a tizenegy km-es *Mont Blanc alagútban történt katasztrófa* volt, mely 1999 tavaszán következett be. Az alagút az akkori idők egyik legnagyszerűbb mérnöki teljesítménye volt, melyet 1965. július 16-án adtak át a forgalomnak. Az alagút nagyban meggyorsította a közúti közlekedést Olaszország és Franciaország között. Segítségével mintegy két órával lehetett a közlekedésben töltött időt lerövidíteni. A kétszer egy sávos alagúton keresztül, melyet a lakók tiltakozása miatt nem bővítettek kétszer két sávosra, évente mintegy kétmillió autó közlekedik. A forgalom felét napjainkban a kamionok és teherautók adják.

Az Európa legmagasabb hegye alatt húzódó alagút egy csapásra vált égő pokollá 1999. március 24-én, melyet az alagút történelmének legnagyobb katasztrófája idézett elő. A tűz, amely 54 órán át tombolt, 39 ember életét követelte, melynek kivizsgálása mintegy két évig tartott. A vizsgálat megállapította, hogy a tűzet egy belga kamion sofőrje okozta, aki lisztet és margarint szállító Volvo teherautójának szellőzőablakán hanyagul kidobta parázsló cigarettáját az alagút elején. A kamion sofőrje a keletkezett tűzet csak későn, az alagút közepén vette észre, ahol megállt és megpróbálta eloltani az égő járművet, de a lángokat nem tudta megfékezni. Ezután a tűz rohamosan átterjedt más, az alagútban rekedt tűzveszélyes anyagot szállító járműre is. A tűz következtében 39 fő halt meg, és 40 jármű égett ki.[2]

Az okokat vizsgálva megállapítható volt, hogy a biztonságtechnikai hiányosságok mellett az emberi mulasztás, felkészületlenség volt a fő tényező. A biztonságtechnika oldaláról többek között problémát jelentett, hogy a baleset bekövetkezte után a jelzőrendszer még kilenc percig engedte a forgalmat az alagútba, korszerűtlen volt a biztonsági rendszer, melyet a baleset után át kellett építeni, a menekülő utak rendszerét pedig felül kellett vizsgálni.

A személyek felelősségének megállapításakor 16 embert vontak felelősségre, melyből csak az alagút biztonsági főnöke kapott letöltendő börtönbüntetést. A felelősök között találhattuk Chamonix település akkori polgármesterét is, aki 6 hónap felfüggesztett börtönbüntetést és tizenötezer euró mellékbüntetést kapott.

A Tauern-alagút katasztrófája:
A Tauern közúti alagút Ausztria Salsburg tartományának egyik legforgalmasabb alagútja. Az 1975-ben átadott alagút 6145 m hosszú, egyszer egysávos, mely a kialakítási mód a legmagasabb baleseti kockázatot hordozza magában.

1999. május 29-én egy teherautó okozott közlekedési balesetet, melyben a sorozatos ütközések következtében tűz ütött ki az alagútban. Az alagúttűzben 12 ember vesztette életét, ötvenen pedig súlyos sérülést szenvedtek. A kiérkező mentőerők a hatalmas füstnek és tűznyomásnak köszönhetően képtelenek voltak megközelíteni a tűz fészkét, a ventilláció pedig csak lassan kezdte megtisztítani az alagutat a füsttől a beavatkozás támogatása érdekében. A veszélyhelyzet elkerülése érdekében az alagutat felújították, a biztonsági rendszert megerősítették, 2006-ban pedig elkezdték az új, párhuzamos alagút építését, amely megnyitása után a közlekedés biztonságát alapjaiban változtatja meg.

A Gotthard-alagút tragédiája:
Svájcot Olaszországgal a Gotthard-alagút a maga 17 km-es hosszával a világ második leghosszabb alagútja, melyet 1980-ban adtak át a forgalomnak. Építésekor sem kerülte már el az emberáldozat, hiszen az építkezés folyamán 53 fő vesztette életét. 2001. október 24-én, egy közlekedési baleset miatt kialakult alagúttűzben pedig 11-en vesztették életüket, és 21-en kerültek kórházba. A baleset idején az alagútban mintegy 200 autó tartózkodott, melyből 128 tudott kimenekülni a baleset bekövetkezése után. A balesetet egy defektet kapott kamion okozta. A kialakult tűz mellett robbanás is súlyosbította az alagúti tragédiát, melynek hatására mintegy 100 m-en beszakadt az alagút mennyezete. A tűz pusztító erejére jellemző volt, hogy közel 200 méteren megsemmisültek az alagút elektronikus biztonsági berendezései. Az alagút három hónapos átépítése során szintén a biztonsági rendszerek korszerűsítése volt a prioritás.

A Mont Blanc, Gotthard, Tauern, továbbá a kapruni alagúttüzekben két év alatt 221 fő halála felhívta a figyelmet az európai vasúti és közúti alagutak tűz- és közlekedésbiztonságával kapcsolatos szabályozások felülvizsgálatára. A fenti példák alapján is belátható, hogy az alagutakban történő közlekedés fokozott biztonsági előírásokat és következetes emberi magatartási szabályok betartását követelnek.[3]

Alagutak biztonságának jogszabályi alapjai

Az Európai Unió, a transzeurópai közúthálózat alagútjaira vonatkozó biztonsági minimumkövetelményekről szóló, 2004. április 29-i 2004/54/EK európai parlamenti és tanácsi irányelv elfogadásával igyekezett a közlekedés biztonságát javítani, melyet a magyar jogharmonizáció az alagutak vonatkozásban a18/2007. (II. 20.) kormányrendelettel valósította meg. A jogszabály a transzeurópai közúthálózatnak a Magyarország területén lévő alagútjaira vonatkozó biztonsági minimumkövetelményeit határozza meg, és az alábbi fogalmakat tisztázza:

- alagút: a transzeurópai közúthálózatnak a Magyar Köztársaság területén lévő, zárt földtani közegbe beágyazott vonalas műtárgya, amely a közutat valamely akadály alatt vezeti át;
- alagút hossza: az alagút teljesen lefedett részén mért leghosszabb forgalmi sáv hossza;
- segélyszolgálat: a területileg illetékes állami vagy önkormányzati fenntartású, vagy az alagút üzemeltetői állományába tartozó szolgálat, amely baleset esetén beavatkozik, ideértve a rendőrséget, tűzoltóságot és a mentőszolgálatot is;
- működési engedély: olyan engedély, amely a biztonsági szempontokat kielégítő alagút forgalom számára történő megnyitását, illetőleg újbóli megnyitását teszi lehetővé;
- műszaki engedély: olyan engedély, amely a közlekedési műszaki szempontokat kielégítő alagút építését, korszerűsítését, forgalomba helyezését és megszüntetését engedélyezi;

- rendkívüli esemény: az alagútban közlekedő jármű műszaki hibája, ütközése, tűz, az alagúthasználó személyi sérüléses balesete vagy a rendeltetésszerű alagúti üzemet veszélyeztető üzemi körülmény;
- alagútkezelő: a Nemzeti Közlekedési Hatóság Kiemelt Ügyek Igazgatósága (a továbbiakban: Hatóság) által kijelölt, a közúti közlekedésről szóló törvényben meghatározott közútkezelő.

A kormány e rendeletében meghatározta az alagutak biztonságával foglalkozó szervezetek feladatát. E jogszabály keretei között nevezte meg a hatóság feladatrendszerét, alagútkezelő illetve a biztonsági tiszt kötelező tevékenységét.

A hatóság köteles gondoskodni:

a. az alagút rendszeres biztonsági vizsgálatáról, az ezekre vonatkozó biztonsági követelmények meghatározásáról,
b. a segélyszolgálatok alagutakkal kapcsolatos képzésére és felszerelésére vonatkozó szervezeti és működési rendszerek, valamint a vészhelyzeti intézkedési tervek kidolgozásáról,
c. rendkívüli esemény miatti azonnali lezárási rend meghatározásáról,
d. a szükséges kockázatcsökkentő intézkedések végrehajtatásáról,
e. az alagút kiviteli tervének a jóváhagyásáról,
f. a működési engedélynek a kiadásáról,
g. a működési engedélytől történő eltérések engedélyezéséről,
h. a működési engedélynek - a biztonsági minimumkövetelmények sérelme esetén történő - korlátozásáról, felfüggesztéséről (a továbbiakban: az alagút lezárásáról) és azoknak a feltételeknek a meghatározásáról, amelyek teljesülése esetén az alagútban a rendeltetésszerű üzem helyreállítható, illetve az alagút a közforgalom számára újra megnyitható,
i. a biztonsági minimumkövetelményektől való eltérések engedélyezéséről.

A kezelő illetve a kezelői feladatok meghatározásakor a jogszabály a korábbi, nemzetközi balesetek tapasztalatait is beépítette. E szerint egy alagútnak csak egy kezelője lehet akkor is, ha az részben Magyarországon részben pedig valamely szomszédos ország területén helyezkedik el. Meghatározza az alagút kezelő részére, hogy az alagútban bekövetkezett rendkívüli eseményről jelentést készítsen, melyet 8 napon belül továbbítania kell a biztonsági tiszthez, a Hatósághoz és az érintett segélyszolgálatokhoz.

Egy-egy súlyos személyi sérüléssel vagy halálesettel járó rendkívüli esemény kapcsán, az alagútkezelő kell, hogy kivizsgálja a balesetet, melyről készült vizsgálati jelentésben elemzi a bekövetkezés körülményeit és megállapítja a szükséges következtetéseket. Ezt a jelentését 30 napon belül köteles megküldeni az érintettek részére, mely segíthet a kárfelszámolás tapasztalatait feldolgozni, ezzel is növelve egy következő beavatkozás hatékonyságát.

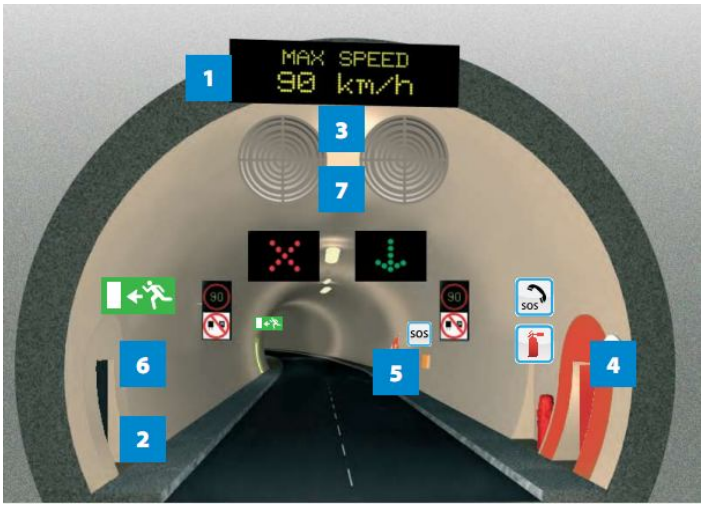
A vonatkozó jogszabály értelmében az alagút üzemeltetője biztonsági tisztet köteles kijelölni, aki azonban több alagút esetén is felelhet a biztonságért. Így van ez természetesen az M6 autópálya négy alagútja esetén is. Munkája során a biztonságot érintő kérdésekben független, döntését a munkáltatója utasítással nem befolyásolhatja. A biztonsági tiszt az alagút használóinak és az üzemeltetésért felelős személyzetnek a biztonsága érdekében koordinálja a megelőző intézkedéseket és óvintézkedéseket.[4]

Munkája során az alábbi feladatokat kell elvégeznie:

a) biztosítja a koordinációt a segélyszolgálatokkal, részt vesz ezen szervezetek alagutakkal kapcsolatos feladat- és tevékenységi körének kidolgozásában;
b) részt vesz a rendkívüli esemény során megvalósítandó intézkedések megtervezésében, végrehajtásában és értékelésében;
c) részt vesz a tervezésétől kezdődően a biztonságot érintő programok, az alagút szerkezeteinek, berendezéseinek és ezek működtetésének meghatározásában új vagy meglévő alagutak módosítása esetében;
d) ellenőrzi az üzemeltetésért felelős személyzet felkészültségét, és részt vesz a rendszeresen tartandó gyakorlatok szervezésében;
e) amennyiben szükséges, javaslatot tesz a kockázatelemzés elvégeztetésére;
f) tanácsot ad az alagutak szerkezeteinek és a berendezéseinek üzembe helyezésével és működtetésével kapcsolatban;
g) ellenőrzi az alagút szerkezeteinek és berendezéseinek megfelelő karbantartását és a szükséges javítások elvégzését;
h) részt vesz a rendkívüli események értékelésében.

Alagutak biztonságát szolgáló rendszerek

Az alagutakban történő biztonságos közlekedés személyi feltételein túl a jogszabály meghatározza azokat a kötelező technikai elemeket is, melyeket az üzemeltetőnek a biztonság érdekében fenn kell tartania. Az M6-os autópálya ill. a rajta lévő alagutak használatakor vannak olyan elemek, melyet a közlekedők is láthatnak, és természetesen vannak olyanok, melyek rejtetten végzik tevékenységüket. A zárt láncú kamerás megfigyelő rendszer, a tűzjelző és látótávolság ellenőrző rendszer, a burkolatba épített sebesség és forgalomszámláló rendszer ellenőrzi a forgalmat. Ezen túl segélykérők, porral oltók, kézi tűzjelzők, vészátjárók, változó fényerősségű előrejelző táblák, légelszívók növelik a veszélyben lévő közlekedők biztonságát.



1: váltakozó fényerejű tábla
2: menekülő útvonal
3: zárt láncú TV (CCTV)
4: segélyhívó fülke
5: segély és tűzjelző készülék
6: vészátjáró
7: hangosbeszélő-, tűz- és szellőzőrendszer

1. kép. Alagút biztonsági berendezések
(forrás: www.mecsekautopalya.hu)

A alagutak üzemeltetője a bátaszéki állomásról a központi számítógépes SCADA rendszer segítségével könnyen riaszthatja a mentésben részt vevő szervezetek, tűzoltóságokat. Ezen túl az üzemeltetőnek lehetősége van a hangosbeszélő rendszeren keresztül a helyes magatartási szabályok mentén utasítani az esetleges baleset miatt az alagútban rekedt személyeket. E

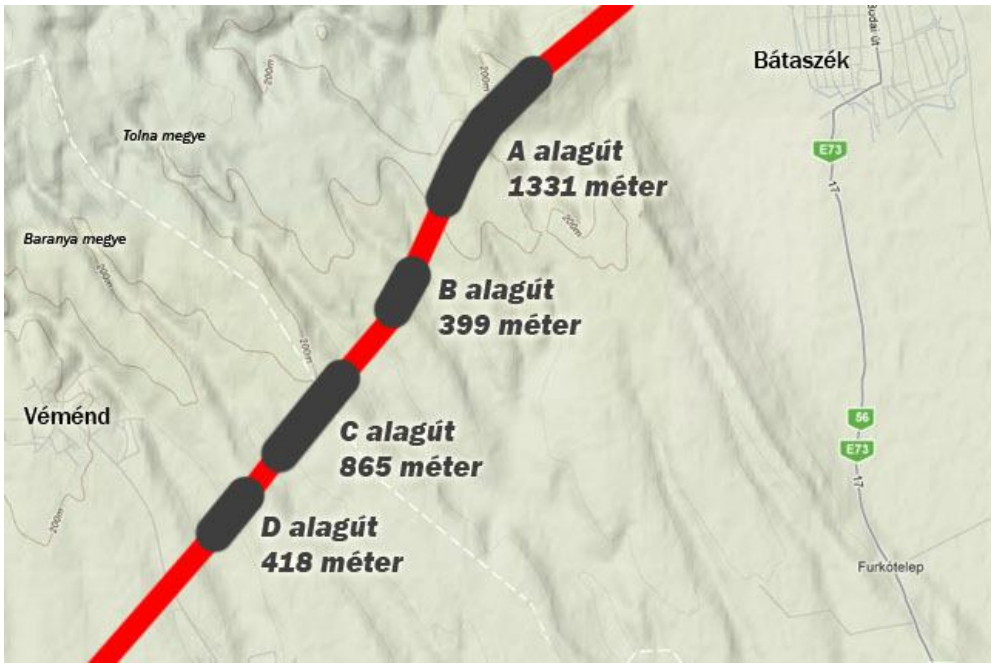
tevékenység szakszerű, határozott elvégzéséhez azonban elengedhetetlenek azok a gyakorlatok melyek a személyzet részére jó értelembe vetten „rutinszerűvé” teszik a katasztrófa felszámolás feladatait. Ezért volt szükség már az ideiglenes forgalomba helyezés előtt egy komplex gyakorlat megtartására.[5]

A gyakorlattal szemben az alábbi követelmények támaszthatóak:

- legyenek a lehető legélethűbbek, és feleljenek meg a meghatározott események forgatókönyvének,
- eredményezzenek világosan értékelhető eredményeket,
- előzzenek meg minden károsodást az alagútban,
- részben lehetnek asztali vagy számítógépes szimulációval végrehajtott gyakorlatok, amelyek kiegészítő eredményt hoznak.

Az M6 alagút gyakorlat bemutatása

Az M6 autópálya Bátaszék és Véménd közötti szakaszán összesen négy alagút van. A leghosszabb az „A” jelű, 1331 m hosszú, „B” 399, a „C” 865 a „D” jelű pedig 418 méter hosszú. Az alagutak közül a C jelűben az Országos Katasztrófavédelmi Főigazgatóság és az üzemeltető Mecsek Autópálya Koncessziós Zrt. közös gyakorlatot tartott 2010. február 23.-n.[6] A gyakorlatra, statiszta szerepkörben felkérték a Rendőrtiszti Főiskola tanulóit valamint a Zrínyi Miklós Nemzetvédelmi Egyetem hallgatóit is.



2. kép. Az M6 autópálya alagutjainak elhelyezkedése
(forrás: http://www.origo.hu/auto/20100402-oriasalagut-es-oriashid-vegigfilmeztuk-az-uj-m6os-autopalyat.html)

A gyakorlat kiindulópontja az események feltételezéseként megfogalmazott veszélyhelyzet beállítása volt. A feltételezett szituáció szerint az alagútban, mely 865 m. hosszú, menet közben kigyulladt egy festékeket és gumiabroncsokat szállító kisteherautó. A gépjármű vezetője az alagút utolsó harmadában megállt, és kézi porral oltó készülékkel megpróbálta a

kezdeti tűzet eloltani, de nem járt sikerrel. A gépkocsivezető elhagyva járműjét és a segélyhívó rendszeren próbált meg segítséget kérni az üzemeltetőtől.

A kialakult füst hatására az alagútban a forgalom feltorlódott, melyből baleset alakult ki. Az alagútban közlekedő iskolásokat szállító busz a feltorlódott kocsisor és rossz látási viszonyoknak köszönhetően a falnak ütközött és felborult. A buszt már kikerülni nem tudó személyautók közül néhányan a buszba rohantak és így szenvedtek balesetet.[7]

A helyzet a feltételezések szerint tovább romlott, amikor az alagútban, a következő baleset is bekövetkezett. Az alagútba érkező, majd az erős fékezés hatására bebicsakló veszélyes anyagot szállító teherautó szenvedett baleset. A teherautó a fékezés hatására a falnak ütközött, majd a rakománya a földön szétszóródott.

A biztonsági szolgálat a zárt láncú TV (CCTV) rendszeren látta az eseményeket, riasztotta a tűzoltóság, mentőszolgálat, rendőrség, NKH szakembereit, akik azonnal megkezdték a helyszínre vonulást majd a beavatkozást. A mentési munkálatok már javában zajlottak, mikor a lezárt pályaszakasz elkerülésére kijelölt „5606 A" jelű útszakaszon, Véménd közelében egy veszélyes anyagokat szállító jármű az árokba csúszott. A megsérült kamion rakománya, mely a szabadba került, erősen mérgező volt. A balesetet szenvedett jármű biztonsági zónájában lakók kimenekítését azonnal el kellett kezdeni, elhelyezésükről gondoskodni kellett. Ennek érdekében riasztották a megyei katasztrófavédelmi igazgatóságot, a polgári védelmi kirendeltséget, valamint megkezdte munkáját a helyi védelmi bizottság is.



3. kép. M6 gyakorlat kezdő helyszíne
(saját forrás)

A gyakorlaton feladattal az alábbi szervezetek vettek részt:

- Mecsek Autópálya Koncessziós Zrt.,
- Országos Katasztrófavédelmi Főigazgatóság,
- Tolna Megyei Katasztrófavédelmi Igazgatóság,
- Baranya Megyei Katasztrófavédelmi Igazgatóság,
- helyi polgári védelmi kirendeltségek,
- katasztrófavédelem Krízis Intervenciós Teamje,
- Mohács Város Hivatásos Önkormányzati Tűzoltósága,
- Szekszárd Megyei Jogú Város Önkormányzata Hivatásos Tűzoltósága,

- Véméndi Önkéntes Tűzoltóság,
- Bátaszéki Önkéntes Tűzoltóság,
- mentőszolgálat,
- rendőrség,
- Nemzeti Közlekedési Hatóság,
- Baranya Megyei Védelmi Bizottság,
- Tolna Megyei Védelmi Bizottság,
- helyi védelmi bizottságok.

A gyakorlat végrehajtása során az élethűséget nem csak a technikai elemek beállítása, a füstképző eszközök használata segítette. Fontos volt a baleset szenvedett járművekben lévő élő személyek - természetesen műsebek segítségével – olyan helyzetbe állítsák a gyakorlat szereplőit, melyek az éles helyzetekre nagyban hasonlítanak.

Ennek érdekében a gyakorlat előkészítő fázisában szakemberek ragasztottak műsebeket a diákokra, felkészítők mondták el, az adott helyzetben hogyan „kell" a sérültnek viselkednie. A mentőszolgálaton kívül, a tűzoltó egységek ill. az OKF által működtetett Krízis Intervenciós Team (KIT) is gyakorolta feladatát, mikor a balesetet szenvedett diákok színészi képességével találta szembe magát.



4. kép. ZMNE hallgatók a gyakorlat felkészülési időszakában, műsebekkel (saját forrás)

A jogszabály értelmében a lehető legélethűbb körülmények között végrehajtott teljes körű gyakorlatokat legalább négyévente meg kell tartani minden alagútban. (Az olyan területeken, ahol több alagút található egymás közelében, teljes körű gyakorlatot legalább egy alagútban kell tartani). Azonban az alagút lezárása csak akkor követelmény, ha elfogadható megoldások biztosíthatók a forgalom elterelésére. A teljes körű gyakorlatok mellett részleges vagy szimulációs gyakorlatokat minden évben kell tartani.

A gyakorlat végrehajtása során a mentőerők nagy létszámban jó eredménnyel szerepeltek, az alagútban történt katasztrófahelyzet felszámolásában részt vevő erők bizonyították képességeiket. Láthatjuk, és reméljük, hogy a periodikusan megtartott gyakorlatok segítik a közlekedés biztonságának megteremtését.

Megelőzés, lakosságfelkészítés lehetőségei a biztonságos közlekedésben

Egy-egy baleset kapcsán az eseménykövető beavatkozások csak a kár mértékének csökkentésére tudnak hatni. Itt is, mint oly sok más területen a megelőzés kell, hogy a biztonság alapja legyen. Ennek érdekében az alagútban közlekedőket is meg kell ismertetni a helyes és követendő magatartási szabályokkal.[8] Az autópálya e részének átadásával párhuzamosan az út kezelője kampányt indított a pályát használó autósok ismeretének bővítésére. Tájékoztató kiadványok készültek, melyek elsősorban az autópálya mentén található benzinkutakon, pihenőhelyeken szerezhetőek be könnyen. Néhány helyes magatartási szabály, mely az alagutakban történő biztonságos közlekedést támogatja:

Az alagút biztonságos megközelítése érdekében a közlekedő:

- Ellenőrizze az üzemanyagszintet!
- Vegye le a napszemüvegét!
- Kapcsolja be a tompított fényszórót!
- Hangolja rádióját a KRESZ-táblán feltüntetett rádióadóra, amelyen forgalmi információkat kaphat!
- Tartsa be a sebességkorlátozást, követési távolságot, változtatható jelzésképű tábla jelzéseit!
- Ne forduljon meg és ne tolasson!
- Vészhelyzet kivételével ne álljon meg!

Amennyiben baleset szenved a gépjármű vezetője, utasa:

- Baleset esetén húzódjon jobbra!
- Kapcsolja be a vészvillogót!
- A legközelebbi segélykérő helyről vagy segélykérő fülkéből értesítse a forgalomirányító központot!
- Szükség esetén nyújtson elsősegélyt!

Tűz esetén a következő magatartási szabályok a követendőek:

- Ha saját járműve fogott tüzet, próbálja meg az autóval elhagyni az alagutat! Ha ez nem sikerül, a leálló öbölben vagy az útpálya jobboldalán állítsa le a járművet és a motort! A legközelebbi segélykérő fülkénél kérjen segítséget és az ott elhelyezett poroltót levéve, kezdje meg az oltást! Ha nem tudja eloltani a tüzet, haladéktalanul hagyja el az alagutat!
- Ha az autó mögött érzékel tüzet vagy füstöt, hajtson ki az alagútból!
- Ha a jármű előtt van a tűz, állítsa le az autót az út jobb szélén, hagyja bent az indítókulcsot, és haladéktalanul távozzon a legközelebbi vészátjárón, illetve az alagút kijáratán át!
- Sűrű füst esetén kövesse a menekülési útvonal-jelzéseket!
- Kövesse a segélyszervezetek/üzemeltető személyzet utasításait!

Alagutak építésnek, használatának környezetvédelmi szempontjai

Alagutak építésnek, használatának környezet- és tájvédelmi szempontjai sem elhanyagolhatóak. Az autópálya e szakaszának építésekor különböző megvalósíthatósági megoldások jöhettek szóba, mint pl. a mélybevágás, szűkített támfalas bevágás lehetősége, azonban a táj és környezetvédelmi megoldások az alagutas kialakítást támogatták. Az

élőhelyek védelme, az építés, a nagymennyiségű kitermelt föld elszállítása, a környezeti terhelés minimálisra csökkentése, az állatok vonulási és keveredési képességének fenntartása fontos érv a beruházás mellett. Az alagutak felett a földfelszín egybefüggő és szinte érintetlen marad, a vadak és más állatok élőhely területe és mozgáslehetősége alig csökken. Ezen előnyökkel szemben, környezetvédelmi szempontból hátrányként a működés során felhasznált nagymennyiségű energia áll, melynek előállítása okozhat károkat környezetünkben. Érdemes e szempontokat is mérlegelnünk mielőtt véleményt alkotunk egy-egy alagút beruházásról, legyen az M6 autópályán megvalósult, vagy a jövő valamely megvalósítandó beruházása.[8]

Összefoglalás

Magyarországon a közúti közlekedésben, mint új kihívás jelent meg az alagutak biztonságos üzemben tartásának a szavatolása. Az európai tapasztalatok feldolgozása, megismerése, az Európai Uniós jogharmonizáció betartása, a rész illetve a komplex gyakorlatok szervezése, tapasztalatainak összegzése, mind a biztonság útján tett lépéseket, erőfeszítéseket jelzik. A közlekedők elvárják a biztonságos közlekedés feltételeinek megteremtését, ugyanakkor a folyamatos lakossági felkészítésről, az ismeretanyagok eljuttatásáról sem szabad elfeledkeznünk. A katasztrófahelyzetek felszámolásában részt vevő szervek a tapasztalatok alapján képesek a minimálisra csökkenteni egy-egy káresemény következményét, de a megelőzés fontosságát nem lehet elégszer hangsúlyozni. A megelőzéshez kell, hogy tartozzon az ésszerű szabályok betartatása, a lakosság, illetve a közlekedők számára nyújtott pontos, közérthető, helyes magatartási szabályok elsajátítása. E három pillér – biztonsági rendszerek, megelőzést támogató intézkedések, feladatait jól ismerő beavatkozó erők – garantálhatják a közlekedésben részt vevők számára a biztonságot.

Irodalom

[1] http://www.vezess.hu/bview.php/?bid=cikk&id=52&cid=23328&actio... Letöltés ideje: 2010. május 26.

[2] http://automenedzser.hu/hirek/20100216_M6.aspx letöltés ideje: 2010. május 26.

[3] Vonza Csilla: Tűz hatása az alagutakban Tanulmány Budapesti Műszaki és Gazdaságtudományi Egyetem Hidak és Szerkezetek Tanszéke 2010.

[4] 18/2007. (II. 20.) Korm. Rendelet a transzeurópai közúthálózatnak a Magyar Köztársaság területén lévő alagútjaira vonatkozó biztonsági minimumkövetelményekről

[5] Mecsek Autópálya Zrt. Alagút biztonsági tájékoztató 2010.

[6] http://www.origo.hu/auto/20100402-oriasalagut-es-oriashid-vegigfilmeztuk-az-uj-m6os-autopalyat.html **letöltés** ideje: 2010. május 27.

[7] http://portal.zmne.hu/portal/page?_pageid=34,135159&_dad=portal&_schema=PORTAL letöltés ideje: 2010. május 25.

[8] Nagy Lajos, Földi László, Nagy Károly: Kárelhárítás veszélyes áruk közúti baleseteinél I. VÉDELEM katasztrófa- és tűzvédelmi szemle VII. évf. 4. szám 48-50. o. (2000)

[9] http://www.unitef.hu/index.php?lang=HU&cid=450 letöltés ideje: 2010. május 26.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Balajti István
balajti@pt.lu

ÖSSZEFOGLALÓ A 2009-ES KALIFORNIAI NEMZETKÖZI RADAR KONFERENCIÁRÓL

Absztrakt

A radartechnológiák fejlődését reprezentáló konferenciák bemutatását az Egyesült Államokban, Pasadenában 2009-ben megrendezett konferencia anyagai közül válogattam.
A konferencia témája: Radarok a tudománytól a rendszerekig, amely magában foglalta a radar technológiák és a mérnöki megvalósítás tudományos elemeit és azok hatását. Mivel a felhasználók, mind a fejlesztők száma egyre növekszik, a fejlett modellezési eljárások, az algoritmusok, a terjedési jelenségek értékelése, és az eszközök kidolgozása beépül a jövő radarfejlesztéseibe.

Newly developed radar technologies that could be interesting for Hungarian experts were selected on papers of the Radar Conference held in Pasadena, California, USA, 2009.
The conference theme, Radars: From Science to Systems, expands the radar technology and engineering focus of previous conferences in this series to include and emphasize scientific or observational requirements and phenomenology that engender the systems that we develop in the radar community. As both the user and development communities expand, advances in modeling, phenomenology, device technologies, and algorithms will be achieved and influence future radar designs.

Kulcsszavak: *radar logisztika, céltárgy-detektálás, szintetikus apertúrájú radar ~ radar logistics, target detection, synthetic aperture radar*

Bevezetés

A megrendezett konferencia jól tükrözte az egy év alatt bekövetkezett fejlődést, de erősen a szponzoráló állami hivatalok, intézmények és a konferencia helyszínének közelében települt cégek elvárásainak felelt meg. A korábban megtartott konferenciákhoz hasonlóan, több

szekcióban és változatos témákban hangzottak el előadások, melyhez szervesen kapcsolódott a cégek, könyvkiadók látványos poszter bemutatója.

Radar korszerűsítési tapasztalatok

Az első, a radarok logisztikájára szakosodott szakemberek számára érdekes előadás, a 68 db nagy hatótávolságú radar teljes korszerűsítésének műszaki részleteit ismertette. A szerző Dr. Brookner és társai, s az előadásuk címe: Design and Implementation of Long Range Radar Service Life Extension volt. Közismert, hogy a tragikus szeptember 11-i események után az Amerikai Egyesült Államok az elavult földi telepítésű „D" (régi jelöléssel "L"sáv 1250-1400 MHz) frekvenciasávban üzemelő radarrendszerét feljavította, célként meghatározva, hogy gazdaságossá tegyék az üzemeltetést. A beépített legújabb műszaki megoldásokkal jelentősen növelték a céltárgy-detektálás biztonságát. Gyakorlatilag az történt, amit a Magyar Légvédelem a 90-es években véghezvitt, azaz, az eredeti radarból csak a települési hely, az antenna rendszer és a kiegészítő elemek egy része maradt meg. A 210 millió dolláros project tartalmazta a radarok teljes vevő, jel- és adatfeldolgozó alrendszereinek, valamint az adórendszerek félvezetősre való cseréjét. A nagyfokú egységesítéssel elérték a radarok élettartam költségeinek mérséklését. Az 1. sz. táblázat szemlélteti a felújított radarok műszaki paramétereinek javulását. Ezek a paraméterek és a megvalósított műszaki megoldások nagyon közel állnak a magyar eredményekhez, melyek a P-37, Szt-68, P-18 és PRV-17 radarok esetén már alkalmazásra kerültek.

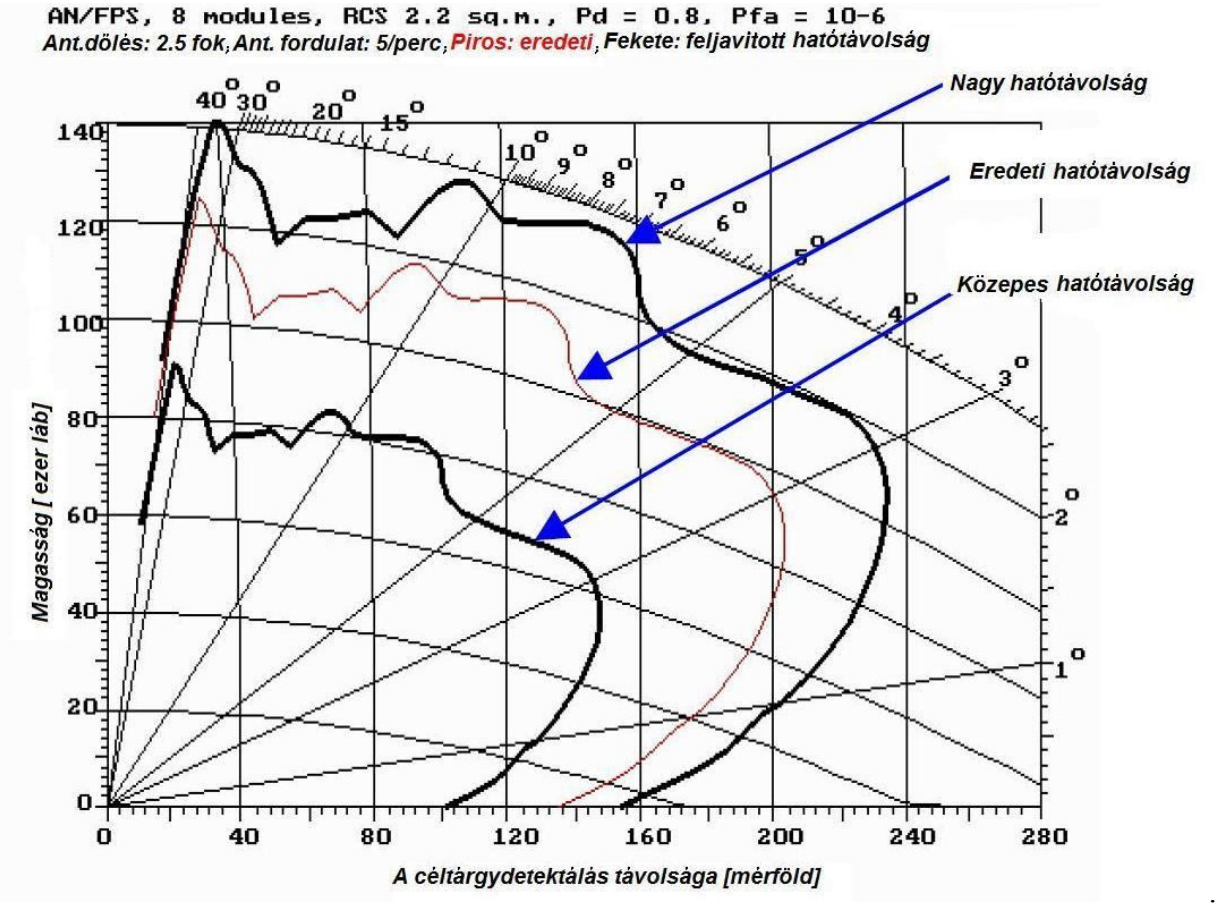
1. sz. Táblázat **Paraméter változás az AN/FPS-8 radar esetén**

Radar Paraméterek	**Korszerűsítés előtt**	**Korszerűsítés után**
Élettartam	0 év	20 +év
Impulzus/Átlag Teljesítmény	2000/4.2 (kW)	~58/5.0 (kW)
Mozgó Ablak Detector	Nem	Igen
Vaklárma Normalizálás	Igen	Igen (Szabvány: 10^{-6})
Adaptív Állócéltérkép	Nem	Igen
Vevő dinamika	62 dB	78+dBTeljes Tartományú STC
Adórendszer stabilitás	< 30 dB	~65 dB
Zavar-alatti céldetektálás	23 dB	~40 dB
Adaptivitás (Software)	Nem	Igen (paraméterezhető)
Paraméter bővithetőség	Nem	Igen (COTS)
Üzemeltetési költség	Magas + kiszámíthatatlan	Alacsonyabb

Dr. Brookner előadásában kiemelte, hogy a vevő és a jelfeldolgozó rendszer jól kihasználja a napjainkban megjelent új lehetőségeket, a rendkívül korszerű jelfeldolgozó algoritmusok radar környezetére szabott adaptivitás előnyeit. Ennek következtében a radarok főbb harcászati-műszaki paraméterei is jelentősen javultak az alábbi területeken:

- Vevőrendszer dinamika
- Adórendszer stabilitás
- Céltárgyak zavar alatti láthatósága.

Fontos tényként említette Brookner, hogy optimalizálták a szárazföldi és vízfelszín fölötti kis radar hatásos keresztmetszettel rendelkező céltárgyak detektálását. Minden radarba beépítettek egy új csatornát, a kiegészítő eszközökkel együtt, az időjárás és a többszörös hullámterjedés érzékelésére, hatásaik minimalizálására. Az 1.sz.ábra szemlélteti az elméleti céltárgy-detektálás növekedést, nagy és közepes hatótávolságok esetére.



1.sz.ábra. Céltárgy detekciós távolság növekedés

Az előadás végén vita alakult ki a szerzők által előnyként feltüntetett „Teljes tartományú STC" – vevőrendszer érzékenység szabályozás, (beleértve a maximális detekciós távolságot, mely kb. 400 km), valamint a radarokban alkalmazott „több-hipotézist alkalmazó" útvonalképzők, hátránya és esetleges szükségessége között. Ez, az első esetben az „angyal" jelenségek elleni védelem, részben elfogadható magyarázat, de az útvonalképzők alkalmazása, mivel a céltárgyak kinematikus képességei előre becslésén alapulnak egy 10 és 12 másodperces adatfrissítési idővel pont a legveszélyesebb manőverező célok kiszűrését eredményezik. Ehhez hasonló eredmények már születtek a volt Haditechnikai Intézetben a 80-as évek végén.

A radarokban alkalmazható modulációk/hullámformák fejlődési irányai

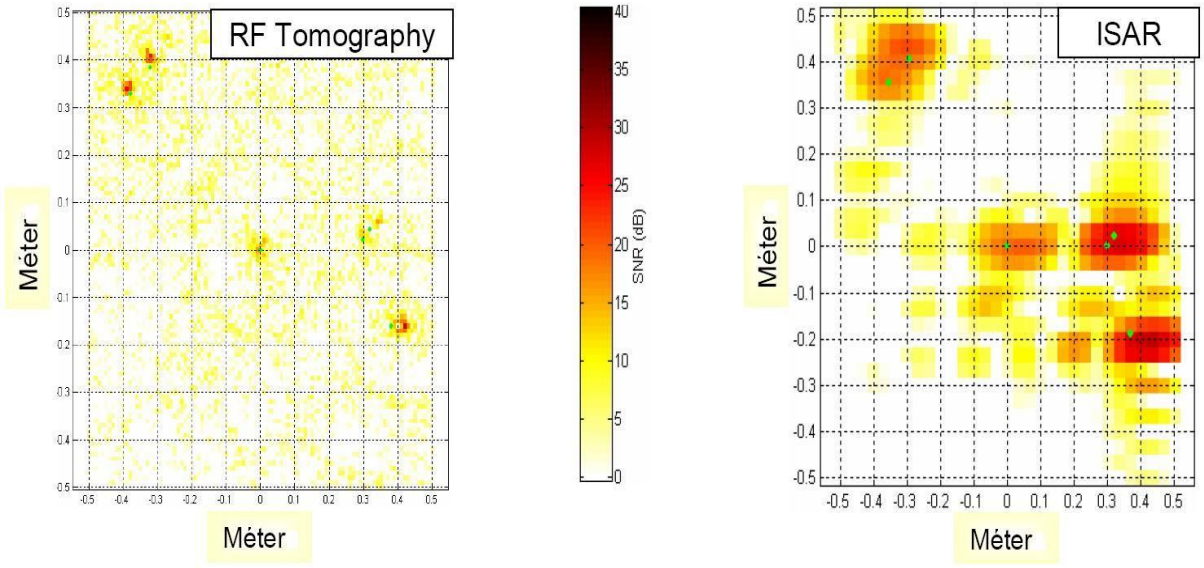
Számomra és a konferencia többi résztvevője számára is az egyik legérdekesebb előadás Dr. Wicks előadása volt. (USAF Research Laboratory. A Brief History of Waveform Diversity) „A hullámforma változatosság rövid története" címmel hangzott el. Az előadás bevezető része röviden áttekintette a radarok által alkalmazott adójelek fejlődését, kiemelve a fejlődés szempontjából mérföldkőnek számító megoldásokat. Ezek közül a legfontosabb az a tény, hogy az 1930-as években elkezdődött radar adójel hullámforma kutatás a 90-es évekre önálló kutatási területté vált. Ekkorra már meghatározásra kerültek azok a jelformák, modulációk, melyek optimálisak az állócél-zónában való céltárgyak detektálására. Napjainkban is tart a 90-es években kezdődött vezeték-nélküli kommunikációval kapcsolatos kutatási-fejlesztési lendület, mely új mérföldkőnek ígérkezik a radarokban alkalmazott modulációk/hullámformák sokszínűségének palettáján.

Ma már tudjuk, hogy túlléptünk az adaptív jelfeldolgozás, nyújtotta lehetőségeken és a környezet „tudás alapon” történő értékeléséből eredő előnyök kihasználására törekszünk. Dr. Wicks a fenti megállapítás jelentőségét a következő példán keresztül mutatta be. Jól ismert, hogy a napjainkban széleskörűen elterjedt adaptív jelfeldolgozási módszerek működése azon alapszik, hogy feltételezzük a vizsgálat alatt lévő cellában mért értékek statisztikai jellemzői hasonlóak a szomszédos cellákban mért értékekhez. Így a szomszédos cellák tartalma referenciaként szolgálhat az éppen elemzés alatt lévő cella tartalmára vonatkozóan. Ezért ha különbséget detektálunk, nagy valószínűséggel a várt jelre bukkanunk. Ez az eljárás elvárja, hogy azoknak a celláknak a tartalma, melyek a viszonyítási alapot képeznek, függetlenek legyenek az éppen vizsgálttól, és eloszlásuk egyenletes legyen az egész vizsgált tartományban. Ha ezek a feltételek nem, vagy csak részben teljesülnek, a jelfeldolgozás minősége romlik. Ezzel szemben a tudás alapú jelfeldolgozással kiegészített radarok kihasználják azt a lehetőséget, hogy előzetes információkkal rendelkezzenek a vizsgálat alatt lévő cellák tartalmára vonatkozóan. Ez a többlet információ real-time spektrum analízissel, a szomszédos cellák keresztkorrelációjára vonatkozó mérésekkel, részletes digitális térképekből, aktuális időjárási és mikrohullám terjedési adatokból beszerezhető és a radarok vevő és jelfeldolgozó rendszerében alkalmazhatók. Így a feladathoz, a környezethez, térben és időben optimalizálható a jel-moduláció. Ez a koncepció úgy kezeli az érzékelőket, mintha intelligens robotok lennének, melyek az élővilág érzékelési módjait utánozzák. Ebben a koncepcióban az egyes elemek viselkedése olyan, mint a madár, a bogár kolóniák vagy halrajok. Ezek, a nem túl intelligens elemek, minőségileg megnövelt képességekkel rendelkeznek és nagyon komplex feladatok végrehajtására is alkalmasak.

Dr. Wicks a „Robot” koncepció illusztrálását az emberi érzékszervek analógiáján keresztül mutatta be. Az ember a memóriáján és intelligenciáján túl öt érzékelési móddal rendelkezik: a látás, amely a nagy-hatótávolságú „felderítést” biztosítja, közepes távolságokra a hallást és a szaglást használjuk és a rövid hatótávolságú érzékelésre a tapintás, és a kóstolás szolgál. Minden érzékszer egymástól független és nem az egyén dönti el, mikor lát, hall vagy szagol, de ha valami felkelti az érdeklődését, arra koncentrálja érzékszerveit, próbálja kiszűrni a zavaró tényezőket, és ha szükségesnek látja, térben közelebb megy. Ez a működési elv nagyban hasonlít a robotérzékelők, pl. egy pilótanélküli repülő működtetési elvéhez, ugyanakkor a különböző hullámtartományokat alkalmazó érzékelők egyidejű alkalmazása és a fent vázolt működés realizálása még kidolgozásra váró feladat.

Ez az új feladathoz strukturált és orientált szintek szerinti és térben elosztott radar rendszer filozófia segíti az átmenetet az úgynevezett hálózat centrikus rendszerek megalkotásához. Sajnos napjaink egy-feladatra orientált radar rendszerei, beleértve az úgy nevezett több-feladatú radarokat is, még nem képesek automatikusan és a feladatra optimalizálva meghatározni, alkalmazni és dinamikusan átkonfigurálni a szükséges radarjel modulációkat. Szintén megoldásra váró feladat a céltárgy, radarhoz viszonyított változó helyzetéből eredő energiaszint ingadozások kezelése. A jelenlegi radar rendszerek új követelményekhez illesztése megköveteli a kiegészítő érzékelők rendszerbe integrálását pl. a céltárgyak radar fényképét előállító, ínvers szintetikus apertúrájú radarokat (ISAR), és a nagyobb felbontást biztositó RF Tomográfiát.

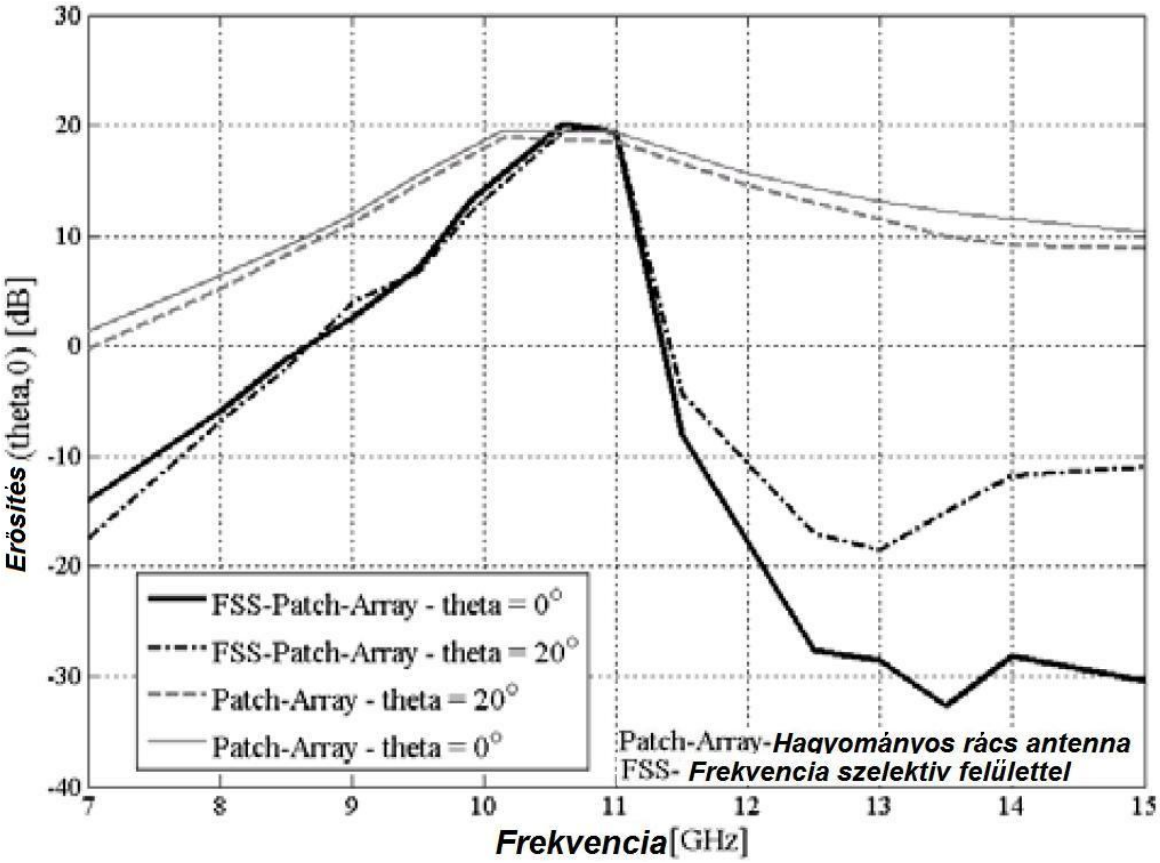
A 2.sz. ábra a két módszer felbontásában megjelenő különbségeket szemlélteti az RF tomográfia javára. (A kicsi zöld „pöttyel” jelölt pontok kis jel-zaj viszony esetre értendők)



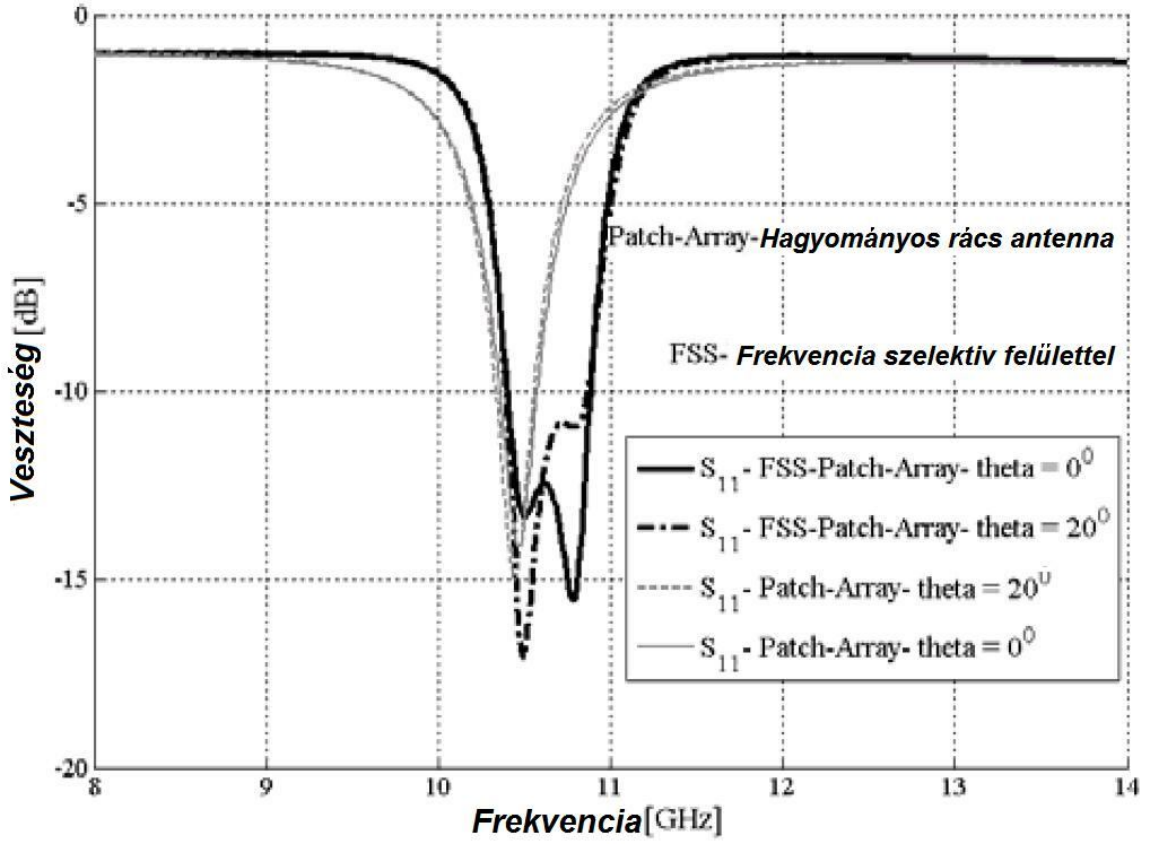
2.sz. ábra. Felbontás növekedés RF tomografia alkalmazásakor

A professzor előadása, összefoglalva arra hívta fel a figyelmet, hogy felvázolt rendszer effektív üzemeltetésének alapvető eleme a „Tudás-alapu vezérlés" megvalósítása, azaz a radarok modulációját optimalizálni kell a céltárgy helyzetváltozásának függvényében.
Megjegyzem, hogy ez a rendszer-koncepció nagyban hasonlít az általam a magyar légtérbiztonság és légvédelem érzékelő rendszerének fejlesztésére tett javaslathoz, mely az Új Honvédségi Szemle 2004-2005-ös számaiban magyar nyelven, míg az AARMS 2004 és 2008 számaiban angolul olvasható.

A következő nagy témablokk, amellyel rendszeresen foglalkozom a radar konferenciákról készült cikksorozatokban, a mikrohullámú technikában alkalmazható különleges képességekkel, tulajdonságokkal rendelkező anyagok. Ezen a területen is óriási fejlődés van az előző évekhez képest Az ezzel kapcsolatos kutatásokat a világ minden táján nagy érdeklődés kíséri, és köztudott, hogy az ilyen anyagok kutatása hazánkban is folyik. A téma fontossága miatt, a „Különleges tulajdonsággal rendelkező frekvencia szelektív anyag fázis-rács antennák számára" (F.Bayolpur, K.Sarabandi: A Metamaterial Frequency-Selective Superstrate for Ohase-Array Applications) előadás anyagát a magyar szakemberek számára is figyelemre méltónak találtam. Ebben az előadásban bemutattak egy új anyagot, amelynek frekvencia szelektív tulajdonsága jól ötvözhetők a fázisantennák RF jelszűrési lehetőségeivel. Az anyag az antenna felületére, felvitelre kerül a hullámhossz egytizedének vastagságában. Alkalmazásával az antennán kialakítható a vett jelek vételéhez illesztett RF szűrők, mely által az antenna méretei jelentősen csökkenthetők. A 3. és 4. sz. ábrákon bemutatott szimulációs eredmények alátámasztják azt a tényt, hogy az antenna sávszélessége 250 %-kal növelhető. A sávszélesség növelése és a fázisantenna méreteinek csökkenése nagyon jelentős szempont a katonai alkalmazásoknál, mivel a hagyományos radar-antennákon való alkalmazáson túl, a kommunikáció és az elektronikai hadviselés lehetőségeit is növeli, mint a zavarás, mint a védelem szempontjából.



3.sz.abra. Antenna jel-atvitel erosites a frekvencia fuggvenyeben



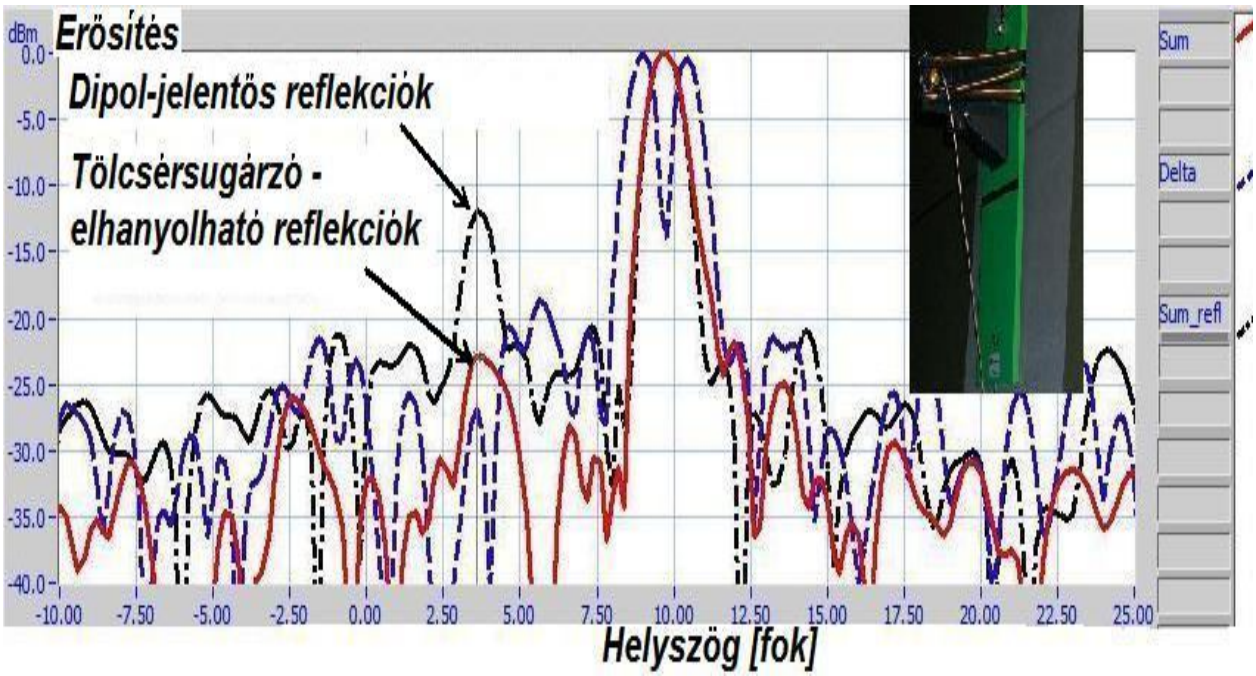
A 4.sz .ábra. „S” paraméterek az átviteli függvény értékelésére az új anyaggal és nélküle

„In Situ” mérési tapasztalatok

A radarok logisztikájával foglalkozó szakértők számára készült az üzemeltetett radarok performanciájának kiértékelését, mérési eredményeit és gyakorlati tapasztalatait összefoglaló előadásom. Címe Mitigation of the "In Situ" Radar Antennas Measurement Reflections and Multipath of the System Performance Checks, és a NAMSA szakembereknek a radar antennák közel-téri és távol-téri mérési eredményeit prezentálta.
Az a tény, hogy a méréseket jelentősen befolyásolja a tereptárgyakról visszaverődött reflekció és többszörös hullámterjedés nem új, de az, hogy ez mennyire bonyolítja a mért eredmények kiértékelését és néhány esetben, milyen extrém paraméterek, megjelenéséhez vezet, komoly figyelmet váltott ki. Az antenna paraméterek távoltérben történő mérése viszonylag egyszerű hiszen „csak” a vett jelek amplitudóját kell mérni. Lehetséges esetek:

- Ha az antenna nyaláb paraméterek kiértékelése kétséges, pl reflekció következtében az oldalnyaláb szint túl magas, akkor legtöbbször elégséges a mérés megismétlése egy új mérőpontból.
- Ha a magas oldal nyalábszintek az új mérőpont oldalszög szerinti elmozdulásával tolódnak el, akkor bizonyítottnak tekinthető, hogy az antenna paraméterei nem romlottak el.

A fő problémát ezzel a méréssel kapcsolatban az jelenti, hogy a radarok általában a környezet legmagasabb pontján találhatók (lásd Zengő/Tubes radartelepítéssel kapcsolatos vitákat), és így a távoli mérőpont kijelölése geometriailag gyakran csak a horizont alatt lehetséges, mely jeltorzuláshoz, megnövekedő reflekciókhoz vezet. Ezért a közeltéri mérések, melyek vagy az antenna felületén vagy attól néhány m-re egy körpalást mentén történnek, egyre nagyobb jelentőséget kapnak, bár ezek a mérések bonyolultabbak. Ugyanakkor a közeltéri méréseket is zavarják az antenna környezetében található, még a mérés érdekében sem elmozdítható oszlopok, épületek. Az 5. sz ábra egy olyan közeltéri mérés eredményét szemlélteti, amikor a közeltérben az antenna sikjában végzett mérési eredményt egy vasoszlopról történő visszaverődés jelentősen torzítja.
A közeltéri mérési adatok Fourier transzformációval átszámításra kerülnek az antenna távoltéri nyalábjára. Itt az eredmény értékelése okoz problémát, mivel az antenna felületét szondázó érzékelő (dipol) nagyon kis energiát bocsát ki, mégis a vételi oldalnyaláb szint energiája nagy. Ennek fizikai oka, hogy az oszlopról visszaverődött energia az egész antenna felületét besugározza, így az antennaerősítés szinte teljes nagyságában megjelenik az eredményben, míg a szonda csak a mért antenna elem környezetét méri. A megoldás „kézenfekvő”, meg kell akadályozni, hogy a szonda energiája eljusson a vasoszlopra és visszaverődjön arról. A gyakorlatban, több kísérlet után, sikerült kielégítő megoldást találni a problémára: a dipol alapu érzékelőt felváltotta egy jelentős irányélességgel rendelkező tölcsérsugárzó. Az 5. ábra azt is jól szemlélteti, hogy az oszlopról visszaverődő energiaszint, és az oldalnyalábszint, jelentősen csökkent.



5.sz.ábra. Reflekció hatásának csökkentése közeltéri mérés esetén

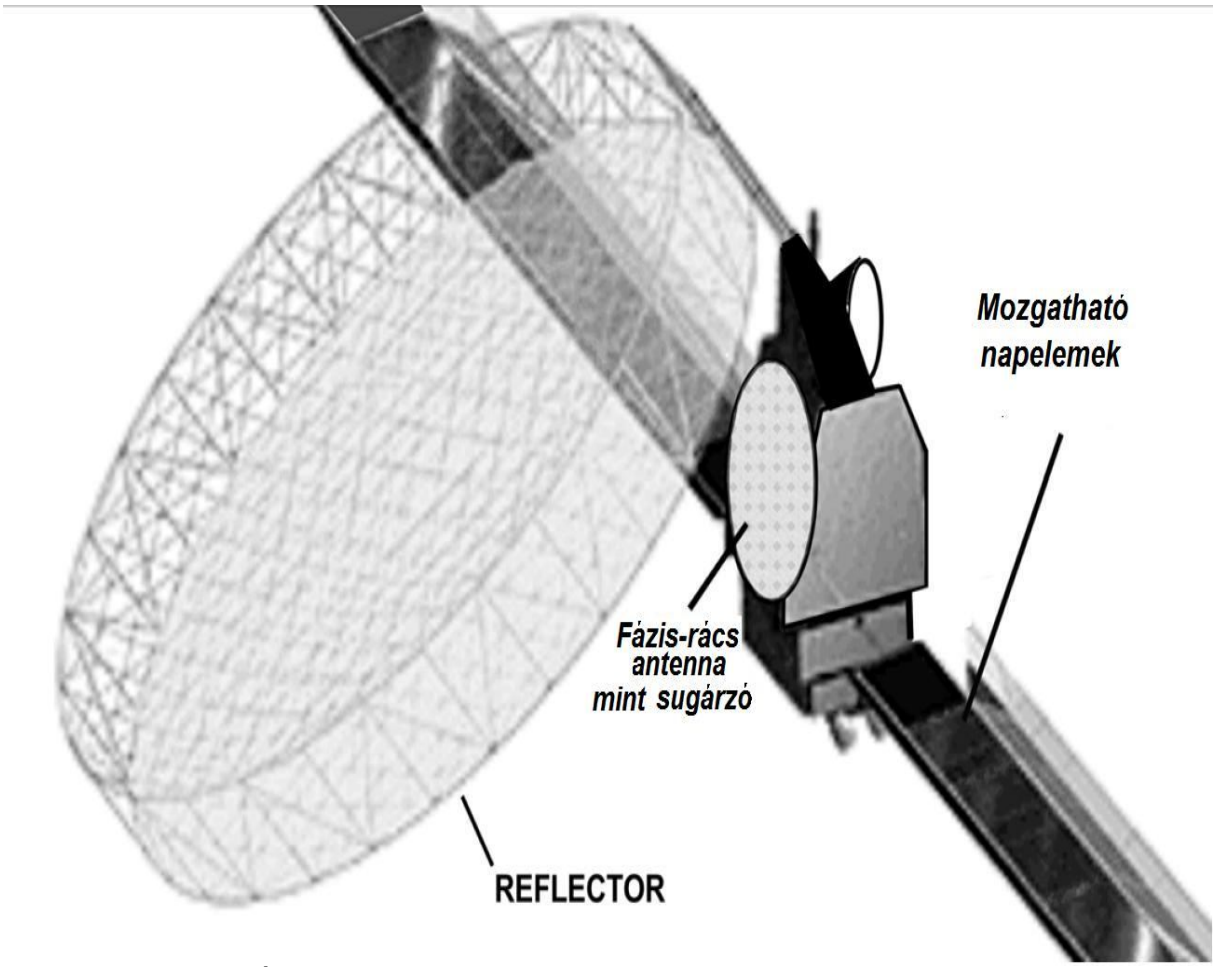
Világűrbe telepíthető radartervek

A következő nagy témablokk, amelyre a konferencia külön szekciót szentelt, a világűrbe telepített radarokkal kapcsolatos kutatások és eredmények áttekintése volt. Ez azért lehet érdekes a magyar olvasók számára, mert a Pécs-környéki radar telepítési helyének megválasztásával kapcsolatban sok téves vélemény látott napvilágot. Számomra az a vélemény, hogy a világűrbe telepített radarok ma már feleslegessé teszik a földi radarok telepítését teljesen érthetetlen és elfogadhatatlan. Egyszerűen belátható, hogy a világűrbe telepített, telepítendő radarokkal szemben másfajta műszaki elvárás fogalmazódik meg, melyek a telepítés körülményeiből következnek. Így például az, hogy a Földhöz legközelebb található műhold-radar pálya felszínhez viszonyított magassága kb. 100km. Ezen a magasságon a műhold (radar) a Földet 1-1,5 óra alatt kerüli meg, így Magyarország felett csak néhány percig tartózkodik.

A légi forgalom biztonsága megköveteli, hogy a hazánk légterében tartózkodó repülő eszközökről legkevesebb 12, de inkább 10 másodpercenként, újadat (információ) álljon rendelkezésre. Ha feltételezzük, hogy valaki megoldja a világűrbe telepítendő légtérellenőrző radar müszaki elvárásait (becslések szerint legalább 2 milliárd USD), meg kell oldania néhány száz műhold-radar pályára állítását, fenntartását, majd a vezérlésük és az adatkommunikáció biztosítását is.

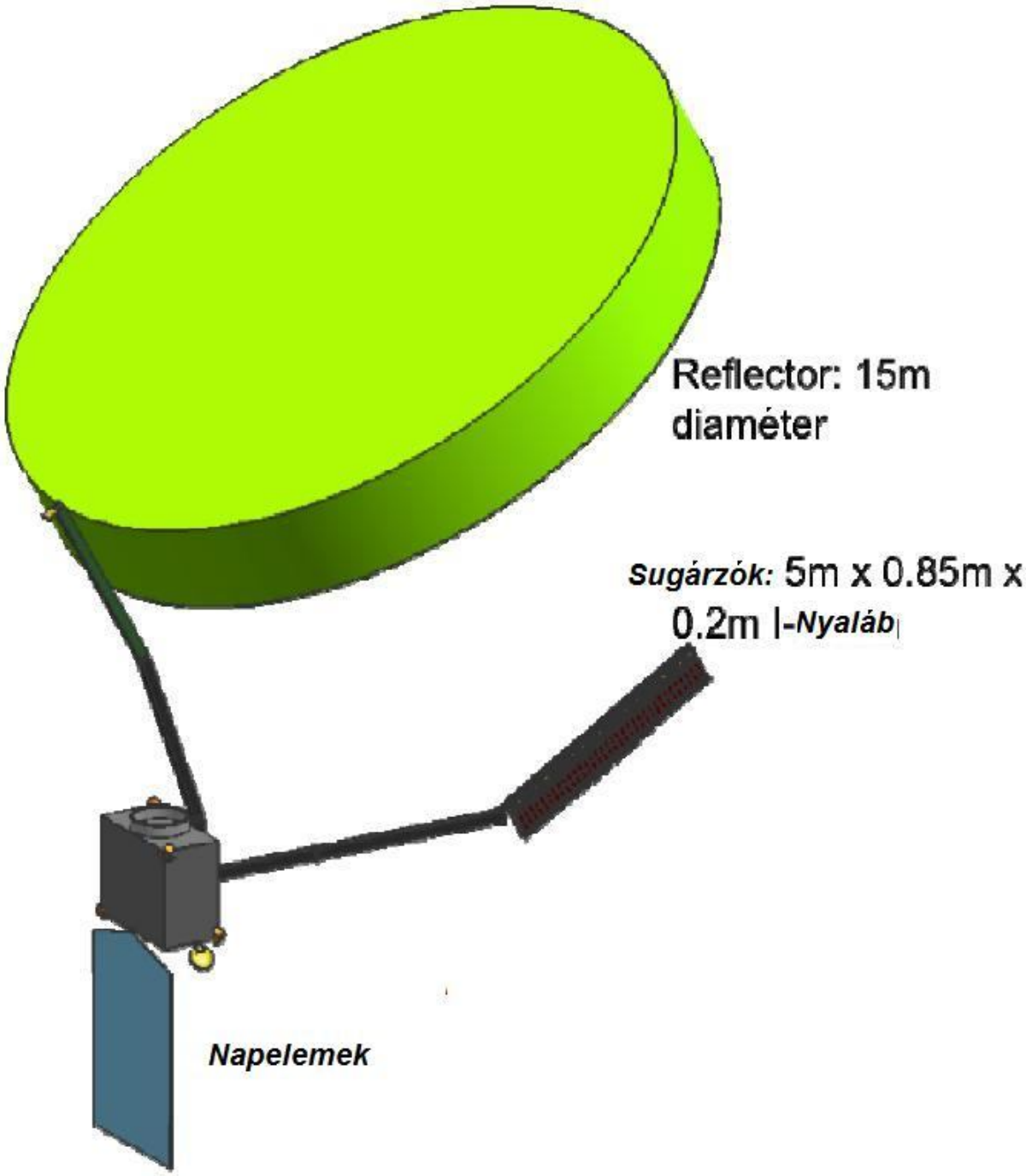
Ahhoz, hogy állandóan Magyarország fölött tartózkodjon egy műhold, 36000km magasságban a Föld felszíne fölött kell keringenie. Ebben az esetben a műholdak száma csak egy, de a Pécs környékére tervezett radar maximális, elméleti céltárgydetektálási távolsága kevesebb, mint 500km. Milyen nagy radart kell építenünk, ha 35 500km távolságra található a céldetektálás területe?

A probléma érzékelésére ismertetek néhány tényt D.Lynch cikkéből (Limitation of Scanning Arrays for Space). Az elképzelést a 6. sz.ábra szemlélteti.



6.sz. ábra. Új típusú nagy antenna felülettel rendelkező műhold-radar tervezet

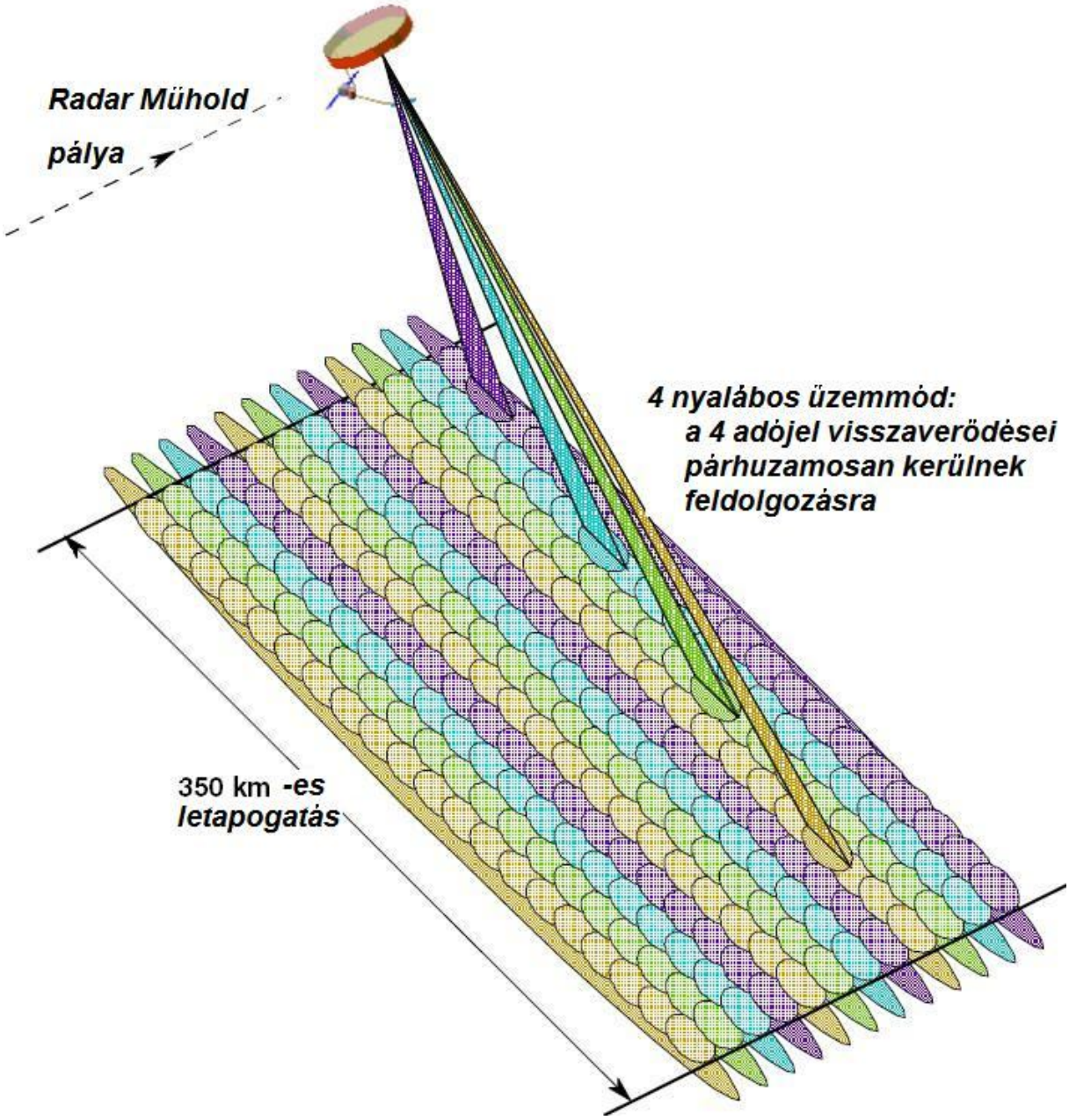
A műhold közepén található Fázis-rács antenna rendszer feladata megegyezik a földön települt hasonló radarantennáéval: a jel erősítése, a sugárnyaláb elektromos kialakítása, és mozgatása a tér elvárt irányába. Az elképzelt antenna kb. 100 000 adó-vevő egységet tartalmaz a hozzájuk tartozó fázistoló és késleltető tápvonalakkal. Így a megoldás nemcsak drágának de tömegénél fogva súlyosnak is ígérkezik, ami a pályára állítás miatt nagyon jelentős probléma. D. Lynch ezért azt javasolja, hogy a fázis-rács antenna egészüljön ki egy esetleg két, megfelelően elhelyezett reflektorral, melyek irányítottságukkal, és megfelelően nagy felületükkel jelentős többlet antenna-nyereséget, adnak. Az így kialakult hibrid radar jelentős tömegcsökkenést eredményez ahhoz a megoldáshoz képest, mely csak egy fázis-rács antenna alkalmazásával kívánja megoldani a feladatot. Ezzel a megoldással a mozgatható napelemek energiája hatékonyan kihasználható.
Hasonló, már a megvalósítás fázisában lévő Szintetikus Apertúrájú Antennával (SAR) rendelkező műhold radar leírását tartalmazza W.T.K. Johnson előadása (Radar Designs for the DESDynI Mission). Az általa említett. radar Földközeli a sarkokhoz igazított alacsony pályán, a Föld vegetációját, felszínének és a jég voltozásának mértékét tudja figyelni. A 7. sz ábra a radar főbb részegységeit és azok méreteit mutatja.



7. sz.ábra. Több frekvenciás nagy antenna nyereségű műhold-radar

Ezeket a SAR eszközöket, képalkotó radaroknak is nevezzük, mivel a koherens jelfeldolgozásnak köszönhetően a felbontóképességük olyan jó, hogy a vett jelekből fényképet tudnak előállítani. A sugárzókat lineáris elhelyezésű fázis antenna biztosítja, míg a reflektort egy 15m átmérőjű reflektor. Ez az új radar lehetővé tesz kb. 100 m-es felbontást a 340 km-es letapogatási sávban. A 8. sz ábra a SAR működését szemlélteti. Az ábrán jól látható, hogy a teljesítmény növelése érdekében, négy párhuzamosan üzemelő nyaláb biztosítja a Föld felszínének letapogatását a „D" (régi nevén"L") frekvencia sávban. (A Pécs környékére tervezett radar ugyanebben a „D" frekvenciasávban üzemelne.)

A SAR a Földkörüli pályáján 3-4 hetente képes lenne újra letapogatni a Földfelszín előzőleg letapogatott részeit. Szakemberek megállapítása szerint, a több éve tartó kutatás, fejlesztés eredményeként, az egyedülálló képességekkel rendelkező radar mégsem lesz majd alkalmas a légi forgalom megfigyelésére.



8.sz. ábra. 4 párhuzamos adatfeldolgozással rendelkező Szintetikus Apertúrájú Radar térletapogatási lehetősége

A csillagközi tér rádiólokációs figyelése

A konferencia utolsó napján lehetőségem volt ellátogatni a NASA legnagyobb radar, rádió navigáció és rádiókommunikáció központjába. (Goldstone Apple Valley Radio Telescope) Ebben a központban folyik a fellőtt űrhajók földi követése, és itt foglalkoznak a Naprendszer bolygóinak és a csillagközi tér rádiólokációs spektrumban való kutatásával is.
A 9. kép a többcélú radarkomplexum egy kis részletét mutatja. A többcélú jelző, a passzív rádiólokáció nyújtotta lehetőségek kihasználását jelenti, pl. a Nap vagy a Jupiter óriásbolygó rendszeres megfigyelését. Fantasztikus élményt nyújtott a mazerek, a folyékony hidrogénnel hűtött kis zajú erősítők, a különböző hullámsávok szétválasztására szolgáló mechanikus szűrők és a rendszerek vezérlésének bemutatott megoldásai.
Láthattuk azokat a radarokat, amelyek rádióteleszkóp üzemmódban interneten hozzáférhetőek az általános-, a középiskolások és az egyetemi hallgatók számára.
Az űrtechnológia a jelen és a jövő fő iparága, melyre már ma el kell kezdeni az elhívatott szakemberek előképzését, és ebben A NASA központban tett látogatásom megerősített. Az „Arany völgyben” található radar rendszerről további információ megtalálható az alábbi http://deepspace.jpl.nasa.gov internetes oldalon.



9. ábra. 34 m tányérátmérőjű rádióteleszkópok a kaliforniai Goldstone völgybe.

A konferencián sok, kiemelten színvonalas előadás hangzott el a legújabb kutatási eredményekről, de mindez jól szerkesztett könyv és CD formában is hozzáférhető az érdeklődök számára. Remélem, ezzel a cikkel is sikerült felkeltenem a témakör iránt érdeklődök figyelmét.

Irodalom

[1] Radar Conference 2009 Proceedings

[2] http://deepspace.jpl.nasa.gov

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Bleier Attila
attila.bleier@gmail.com

Rajnai Zoltán
rajnai.zoltan@zmne.hu

A STACIONER HÁLÓZATON HASZNÁLT TECHNOLÓGIÁK JAVASOLT KIALAKÍTÁSA

Absztrakt

Jelen tanulmányban a szerzők bemutatják javaslatukat a Magyar Honvédség fejlett Ethernet és IP hálózati eszközökre épülő stacioner hálózatának kiépítésére. A szerzők részletesen elemzik a jelenlegi hálózati paraméterek beállításait, amelyek ennek jobb felhasználását teszik lehetővé.

In this paper the authors provide a new proposed system design for the fixed network of the Hungarian Army, based on advanced Ethernet and IP networking gear. The authors describe the proposed parameter settings in detail that would make a better use and potential utilization of the current network.

Kulcsszavak: *hálózat, kommunikáció ~ network, communication*

Bevezetés

A Magyar Honvédség gerinchálózat kialakításakor, tervezésekor bizonyos általános irányelveket szükséges figyelembe vennünk, ilyenek például az Összhaderőnemi Doktrínában meghatározott irányelvek, mint azt már korábban (1) kifejtettük. Az irányelvek meghatározásakor szükséges a használt különböző belső és külső útválasztási protokollok beállításainak, a hibadetektálás és hibavédelem módjának, a hálózat által nyújtott szolgáltatásoknak és a szolgáltatásminőségnek, ill. a hálózat biztonsági beállításainak a meghatározása. A szolgáltatói IP/MPLS hálózatok által nyújtott szolgáltatásokról egy remek áttekintést ad a (2) cikk.

A hálózaton használt protokollok javasolt beállításai

Mind az IS-IS, mind az OSPF szóba jöhető belső útválasztó protokollok (IGP-k) a stacioner hálózatban. Mindkét protokoll állapot-út protokoll családba tartozik és hasonló jellegzetességekkel rendelkezik a stabilitás, skálázhatóság és Traffic Engineering és konvergencia terén.

A két protokoll hasonló annyiban, hogy:

- funkcióban és mechanizmusban nagyon hasonlóak
- állapotút algoritmusok (a hálózati ábra elosztott, mindenegyes router függetlenül számolja az utakat a elosztott hálózati ábra alapján)
- Kétszintű hierarchiával rendelkezik
- Designated routert választanak LAN-okon
- széleskörűen használtak
- több együttműködő implementációja van
- támogatják az authentikáció titkosítását

Főbb különbségek:

- Enkapszuláció
    - OSPF IP felett fut
    - ISIS- L2 felett fut
- területi terv
    - OSPF terület határok a routeren belülre esnek, tehát egy router több területhez is tartozhat
    - IS-IS terület határok élekre esnek, tehát egy router csak egy L1 területbe tartozhat (plusz még a L2 gerincre)
- A döntés, hogy az egyik protokollt a másik elé helyezzük, pusztán preferencia alapon történhet – amennyiben a Magyar Honvédség üzemeltető személyzete jobban ismeri valamelyik protokollt, akkor azt érdemesebb előnyben részesíteni. Traffic engineering esetén a ISIS némi előnyt biztosít (részletesebben lehet információkat kinyerni, és jobban támogatja a hosztnevek alkalmazását)

Tervezési javaslatok:

1. Függetlenül melyik protokollt választjuk kiindulópontnak, a gerinchálózatot célszerű egy egységes területnek tervezni
    a. OSPF egy gerinchálózat (area 0.0.0.0)
    b. IS-IS egy level-2 terület
2. Mindkét esetben a résztvevő interfészek a következők:
    a. Gerinchálózati belső linkek (PE-P, P-P)
    b. loopback interfészek
3. Traffic Engineeringet engedélyezzük OSPF-re, ill. ISIS-re (bizonyos router típusoknál ez az alapértelmezett)

4. Graceful Restart funkció engedélyezése (a router újraindulásakor az újraindulásról a szomszédokat értesíti)
5. Non-stop Forwarding (a folyamatos csomagtovábbítás biztonsítására, ha vezérlési síkbeli hiba van az útválasztókon)

A gerinchálózatban MP-BGP csomagokat célszerű átvinni, az NLRI információ továbbítására a különböző címosztályok között. A Magyar honvédség hálózatában ezt a következő esetben érdemes használni:

- Unicast IP-VPN kialakításakor (L3 IP VPN)
- Unicast IPv4 továbbítására (autonóm-rendszerhatárok között)
- L2VPN szolgáltatásra (BGP jelzésrendszerrel)
- VPLS szolgáltatásra

Az utóbbi két esetben LDP is használható a jelzéskialakításra (signaling). A BGP skálázhatóságának javítására, Route-Reflectorokat (RR) javaslunk. A teljes Magyar Honvédség hálózata egy privát (64512-65535) autónom rendszerbe esik. A belső csomópontok között IBGP, a külsők felé E-BGP használata javasolt, így az útvonalak kialakítása finomabb, és pontosabb szolgáltatási határ tesz lehetővé a harmadik rétegben. Konföderációk használata nem szükséges.
A hálózaton javasolt az MPLS kialakítása, amely a szolgáltatói hálózatban két főbb célt szolgál:

- VPN hálózati szolgáltatások kialakítását
- Traffic Engineering (TE) szolgáltatások kialakítását

Az MPLS technológia alapja az LSP (Label Switched Path – címkekapcsolt útvonal), amely két protokoll segítségével alakítható ki:

- Label Distribution Protocol (LDP)
- Resource Reservation Protocol with Traffic Engineering Extensions (RSVP-TE)

Az LDP működése automatikus, és minimális üzemeltetési beállítást igényel, azonban nem rendelkezik Traffic Engineering és Fast Reroute képességekkel, emiatt az RSVP-TE használata javasol. Helyes beállításokkal az RSVP-TE 10 miliszekundumos beállításra képes, a gyors konvergencia nagyon fontos nagy rendelkezésre állású hálózatok tervezésekor. A LSP jelzésrendszer tervezésekor kialakíthatunk hierarchiákat is,

1. LDP over RSVP (mind LDP+RSVP) egyaránt használt.
2. LSP hiearchiák : RSVP – TE, RSVP –TE-ben

Az LSP jelzésrendszer kialakításától függetlenül, különleges figyelmet szükséges folytatni a speciális esetekre – így a hangjelzésrendszerre és a hangforgalomra.

Hibadetektálás, hibavédelem

BFD használata ajánlott az Ethernet linkeken. “draft-katz-ward-bfd-00.txt”-ből idézve: a BFD rövid-időtartamú hibadetektálásra képes a szomszédos címtovábbító motorok között, beleértve az interfészeket, adatlinket és a csomagtovábbító motorokat is. A hardver platformtól függően, a hiba detektálása 10 ms-os nagyságrendben lehet. Néhány közeg (pl. Ethernet) nem biztosítja a gyors hibadetektálás lehetőségét, a BFD segítségével ez biztosítható, így a gyors hibadetektálás lehetséges a link-típusától függetlenül. PoS interfészek esetén (STM1-4-16-64) a BFD használata sok esetben szükségtelen, az SDH APS algoritmusa miatt.

A hibadetektálási idő mellett, a hibavédelem rendkívül fontos egy nagy rendelkezésre állású hálózat tervezésekor. A hibavédelemre alapvetően két megoldás létezik:

- végponttól –végpontig – útvonalvédelem
- pont-pont – helyi védelem

A legtöbb nagy rendelkezésre állású hálózatban mindkettő használt, és ezek használata a Magyar Honvédség hálózatában is javasolt. A hálózati telepítésekkor általános gyakorlat az elsődleges-tartalék megközelítés az útvonalvédelemre. Ebben a felépítésben két LSP-t használnak:

- elsődleges: normál üzemben használt
- másodlagos: csak hibaesetben használt, amikor az elsődleges LSP út már nem áll rendelkezésre

Azért, hogy a másodlagos útnak elegendő védelme legyen szükséges, hogy egy hiba ne befolyásolja az elsődleges és a másodlagos utat is. Ahhoz, hogy ezt elérjük az elsődlegesnek és a másodlagos LSP-nek két független úton kell keresztülmennie a hálózaton. A két különböző útvonal egyszerűen elérhető, ha az LSP-k egy IGP területen belül vannak, ebben az esetben használhatóak az IGP Traffic Engineering (TE) képességei.
A helyi védelem esetén csak a hiba lokális környezetében kerül a forgalom átirányításra. A végpont-végpont (útvonal) védelemhez képest (amely a teljes jelzés végigfuttatását igényli a végpontig), a helyi védelem gyorsabb hibajavítást tesz lehetővé.
A helyi védelmi mechanizmusok kétféle osztályba sorolhatóak

- Osztályozhatóak a védett erőforrások típusa szerint, amely lehet egy él vagy egy csomópont. Így a helyi védelem lehet élvédelem vagy csomópontvédelem. A védett erőforrástól függetlenül, a helyi védelmi mechanizmusokra együtt, mint helyi védelemre, vagy gyors útvonalváltás (FRR) hivatkozhatunk
- A védelmi út által védett LSP-k száma alapján is osztályozhatunk, így lehet 1:1, vagy N:1 védelem. Természetesen itt figyelembe kell venni a tartalékút skálázhatóságát, és hogy a forgalom hogyan továbbítható a védelmi úton

Hálózati szolgáltatások, szolgáltatásminőség biztosítása

Az edge telephelyekként jelölt telephelyeken az alábbi szolgáltatásokat kell, hogy egy MPLS PE útválasztó nyújtson:

- biztonságos hozzáférés Internet hálózati szolgáltató hálózatához - így a forgalom a lehető legrövidebb úton, megbízható és biztonságos szolgáltató hálózatán keresztül jusson el az Internetre
- MPLS L2, L3 IP VPN hálózati szolgáltatás, a belső hálózati forgalmak számára
- Hangszolgáltatás biztosítása, a hangforgalmak migrálása a hálózatra
- Dedikált útvonalak biztosítása a hálózaton, a különböző jellegű és célú adatoknak, ezen típusú adatok közti világos szeparáció létrehozása
- Meglévő egyéb szolgáltatások migrálásának a támogatása
- IPv6 képesség
- Mobil adatszolgáltatások támogatása

Az MPLS VPN nem pusztán forgalmi izolációt jelent, hanem arra is biztosít lehetőséget, hogy nem IP alapú második rétegbeli forgalmat is keresztül lehessen vinni a hálózaton. Mindenegyes VPN független, logikai hálózati szegmenst képvisel mind a vezérlési mind a továbbítási síkon. Ez forgalomvédelmet biztosít transzparens módon a hálózati rétegben, a gerinchálózatot használó ügyfeleknek.

Layer 2, Layer 3 VPN szolgáltatásokkal a hálózat egyes szolgáltatásait forgalmilag elválaszthatjuk egymástól. A Layer 2 alapú VPN arra biztosít lehetőséget, hogy a hálózat L2 szint felett transzparansen virtuális "kapcsolóként" viselkedjek. A L3 VPN arra biztosít lehetőséget, hogy a hálózatok L2 forgalmát az egyes telephelyeken leválaszthassuk. Ennek számos előnyei lehetnek, néhányat itt soroltam fel:

- szolgáltatásminőség biztosítása, az egyes hálózati szolgáltatások számára (így pl. egy nagyobb fontosságú szolgáltatás számára prioritást tudunk biztosítani)
- dedikált erőforrások biztosítása az egyes szolgáltatásokra
- forgalmi szeparáció így az egyes szolgáltatások biztonságosan, és szeparáltan futhatnak egy virtualizált hálózaton

A szolgáltatásminőség biztosítására legkevesebb 4 szolgáltatásosztályt javaslok (ezek megfelelnek a 3GPP Release 4 dokumentum által meghatározottaknak. Az alábbi táblázat ezt határozza meg:

	Delay	Buffering	Traffic Symmetry	Bitate
Conversational	▪ Minimum fixed	No	Symmetric	Guaranteed
Streaming	▪ Minimum variable	Allowed	Asymmetric	Guaranteed
Interactive	▪ No guarantees (moderate variable)	Allowed	Asymmetric	No guarantees
Background	▪ No guarantees (big variable)	Allowed	Asymmetric	No guarantees

A conversational és a streaming osztályok főként a valós-idejű forgalmi folyamokat határozzák meg (pl. hang, video, jelzés) míg az interaktive és a background osztályok főként az adat alapú alkalmazásoknak (FTP,Telnet,Email, WWW, etc…). A DiffServ architektúra használt a legtöbbször az erőforrások allokálására. A DiffServ kombinálható a Traffic Engineeringel, így a két technológia kiegészíti egymást (pl. a gerinchálózaton Traffic Engineering + Diffserv, a hozzáférési és aggregációs hálózaton Diffserv alapú QoS.

A gyakorlatban a Magyar Honvédség hálózatán az alábbi szolgáltatás osztályokat használata javasolt:

- VoIP jelzés - signaling - (H.323)
- VoIP hang - voice (RTP)
- Üzemeltetési és IT szolgáltatások – O&M and IT
- Internet

A táblázatban megjelöltük a szolgáltatásosztályokhoz tartozó DSCP osztályokat és az EXP biteket. A különböző MPLS technológiát javaslok az egyes szolgáltatásokhoz. A DSCP (Diffserv Code Point) az IP fejléc QoS célra fenntartott mezője, az EXP pedig az MPLS fejléc QoS célra fenntartott mezői. Így mind tiszta IP, mind IP/MPLS hálózaton meg tudjuk valósítani a QoS-t.

Forgalom típusa	DSCP	EXP	Használt MPLS technológia
VoIP jelzés (H.323)	AF41	4	VPLS
VoIP hang (RTP)	AF43	5	L3VPN
O&M és IT szolgáltatások – O&M	BE	0	L3VPN
Internet traffic	BE	0	L3VPN

A VPLS az MPLS szolgáltatás feletti virtuális privát LAN szolgáltatás. A szolgáltatás felhasználója szempontjából a hálózat egy LAN hálózatnak látszik. L3VPN az RFC 2547bis szabványban meghatározott 3-dik rétegbeli (MP-BGP) jelzésrendszert felhasználó virtuális magánhálózati szolgáltatás. Ezekben a cikkek (3), (4) az IP/MPLS gerinhálózatok ideális fejlesztését.
A hálózaton fontos, az egyenletes és stabil szolgáltatásminőség biztosítása, és ezek mérése. A szolgáltatásminőséget a KPI-k (Key Performance Indicatorok) határozzák meg – ezek az ún. szolgáltatátás minőségi jellemzők.Az alábbi táblázat a legfontosabb KPI-ket határozza meg a különböző szolgáltatás osztályokra, az itt használt táblázathoz a 3GPP forgalmi osztályait vettem alapul. Ezek alapján a hálózati elemeken létrehozhatóak a szolgáltatásminőség (Qos) profiljai, és tervezési dimenziói. Az egyes szolgáltatások a valósidejű (Conversational), jelzés (Signalling), streaming (nem valósidejű, de folyamatos szórással sugárzott) az interaktív (Interactive) – amely egy kvázi valósidejű, és a hátter (Background) – tehát best effort jellegű forgalom.
A használt KPI paraméterek a következőek:

- átlagos késleltetés (average delay) – miliszekundumban
- maximális késleltetés (maximum delay) – miliszekundumban
- a késleltetés változása (jitter)
- csomagvesztés (packet loss)
- átkapcsolási idő (failover time)

	Average Delay (msec)	Maximum Delay (msec)	Jitter (msec)	Packet Loss	Failover Time
Conversational	<20	<100	<5	$<10^{-4}$	2 sec
Signaling	<20	<100	/	$<10^{-4}$	/ (Relies on protocol failover)
Streaming	/	/	<100	$<10^{-3}$	5 sec
Interactive	<55	/	/	$<10^{-4}$	5 sec
Background	<108	/	/	$<10^{-3}$	/

Az egyes paraméterek folyamatos monitorozása szükséges, ezt az ún. SLA monitoring rendszereken keresztül biztosítható. Ezek a rendszerek a KPI paramétereket a hálózat folyamatos mérésével állapítják meg. A hálózati paraméterek értéke meg kell, hogy feleljen az SLA szerződésben meghatározott rendelkezésre állási és KPI paraméter értékeknek. Az SLA szerződés a hálózat üzemeltetője és a hálózat felhasználói között kell, hogy létrejöjjön.

A hálózat biztonságának biztosítása

A stacioner hálózat kialakításakor egy másik kiemelt kérdés a hálózat biztonságának biztosítása. Itt a elsősorban az informatikai biztonság kérdésével foglalkozom, a fizikai és egyéb biztonsági kérdésekre itt nem térek ki.

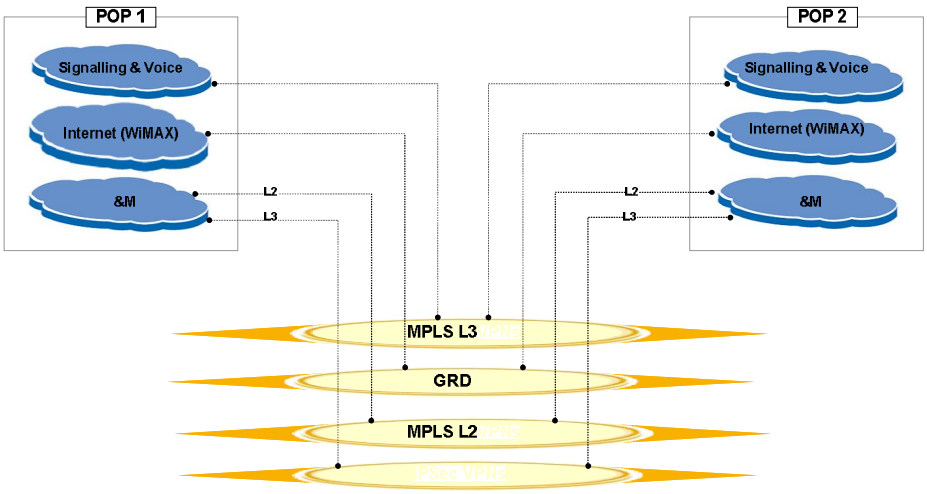
A hálózati biztonság a hálózati biztonsági zónák ("Security Domains") alapvető koncepciójára épülnek. Mindenegyes biztonsági terület összeségében különböző titkosítási szinten lévő forgalmat visz, tehát különböző típusú forgalomnak felel meg, amely különálló privát hálózatnak felel meg.
A privát hálózat a következő kettő típusok egyike lehet:

- fizikai privát hálózat, ahol mindenegyes forgalmi típus egy dedikált fizikai infrastruktúrát használ (tehát külön LAN switcheket routereket, átviteli utakat stb.)
- virtuális privát hálózat, ahol több forgalmi típus egy közös fizikai infrastruktúrán osztozik (ebben az esetben a szeparáció még mindig megvalósul az ún. erőforrás "virtualizáció" által)

Általában véve a különböző típusú privát hálózati forgalmak nem keverednek. De, bizonyos meghatározott pontokon átmehetnek egy biztonsági zónából egy másikba, de kizárólag meghatározott hálózati elemeken keresztül (eg. tűzfalakon keresztül) és csak meghatározott és szigorú szabályoknak megfelelően – amit a biztonsági szabályzat ír elő.
A hálózati virtualizáció egyre jobban meghatározó technológiává válik a hálózati iparágban.
Különböző technológiák használnak erre:

- virtuális LAN-okat (VLAN-ok)
- IP/MPLS VPN-ek – IP MPLS virtuális privát hálózatok , akár a második (L2VPN, L2circuit) akár a harmadik rétegben (L3VPN)
- IPSecurity (IPSec) – titkosítás használata az IP hálózati szinten

Általában véve, a VLAN-okat egy hálózati POP (Point of Presence)-on belül használnak, az MPLS-t pedig a gerinchálózaton. Az IPSec egy további titkosított biztonsági réteget képezhet, szuperszenzitív forgalmak számára, úgy mint O&M, számlázás, törvényes lehallgatás (LI). Ezek a technológiák nem zárják ki egymást , de általában nem ugyanazon a forgalmi típuson, vagy hálózati rétegben fordulnak elő. Az alábbi ábra a szolgáltatásosztályok VPN technológiával való szeparációját mutatja be. Ezek a VPN osztályok skálázhatóak, hogy olyan további forgalmi osztályokat tartalmazzanak, amelyeket a jövőben kívánnánk használni.



Az üzemeltetési célú (O&M) forgalom IPSec titkosítással ellátott lehet, az általános célú Internet forgalmat nem célszerű titkosítani, a hang és belső célú minősített forgalmak titkosítással ellátottak lehetnek.

Az alábbi technológiák használata javasolt a IP hálózat biztonságának növelésére:

- az irányított broadcast üzenetek szűrése
- távoli menedzsment hozzáférés meghatározása és naplózása, titkosított protokollokon keresztül
- SNMP Set üzenetek tiltása
- alapértelmezett az útválasztó felé menő ARP üzenetek korlátozása, ez leszűri az ún. ARP viharokat, amelyet a hibás beállítások vagy rosszindulatú cselekedetek indítják, az ARP üzenetek mennyiségét az Ethernet interfészeken tovább korlátozhatjuk
- A fenntartott hoszt és hálózati címek (ún. Marsi, vagy Martian címek), amelyről minden útválasztási információt figyelmen kívül kell hagyni
- DoS támadások a gyorsan változó forráscímeket használhatnak , amelyeket a támadók a lokalizálás és szűrés kivédésére használnak
- az ún. unikaszt RPF (Reverse Path Forwarding), úgy semlegesíti ezeket a támadásokat, hogy csak olyan csomagokat továbbít amelynek a forráscímei érvényesek és megfelelnek az útválasztó table által meghatározottaknak, az unikaszt RPF szolgáltatás, olyan problémák elhárításában segít, amely a hamisított forrás IP címeket nem engedi be a hálózatban azáltal, hogy csak az útválasztó table által ellenőrizhető forrás IP című IP csomagokat továbbítja, a többit eldobja
- az ICMP elárasztásos és hasonló támadások elleni védelem érdekében az útválasztó felé irányuló ICMP forgalommennyiség korlátozását javaslom
- A TCP SYN flood támadások elkerülése érdekében, amikor a támadó egy szkriptet vagy programot használva TCP nyitási (SYN) üzeneteket generál, olyan sebességgel amely gyorsabb mint az áldozat bontási ideje
- ezért javasolom, hogy a TCP SYN üzeneteket korlátozzuk
- A PE útválasztókon sávszélesség korlátok használatot javaslom
- Protokoll biztonságterületén az összes használt útválasztási protokollra (BGP, OSPF, IS-IS, RIP és RSVP) a HMAC-MD5-ös authentikáció beállítását javaslom
- Az útválasztóval a kommunikáció csak titkosítottan történhet:
    - ssh (secure shell), a router inband menedzsmentjére az SSH titkosított kommunikációt biztosít, egy nem megbízható hálózaton
    - SCP (secure copy), az SSH titkosítási mechanizmusán keresztül, titkosítottan másol fájlokat a hosztok között
    - Központi authentikációs szolgáltatást használva az útválasztókon, a hálózati belépés egyszerűsödik
        - ezt RADIUS, vagy TACACS+ protokollokon keresztül lehet megoldani
        - OTP (one time password) egyszeri használatú jelszavak használata
    - az útválasztó motorhoz bejövő forgalmak szűrése
        - a router erőforrások (CPU óraciklusok, és kommunikációs sorok) védelme érdekében csak a megbízható forrásból származó protokoll és vezérlési információkat engedélyezhetjük az útválasztó motor felé

Összegzés

A cikkben a Magyar Honvédség stacioner IP/MPLS gerinchálózatán javasolt beállításait mutattuk be. A cikkben szereplő technológiák a polgári életben már bizonyított nagy

rendelkezésre állású szolgáltatói környezet megfelelő adoptálása a Magyar Honvédség stacioner gerinchálózatára. Az adoptáció legnagyobb kihívása Munk Sándor szerint az infokommunikációs rendszerek között az interoperabilitás megteremtése (5), erre az IP/MPLS protokoll teremt lehetőséget.

Irodalomjegyzék

1. The challanges of the 21st century and the requirements of the Hungarian Army. Attila, Bleier. Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-11-1.
2. MPLS alapú IP hálózatok. Dr. Varga Balázs, Géczi Csaba. p. 37-63, MATÁV : MATÁV, 2001., PKI Közlemények 45.. kötet. HU-ISSN 1216-3961.
3. Ethernet alapú szolgáltatói hálózatok és szolgáltatások. Dr. Varga Balázs, Géczi Csaba. p. 137-165, Budapest : Matáv, 2003., PKI közlemények 47. . kötet. HU ISBN: 1216-3961.
4. Szolgáltatói IP gerinchálózat kiépítése Ethernet alapon. Attila, Hámori András - Tanács Ferenc - Balogh. p. 83-99, Budapest : Magyar Telekom Nyrt., 2005., PKI Közlemények 49.. kötet. HU-ISSN 1216-3961.
5. Interoperability infrastructure in military infocommunication systems. Sándor, Munk. Budapest : ZMNE, Communications 2005. ISBN 963 7060 11 1 .
6. The Multi-National Missions and the Network Enabled Capability. Károly, Fekete. Budapest : ZMNE, Communications 2005. ISBN 963 7060 11 1.
7. Unification of the Hungarian Governmental communications systems. Erik, Pándi. Budapest : ZMNE, Communications 2005. ISBN 963 7060 11 1.
8. Magyar Honvédség elvárásai és a XXI század kihívásai. Attila, Bleier. Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-57-1.
9. Az Észak-Atlanti Szervezetet kiszolgáló kommunikációs rendszerek jellemzői. Pándi Balázs, Pándi Erik. Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-57-1.
10. A jövő várható háborúinak és katonai konfliktusainak a hatása a hazai tábori kommunikációs rendszer megújításának folyamatára. Pándi Balázs, Pándi Erik. Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-11-1.
11. New possibilities of wireless trends in the area of mobile infocommunication and management. Erika, Magyarné Kucsera. p. 166- 174, Budapest : ZMNE, 2007., Communications 2007. kötet. ISBN 978-963-7060-31-1.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Deák Ferenc
deak@nct.hu

LÉTRADIAGRAM FORDÍTÓK ELMÉLETE PLC VEZÉRLÉSEK SZÁMÁRA III.

Absztrakt

A létradiagram egyszerű, programozási képzettséggel nem rendelkező szakemberek számára is érthető nyelv, ennek köszönhető, hogy az elmúlt 20-25 évben az egyik legnépszerűbb ipari programozási formává vált. Bár létradiagramos PLC (Programmable Logic Controller) rengeteg létezik a piacon, az ezeket feldolgozó fordítóprogramok irodalma meglehetősen szegényes. Az alábbi cikk az NCT új vezérléscsaládja számára kidolgozott PLC fordító elméleti hátterét mutatja be. Ez az algoritmus szakít az irodalom által ismertetett megközelítéssel, és gráfelméleti oldalról közelíti meg a kérdést, ami egy jól áttekinthető, szemléletes többlépcsős megoldást eredményez.

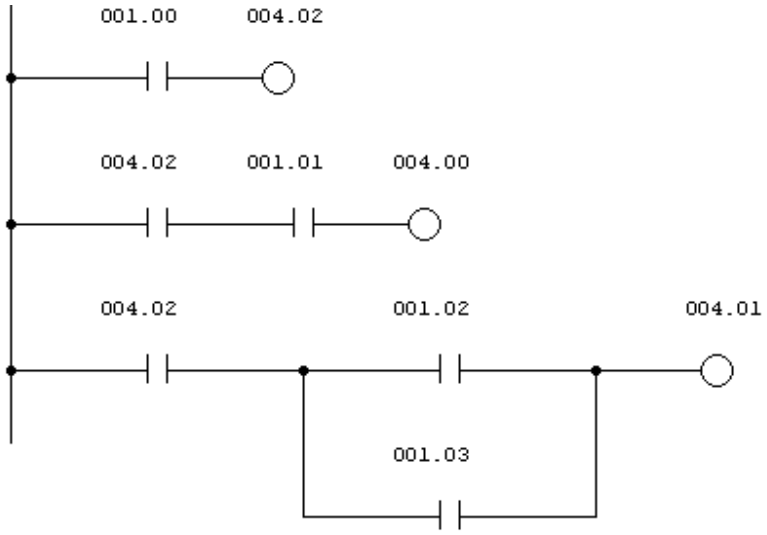
Relay ladder logic has become one of the most popular discrete control programming systems in the last 20-25 years. Programmable Logic Controllers (PLCs) usually can be programmed by wiring up relay contacts and coils on screen. This virtual circuit is transformed into a list of instructions in sequence. In this paper, the translation theory of relay ladder logic for new generation NCT controllers is examined. In contrast to solutions accessible in the literature this algorithm is multiphase, expressive and based on graph theory.

Kulcsszavak: *PLC, Létradiagramm, fordító ~ PLC, Programmable logic controllers, relay ladder logic, compiler*

BEVEZETÉS

Az előző két részben a fordítási algoritmust ismertetettük. Most két olyan esetről lesz szó, amivel az általános algoritmus megértését nem kívántuk elbonyolítani. Különösen fontos a számlálók esete, mivel a kereskedelemben kapható PLC-kkel ellentétben, ez az algoritmus lehetővé teszi, hogy számláló ne csak a létrafok jobboldalán állhasson, hanem bárhol, és kimenetét feltételként szabadon fel lehessen használni.

SPECIÁLIS ESETEK: IDEIGLENES RELÉK KIBONTÁSA



1.ábra. PLC program, melyben ideiglenes relé alkalmazása javasolt

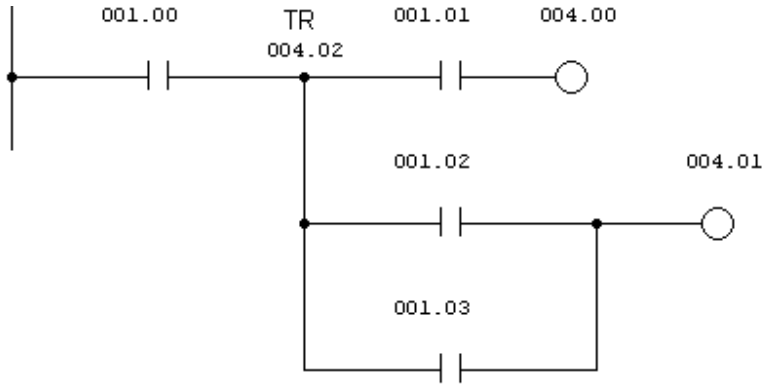
Ha az érintkezőket a diagramban vezetékdarabok felhasználásával sorosan illetve párhuzamosan kötjük, akkor köztük ÉS illetve vagy kapcsolatokat hozhatunk létre, így összetett logikai kifejezéseket valósíthatunk meg.

Ha valamilyen logikai kifejezés eredményét többször fel szeretnénk használni a PLC programban, akkor két dolgot tehetünk:

a) A logikai kifejezést annyi példányban megismételjük, ahányszor szükségünk van rá. Ez két problémát vet fel. Egyrészt, ha módosítani, akarjuk, akkor az összes előfordulását módosítani kell, aminek elmulasztása hibákhoz vezethet, másrészt a kifejezés értékét többször ki kell számítanunk. Másrészt a kifejezést minden előfordulásakor újra meg újra ki kell értékelnie a PLC-nek, ami nem gazdaságos
b) Létrehozunk egy ideiglenes relét. A diagramban (1.ábra) a többször felhasznált kifejezést a 001.00 érintkező szimbolizálja. (Az 1.ábra egy meglehetősen egyszerű esetet mutat be,

az ideiglenes relé alkalmazása természetesen csak akkor éri meg, ha a 001.00 érintkező helyén valamilyen bonyolultabb kifejezés áll.) Az ideiglenes relé a 004.02-es relé, amelyet igazi kimenetként nem használunk fel, egyetlen célja, hogy további kifejezésekben szerepeljen.

Az fenti ábrán (1.ábra) szereplő kapcsolást egyszerűbben is rajzolhatjuk, ezt mutatja a 2. ábra, ahol az ideiglenes relét egy vezetékdarabban rejtjük el, és TR jellel jelöljük.

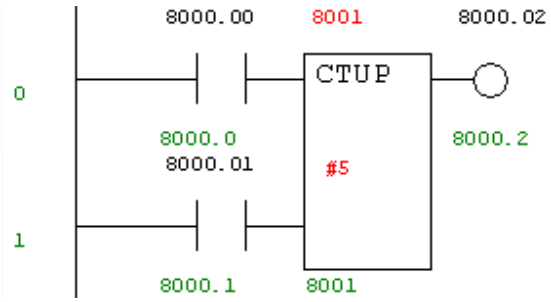


2. ábra. Ideiglenes relé alkalmazása

Az ideiglenes relé alkalmazása azonban a fordító algoritmus módosítását igényli. Az új algoritmus a következő:

1) Létrafokokra bontás.
2) Gráf reprezentációra alakítás
3) Ideiglenes relék kifejtése. Ennek során a 2. ábrának megfelelő gráfot átalakítja a PLC fordító az 1. ábrának megfelelő gráffá. (Erre a pontra egy példa a „Speciális esetek: számlálók" fejezetben található).
4) Mivel az előző lépésben egy létrafokból több keletkezik, ezért a létrafokokra bontást meg kell ismételni. A létrafokokra bontás megegyezik az első lépésben alkalmazott módszerrel, mely egy korábbi fejezetben került ismertetésre, azzal a különbséggel, hogy itt a létrafokokra bontás már a gráf reprezentáción történik.
5) A fordítás többi lépése megegyezik a korábban leírtakkal.

SPECIÁLIS ESETEK: SZÁMLÁLÓK



3. ábra. Számláló a létradiagramban

Az cikkben bemutatott számlálónak baloldalon egy léptető, és egy reset bemenete van. Kimenete a számláló típusától és állapotától függően aktív, vagy nem aktív. A kimenet opcionális, amennyiben nincs kimenete, akkor ezt a fordító pótolja egy a PLC program írója számára láthatatlan „nyelő”- vel.

A számlálók belső működése a fordítási algoritmus szempontjából érdektelen, viszont abban lényegesen eltérnek a többi létradiagram-elemtől, hogy a több helyen is szerepelnek a mátrixban (mivel több lábuk van a baloldalon). Ezt úgy lehet elérni, hogy a mátrixban nem maguk a létradiagram elemek szerepelnek, hanem csak referenciák melyek a létradiagram elemre mutatnak. Ezt a megoldást mutatja be a 1. és 2. táblázat.

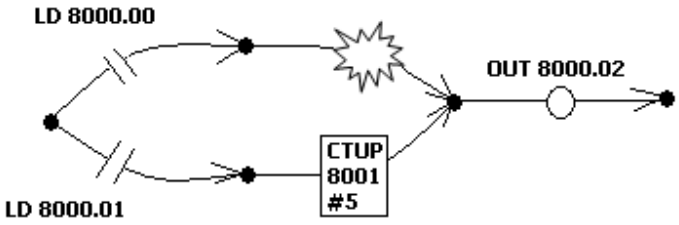
Azonosító	**Típus**	**Cím**	**Index**
1	Számláló	8001	#5
2	Érintkező	8000.00	-
3	Érintkező	8000.01	-
4	T-elágazás	-	-
5	T-elágazás	-	-
6	Tekercs	8000.02	-

1. táblázat. Létradiagram elemek felsorolása

4	2	1	6
5	3	1	-

2. táblázat. Létradiagram elemek a mátrixban

Az ebből fordított gráf alakot mutatja a 4. ábra.



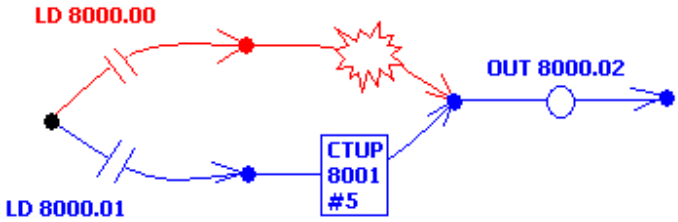
4. ábra. Számláló gráf alakja

A számláló első előfordulását egy speciális – itt „CSILLAG”-gal jelölt – élnek fordítjuk, a második előfordulás maga a számláló. A „CSILLAG”-nál a felső, a második előfordulásnál az alsó lábat vesszük figyelembe a baloldalon. A jobboldali láb mindkét esetben ugyanarra az OUT élhez csatlakozik.

A „CSILLAG”-ot az OUT-hoz és az ideiglenes relékhez hasonlóan ún. jobboldali elemnek tekintjük. A „CSILLAG”-ra és az OUT-ra alkalmazzuk a „Speciális esetek: ideiglenes relék kibontása” fejezetben leírt algoritmus 3. pontját a következőképpen:

1. Kezdetben minden elem színtelen.
2. Előbb a „CSILLAG”, majd az OUT mint jobboldali elemből kiindulva színezünk.
3. Választunk egy eddig még nem használt színt, és nyilakkal ellentétes irányban haladva beszínezzük a még nem színes éleket.

A lépés után a gráfot a 5. ábra mutatja.



5. ábra. A gráf a másodlagos létrafokokra bontás után

A különböző színű másodlagos létrafokokat egymástól függetlenül alakítjuk utasításlistává: a 1. mnemonic kód az első, az 2. mnemonic-kód a második létrefokot mutatja.

Egy összefésülési lépésben a CTUP –AND LD-ot CTUP-ra cseréljük, így az AND LD eltűnik. A két létrafokból keletkezett utasításlistát egymás után fűzzük, a „CSILLAG” parancsokat egyszerűen töröljük (3. mnemonic kód).

```
LD 8000.00
„CSILLAG”
```

Mnemonic kód 1: első létrafok

```
LD 8000.01
CTUP
8001
#5
AND LD
OUT 8000.02
```

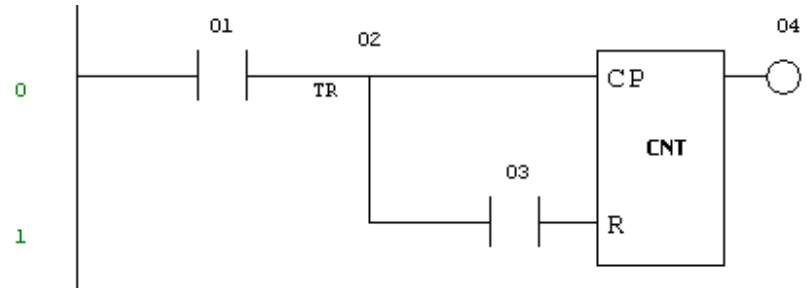
2. Mnemonic kód: második létrafok

```
LD 8000.00
LD 8000.01
CTUP
8001
#5
OUT 8000.02
```

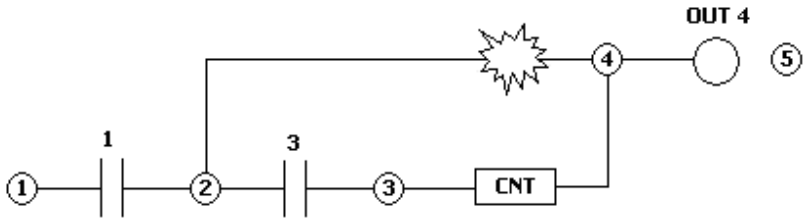
3. mnemonic kód: „CSILLAG”-ok törlése után

A CTUP utasítás a végrehajtás során két adatot vesz ki a veremből (léptetőjel és reset), és egyet tesz bele (az OUT számára).

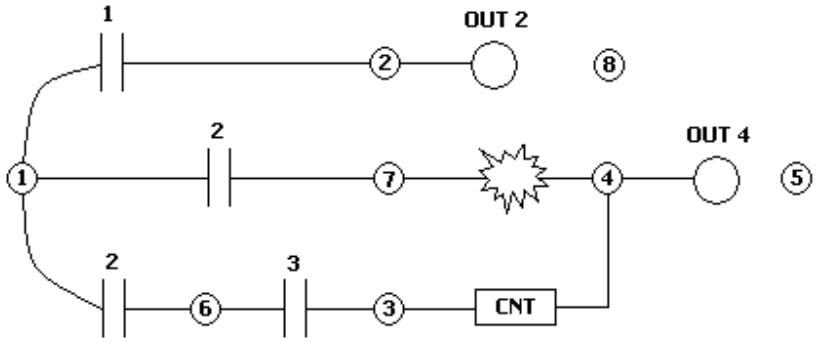
A fordító helyes működéséhez azonban módosítanunk kell a soros összevonás szabályait. A 6. ábrán látható létra feldolgozásának lépéseit a 7-9. ábra mutatja.



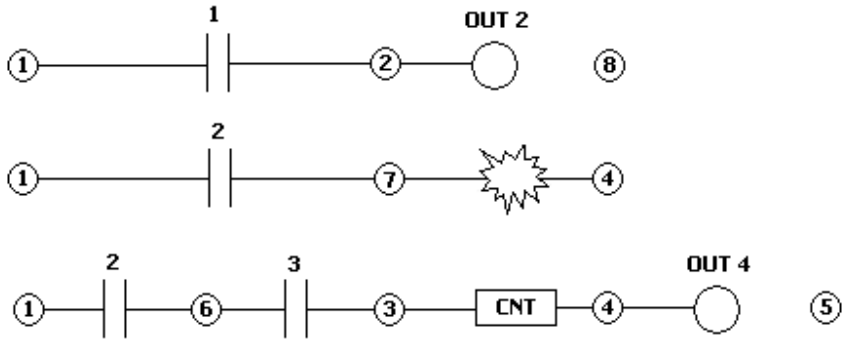
6. ábra. Példa a soros összevonás módosítására



7. ábra. Gráf alak



8. ábra. A TR-ek kibontása után



9. ábra. Másodlagos létrafokok

A harmadik létrafok esetében nem mindegy, hogy a soros összevonásokat milyen sorrendben hajtjuk végre. A 7.és 8. mnenomickód mutatja, hogy mi keletkezi, ha a 6-3 pontok közötti éllel kezdjük az átalakítást. A másik létrafokkal együtt a kész programot mutatja a 9. mnemonic-kód, ami hibás, mivel többet teszünk a verembe, mint amennyit kiveszünk. (Veremtartalom változásának összege nem zérus).

```
LD 2
LD 3
CNT
ANDLD
ANDLD
OUT 4
```

4. mnemonic-kód: AND LD kifésülése előtt

```
LD 2
LD 3
CNT
OUT 4
```

5. mnemonic kód: AND LD kifésülése után

A másik két létrafokkal együtt (a zárójel a veremtartalom változását jelzi):

```
LD 1        (+1)
OUT 2       (-1)
LD 2        (+1)
LD 2        (+1)
LD 3        (+1)
CNT         (-1)
OUT 4       (-1)
```

6. mnemonic kód: Az összes létrafok együtt

A 10-12. mnemonic kód mutatja a helyes megoldást: 1-6 éllel kell kezdenünk. A 1-3. pszeudó kód, és a 10-11. ábra mutatja a helyes algoritmust.

```
LD 2
LD 3
AND LD
CNT
ANDLD
OUT 4
```

7. Mnemonic kód: Eredmény, ha az 1-6 éllel kezdünk

```
LD 2
AND 3
CNT
OUT 4
```

8. Mnemonic kód: az összevonások után

```
LD 1        (+1)
OUT 2       (-1)
LD 2        (+1)
LD 2        (+1)
AND 3       (0)
CNT         (-1)
OUT 4       (-1)
```

9. Mnemonic kód: A többi létrafokkal együtt

```
Amíg van változás
{
        Felesleges „CSILLAG”-ok törlése
        Soros-párhuzamos összevonások
        „CSILLAG” és számláló összevonások
}
```

1. pszeudó kód: Összevonások algoritmusa

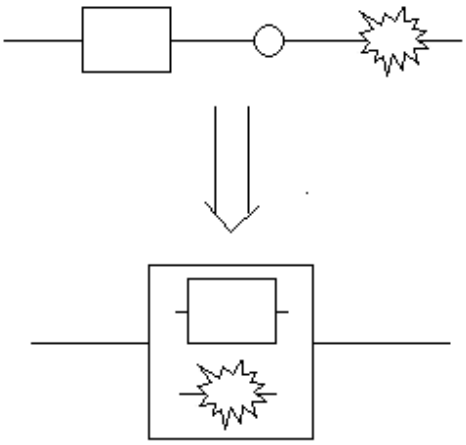
```
Amíg van változás
{
        Minden élre
        {
                Megvizsgáljuk, hogy össze lehet-e vonni másik éllel.

                Ha igen
                        Akkor soros-párhuzamos összevonást végzünk
        }
}
```

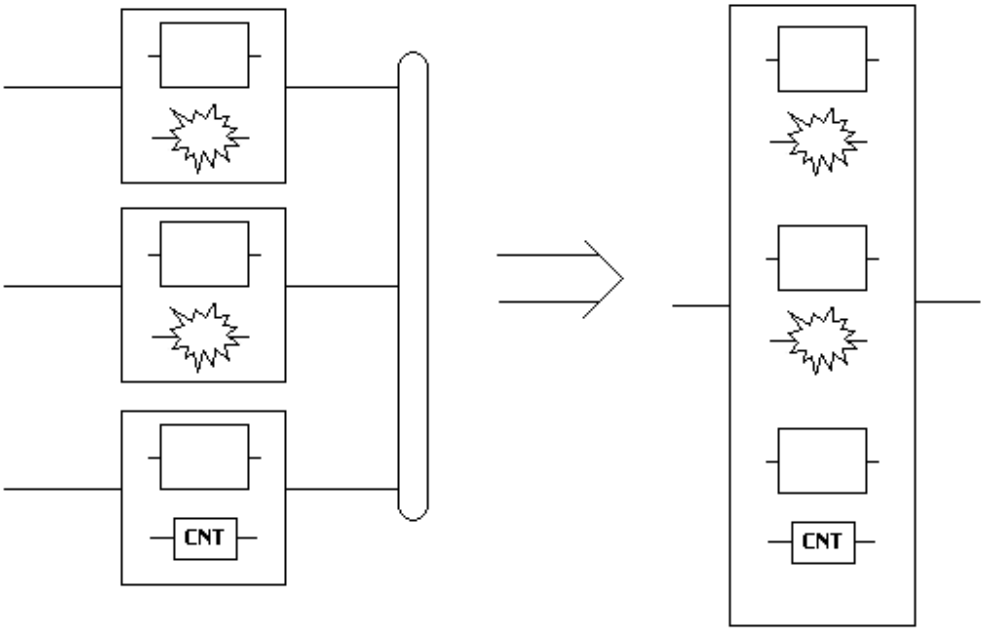
2. pszeudó kód: Soros-párhuzamos összevonás algoritmusa

```
Minden élre
{
        Számláló vagy „CSILLAG” összevonást végzünk
}
```

3. pszeudó kód: „CSILLAG” és számláló összevonások algoritmusa



10. ábra. A csillag összevonás



11. ábra. A számláló összevonás

IPARI ALKALMAZÁSOK

Az új PLC első alkalmazása rendhagyó módon egy kovácsoló gyártósor irányítása volt. A PLC önállóan – NC modul nélkül – üzemel, és egy hidraulikus prést, egy körasztalt, egy indukciós kemencét és önálló robotvezérlőkön keresztül három ipari robot munkáját irányítja. Azóta egy fogazógép, egy dörzshegesztőgép és egy karusszel eszterga felújítását is ezzel a vezérléssel oldottuk meg, és várhatóan 2010 tavaszától már a sériagyártás is megkezdődik.

TOVÁBBI FEJLESZTÉSEK

A szöveges PLC nyelvek vitathatatlan előnye, hogy a PLC programok szerkesztése a jól kidolgozott általános célú szerkesztőkkel megoldható. A szöveges kód – bár nehezebben érthető – de nagyon rugalmas. Ezt a létradiagram esetében felhasználóbarát szerkesztő kidolgozásával ellensúlyozható. A PLC szerkesztőnek együtt kell működnie a villamos tervezőrendszerekkel is. A hatékonyságjavítás fontos területe, az egyre összetettebb PLC utasítások beépítése, mellyel a PLC program tömörebbé, a PLC program megírása lényegesen gyorsabbá tehető.

Bár az első őspéldányok elkészítése óta az NCT létradiagram szerkesztője sokat fejlődött, mégis célszerű a szerkesztőt erőteljesen fejleszteni, mivel minden munkaóra, amit PLC programozók munkáját gyorsító megoldások kidolgozásával töltünk, többszörösen megtérül.

FELHASZNÁLT IRODALOM

[1] IEC 61131-3 Programmable controllers - Part 3: Programming languages International Standard, International Electrotechnical Commission, 2003

[2] John T. Welch: Translating unrestricted relay ladder logic into Boolean form. Computers in Industry, 20 (1992) 45-61

[3] NCT szerszámgép vezérlések PLC programozási leírása
http://www.nct.hu/pdf/NC_Documents/Magyar/Telepites/magplc.pdf

[4] H. A. Barker, J. Song, P. Townsend: A rule based procedure for generating programmable logic controller code from graphical input in the form of ladder diagrams, Eng. Appli. of AI, 1989, Vol. 2, December

[5] R. Wareham, Ladder diagram and sequential function chart languages in programmable controllers, Can. Mach. Metalwork., December 1988, pp. 25-26.

[6] R. Devanathan, Computer aided design of relay ladder diagram from functional specification" Int. Conf. on Industrial Electronics, Control and Instrumentation – IECON, 1990, pp. 527-531.

[7] D. Harel, Statecharts: a visual formalism for complex systems, Sci. Comput. Programming Vol. 8, 1987, pp. 231-274.

[8] M. Courvoisier, R. Valette, J. Bigou and P. Esteban, A programmable controller based on a high level specification tool, IECON 1983, pp. 174-179.

[9] T. Murata, N. Komoda, K. Matsumaoto and K. Haruna, A Petri-net based controller for flexible and maintainable sequence control and its applications in factory automation, IEEE Trans. Ind. Electron, Vol. IE-33, No. 1, February 1986, pp. 1-8.

[10] IEC PAS 62407 Real-time Ethernet control automation technology (ETHERCATTM), International Electrotechnical Commission, 2005

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Fleiner Rita
fleiner.rita@nik.uni-obuda.hu

AZ ADATBÁZIS-BIZTONSÁG ALAPJAI

Absztrakt

A publikáció az adatbázis-biztonság fogalmának, helyének és szerepének vizsgálatával foglalkozik. A szerző bemutatja az adatbázis-biztonság eddigi értelmezéseit és a fogalomban idők során bekövetkezett változásokat, fejlődéseket; feltárja az informatikai biztonság és az adatbázis-biztonság kapcsolatrendszerét; illetve elemzi az adatbázis-biztonság helyét, szerepét és jelentőségét az informatikai biztonságon belül. Végül pedig ismertetésre kerül a szerző által javasolt adatbázis-biztonság fogalom értelmezése.

The publication studies the concept, the place and the role of database security. The author describes the different interpretations of database security up to the present, the changes and the evolution of the concept during the times. Furthermore the relationship between information security and database security is revealed and the place, the role and the importance of database security within information security is analysed. At the end the model of database security is presented by the author.

***Kulcsszavak**: adatbázis-biztonság, informatikai biztonság, adatbiztonság, adatbázis-biztonság tulajdonságai ~ database security, information security, data security, database-security goals*

BEVEZETÉS

Az utóbbi években egyre több olyan eset került nyilvánosságra, melyben bizalmas információk, ügyféladatok szivárogtak ki adatlopás, hacker támadás vagy hűtlen kezelés miatt. Egy-egy ilyen incidens az érintett szervezet számára számtalan káros hatással jár együtt, jelentősen ronthatja annak hírnevét, a kártérítési kötelezettség extra költségeket vonhat maga után, a meghamisított adatok és rendszerek visszaállítása időveszteséggel és többletmunkával párosul, továbbá meg kell említeni, hogy sok esetben még jogi pereskedések, bírósági eljárások is

az esetek következményeiként léphetnek fel. Mára az adatok védelmének kérdése a vállaltok és szervezetek általánosan elfogadott feladata lett.

Napjainkban a felgyülemlett óriási adatmennyiséget - egyre szélesebb körben - adatbázisokba szervezve tárolják. Az adatbázis adatoknak számítógépekben tárolt, valamely adatmodell szerint strukturált gyűjteménye. Az adatbázisokban tárolt adatok kezelését speciális alkalmazások, az úgynevezett adatbázis-kezelő rendszerek biztosítják. Az informatikai rendszerek jelentős részének működésében az adatbázis-kezelő rendszerek és az általuk tárolt adatok lényeges, esetenként kiemelt szerepet játszanak. Az adatbázisok biztonságának megsértése (működésképtelenné tétele, meghamisítása, a tárolt adatok jogtalan megismerése) az adott informatikai rendszer és az általa nyújtott szolgáltatás biztonságát fenyegeti. Ebből következően lényeges kérdés az adatbázis-biztonság megvalósítása, szabályozása és támogatása.

Jelen publikáció alapvető célja az adatbázis-biztonság fogalmának, helyének és szerepének vizsgálata. Ezen belül a publikáció:

- bemutatja az adatbázis-biztonság eddigi értelmezéseit és a fogalomban idők során bekövetkezett változásokat, fejlődéseket;
- feltárja az informatikai biztonság és az adatbázis-biztonság kapcsolatrendszerét;
- elemzi az adatbázis-biztonság helyét, szerepét, jelentőségét az informatikai biztonságon belül;
- ismerteti a szerző által alkalmazott adatbázis-biztonság fogalom értelmezését.

ADATBÁZIS-BIZTONSÁG ÉRTELMEZÉSÉNEK ALAKULÁSA

Az adatbázisok története szorosan összefügg az adatmodellek és az adatbázis-kezelő rendszerek történetével. Az adatbázis rendszerek folyamatos fejlődése hatással van az adatbázis-biztonsághoz tartozó fogalmak értelmezésére. Edgar F. Codd 1969-ben, az IBM munkatársaként kidolgozta a mai napig is legnépszerűbb és legelterjedtebb adatbázis típus logikai modelljét, a relációs adatmodellt. Ez az első adatmodell, amelyben már élesen szétválik a logikai és a fizikai adatbázis. Az adatbázisok magas szintű tervezésének fejlődésében egy másik jelentős időpont 1976, amikor is Peter Chen ismertette az egyed-kapcsolat adatmodellt, mely szoros kapcsolatban áll a relációs modellel és a gyakorlatban ma is elterjedt módszere az adatbázisok magas szintű tervezésének.

Az adatbázis-kezelő rendszerek jelenlegi, korszerű formái csak az 1960-as évek közepén kezdtek el kialakulni, azóta viszont folyamatosan fejlődnek. Az IBM-nél az 1970-es évek közepén Codd relációs modelljéhez kötődően kifejlesztették a System-R - ma DB2 - nevű adatbázis-kezelő szoftvert. Közben a CIA-nél is elindult egy Orákulum – angolul Oracle – nevű projekt, melynek célja egy olyan adattár létrehozása volt, amely a CIA minden felmerülő kérdését gyorsan, hatékonyan, és aránylag olcsón meg tudja válaszolni. A projekt egy idő után a CIA-nél véget ért, de a munka az 1977-ben alapított Relational Software Inc. (RSI, 1982-től Oracle Corp.) keretein belül folytatódott. 1978-ban elkészült az Oracle nevű adatbázis-kezelő rendszer első verziója, melynek lekérdező nyelve már az SQL elődjére, a SEQUEL-re alapult. 1986-ban az SQL, mint a relációs adatbázisok lekérdezőnyelve az Egyesült Államokban is, és Európában is szabványossá vált.

Napjainkban adatbázis-kezelő rendszer alatt több felhasználós, hálózatos környezetben működő, az adatbázisokhoz való hozzáférést, a felhasználói folyamatok zavartalan működését biztosító szoftveralkalmazást értünk. Adatbázisnak nevezzük valamely adatmodell szerint tá-

rolt adatok halmazát, melyet az adatbázis-kezelő rendszer kezel. Az adatbázisokban koncentráltan található adatok biztonsága és védelme a kezdetektől fogva fontos feladat volt, azonban az adatbázisok elérési módjainak kiszélesedésével és a felhasználói kör kibővülésével új problémák, kihívások jelentek meg. Ezek a folyamatok hatással voltak az adatbázis-biztonság és védelem fogalmainak megváltozására is.

Adatbázis-biztonsággal kapcsolatos fogalmak az angol nyelv esetében több kifejezés formájában is előfordulnak. Ezek közé tartoznak a 'database security', 'database assurance', melyeket adatbázis-biztonságnak fordítunk, illetve a 'database protection', magyarul adatbázis védelem.

Az adatbázis-biztonság vizsgálata kapcsán hangsúlyozni kell, az általunk vizsgált témakör eltér az adatvédelem fogalmától. Az adatvédelem a személyes adatok védelmével, biztonságával kapcsolatos fogalom, mellyel az Adatvédelmi törvény [1] foglalkozik részletesen. Eszerint az adatvédelem a személyes adatok gyűjtésének, feldolgozásának és felhasználásának korlátozása, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége. Az informatikai szaknyelv is elfogadta azt, hogy az adatvédelem az Adatvédelmi törvény által meghatározott adatok csoportjára vonatkozik.

Adatbázis-biztonság értelmezésekor nem szorítkozunk az adatok csak egy bizonyos csoportjára, hanem az informatikai rendszerekben, azon belül adatbázis rendszerekben tárolt adatok egészének védelme, biztonsága képezi a vizsgálatunk tárgyát. A következőkben áttekintjük több forrást megvizsgálva az adatbázis-biztonság fogalmának értelmezéseit.

Először megvizsgálunk néhány több kiadást megélt, felsőoktatásban is használt adatbázis témájú szakkönyvet. C.J.Date: An Introduction to Database Systems című könyvében [2] 27 fejezet közül egyet a biztonság témájának szentel, ahol az adatbiztonság fogalmát tisztázza elsőként. Véleménye szerint a biztonság az adatok védelmét jelenti a jogosulatlan felhasználók elől. Az adatbázis-kezelő rendszer rendelkezik biztonsági alrendszerrel, mely a hozzáférési kéréseket mindig egyezteti a rendszer katalógusában található biztonsági megszorításokkal, ezáltal biztosítva a biztonságos működést. Adatbázis-biztonság témakörébe tartozó problémákat, feladatokat vet fel és elemez, melyek közé az adatokhoz való hozzáférés szabályozása (access controll), azaz adatbázis felhasználók jogosultságainak beállítása, statisztikai adatbázisok biztonsági problémái (azaz megengedett lekérdezésekkel nem megengedett információkhoz megszerzésének kérdésköre), adatok titkosítása és nézetek definiálása tartoznak.

Elmasri, Navathe: Fundamentals of Database Systems című könyv [3] adatbázis-biztonság címet viselő fejezete azokat a technikákat tekinti át, melyek a különböző fenyegetések ellen védik az adatbázisokat. A fenyegetések az adatok integritásának, rendelkezésre állásának és megbízhatóságának sérülését eredményezhetik. C.J.Date könyvében tárgyalt témák mellett a szerzők az adatbázis-kezelő rendszerek működésének biztonságát is felvetik. A támadás célpontja lehet az adatvagyon vagy pedig az azt kezelő informatikai rendszer. Az adatbázis-kezelő rendszer feladatának tekinti a támadás megelőzésének illetve felfedésének feladatán túl a támadó elszigetelését, a sérülés kiértékelését, a rendszer újra konfigurálását, az adatok és a rendszer funkciók sérülésének kijavítását és a hiba jövőbeni kiküszöbölését.

Az adatbázis-biztonság felsőfokú oktatásban való megjelenésének lehetőségeit tárgyaló cikkekben megtalálhatjuk azokat a témaköröket, melyeket a szerzők a témába illőnek találnak. Ezek közé tartoznak például az adatbázisok konzisztenciáját biztosító megszorítások (például az elsődleges és idegen kulcs megszorítások), a sor szintű biztonság, az adatokhoz való hoz-

záférés szabályozásának lehetőségei, a hitelesítés, a többszintű biztonság, a közvetett következtetés (inference), az adatbázisban tárolt adatok titkosítása és az adatbázis audit [4]. Adatbázis-biztonság oktatási tematikában egyre inkább teret nyer az adatbázis-kezelő rendszerek megfelelő karbantartása, a szoftver aktuális frissítéseinek telepítése. Hangsúlyossá válik a tradicionális adatbázis-biztonsági témák mellett–amik magának az adatbázisnak a biztosításáról szólnak - új területek tárgyalásának igénye, melyet a webes és hálózatos elérések számának növekedése, a bonyolult és heterogén kliens-szerver architektúrák kialakulása és az alkalmazás szerverek elterjedése váltott ki. Az új területek közé tartoznak a következők: operációs rendszer és adatbázis-kezelő rendszer biztosítása, alkalmazás biztosítása és sql injekció, többszintű biztonság, adattárházak, adatbányászat, statisztikai biztonság és adatbázis-biztonsági politikák készítése. [5], [6]

Az adatbázis-biztonság fogalmát az indiai CERT szervezet a következőképpen határozza meg [7]: Adatbázis-biztonságnak nevezzük azokat a rendszereket, folyamatokat és eljárásokat, melyek megvédik az adatbázist az előre nem tervezett tevékenységektől. A nem tervezett tevékenységek körébe soroljuk a jogosultságokkal rendelkező felhasználók visszaéléseit, a rosszindulatú támadásokat, vagy nem szándékos hibákat, melyeket jogosultságokkal rendelkező felhasználók vagy folyamatok követnek el. Az adatbázis-biztonság része egy tágabb szakterületnek, az informatikai biztonságnak.

Az adatbázis-biztonság tárgykörének vizsgálata kapcsán érdemes megvizsgálni az USA Védelmi Minisztériuma által kiadott Adatbázis-biztonság Technikai Megvalósítási Útmutató [8] tartalmát. Az adatbázisban tárolt adatok védelmét az adatbázis-kezelő rendszer által nyújtott védelmi lehetőségeken keresztül vizsgálja meg, tehát ebben a szemléletben az adatok biztonsága és az azokat kezelő informatikai rendszer biztonsága egymástól elválaszthatatlan fogalomként jelenik meg.

A bemutatott értelmezések alapján is látható, hogy az adatbázis-biztonság értelmezése az idők folyamán megváltozott, kibővült. A szűkebb típusú értelmezés szerint az adatbázis-biztonságot a tárolt adatok biztonsága jelenti, ezen belül az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, ez a hozzáállás az adatbázis-kezelő rendszerekről nem tesz említést. Ez a szemléletmód az adatbázis-kezelő rendszerek első megjelenésétől kezdve megfigyelhető. A rendszerek fejlődésével és elterjedésével egy tágabb típusú értelmezés is megjelent, mely a tárolt adatokat és az ezeket kezelő adatbázis-kezelő rendszert tekinti a biztonság védendő objektumának. Az adatbázis-biztonságnak ezt a megközelítését találhatjuk meg az előzőleg hivatkozott USA Védelmi Minisztériuma hozzáállásában.

Az adatbázis-biztonság alanyának meghatározása mellett szólni kell a védendő tulajdonságok halmazáról is, amik természetesen konkrét alkalmazások és környezetek esetén eltérőek lehetnek. A biztonsági tulajdonságok elemzését az informatikai biztonság területén megtalálható tulajdonságok vizsgálatán keresztül érhetjük el, majd értelmezhetjük adatbázis-biztonságra vonatkozóan. A biztonság védendő tulajdonságai között három alapkategóriát mindig megtalálunk a magyar és a nemzetközi szakirodalom egyaránt, ezek a következők: bizalmasság (confidentiality), sértetlenség (integrity), rendelkezésre állás (availability). Ezek mellett még egyéb tulajdonságok is léteznek, mint például a letagadhatatlanság (non-repudation), hitelesség (authenticity), elszámoltathatóság vagy követhetőség (accountability vagy auditability), megbízhatóság (reliability) és garancia (assurance). A Közigazgatási Informatikai Bizottság által készített Magyar Informatikai Biztonsági Ajánlásokban [9] a következő meghatározásokat találjuk.

- Bizalmasság: Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.

- Sértetlenség: Az adat tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

- Rendelkezésre állás: Az informatikai rendszerelem – ide értve az adatot is – tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem a szükséges időben és időtartamra használható.

Látható, hogy ezen értelmezés a sértetlenség jelentésébe beleolvasztja a letagadhatatlanság és hitelesség tulajdonságokat anélkül, hogy megnevezné őket. Egy másik szintén kormányzati dokumentumban [10] olvashatjuk a következőket: „A sértetlenség fogalmába –jelen dokumentum megközelítése szerint– beleértendő az információk letagadhatatlansága és hitelessége is." Ezen tulajdonságok értelmezése a dokumentum szerint a következő

- Letagadhatatlanság: Olyan biztonsági tulajdonság, amely megfelelő bizonyítékokkal szolgál az informatikai rendszerben végrehajtott tevékenységek későbbi ellenőrizhetőségét illetően.
- Hitelesség: A hitelesség az entitás olyan biztonsági tulajdonsága, amely egy vagy több hozzá kapcsolódó tulajdonságot más entitás számára bizonyíthatóvá tesz.

Az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Kormány rendeletben [11] a sértetlenséget szintén kibővített tartalommal definiálják a következő módon: biztosítandó, hogy a rendszerben kezelt adat tartalma és tulajdonságai az elvárttal megegyezzenek - ideértve a bizonyosságot abban, hogy az elvárt forrásból származik és a származás megtörténtének bizonyosságát is -, továbbá a rendszerelemek a rendeltetésüknek megfelelően használhatóak legyenek.

Az ISO/IEC 27001:2005-ös szabvány [12] elsődlegesen a bizalmasság, sértetlenség és rendelkezésre állás tulajdonságait emeli ki, de szól arról, hogy egyéb jellemzők is fontosak lehetnek, mint például a már említett letagadhatatlanság és hitelesség, emellett viszont szól még az elszámoltathatóság és megbízhatóság tulajdonságokról is. Az elszámoltathatóság az entitások (például felhasználók) tevékenységeinek nyomon követhetőségét jelenti az adott entitás felelősségének megállapíthatósága érdekében. A megbízhatóság több mutatóval jellemzett működőképességet jelent.

Adatbázis-biztonság nézőpontjából a bizalmasság annak biztosítása, hogy az adatok csak az arra jogosultak számára legyenek elérhetőek, a bizalmasság elvesztése az adatok illetéktelenek általi hozzáférését, megismerését jelenti. A sértetlenség azt jelenti, hogy a tárolt adatot, illetve az adatbázis-kezelő rendszert csak az arra jogosultak változtathatják meg, azok észrevétlenül nem módosulhatnak és nem törölhetők. A rendelkezésre állás annak biztosítása, hogy a felhatalmazott felhasználók hozzáférjenek a szükséges adatokhoz. A rendelkezésre állás megsértése azt jelenti, hogy az adatokhoz, illetve az adatbázis-kezelő rendszerhez való hozzáférés egy adott időtartamra nézve megsérül, vagy teljes mértékben megszűnik.

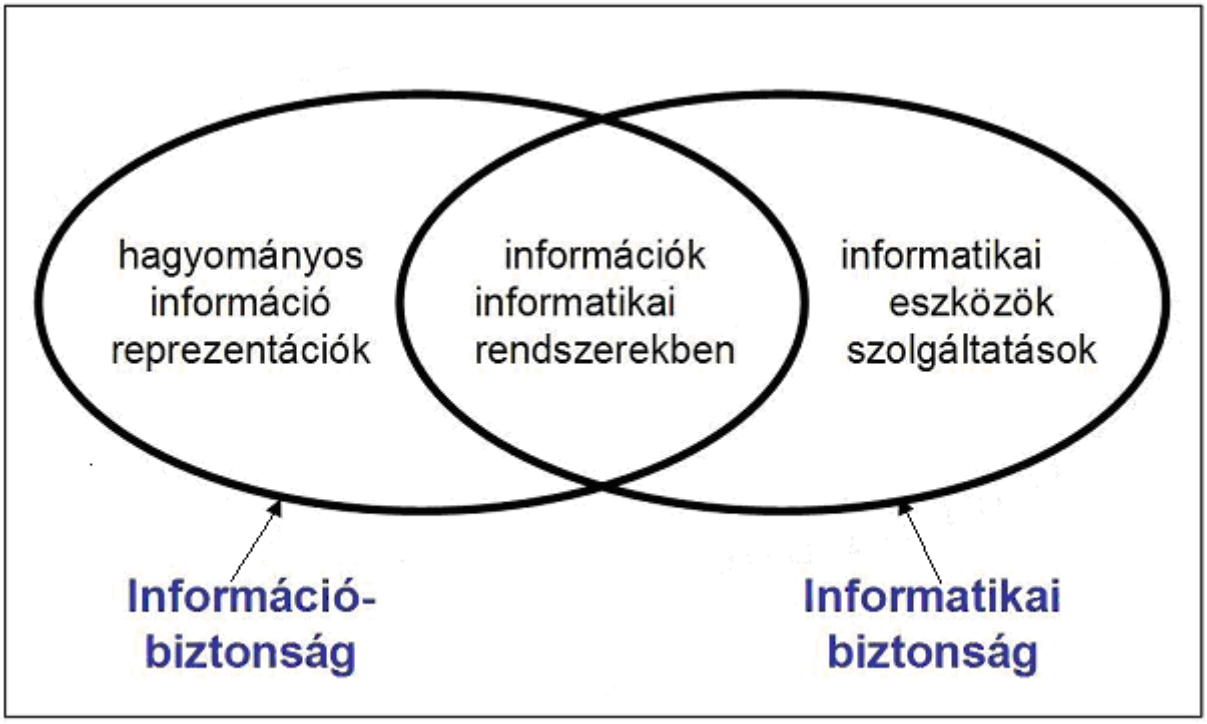
Az adatbázisok védelme szempontjából a bizalmasság, sértetlenség és rendelkezésre állás biztosításának követelménye mindenképp fontos szerepet játszik. A letagadhatatlanság és a hitelesség biztonsági kritériumait adatbázisokkal kapcsolatban ritkán említik, ezeket szokás a sértetlenség biztonsági tulajdonság részének is tekinteni. A letagadhatatlanság az a biztonsági tulajdonság, amely megfelelő bizonyítékokkal szolgál az adatbázis-kezelő rendszerben végrehajtott tevékenységek későbbi ellenőrizhetőségét illetően, ezt auditálhatóságnak vagy elszá-

moltathatóságnak is szokták hívni. A hitelesség az adat forrásának, eredetének a valódiságát jelenti.

ADATBÁZIS-BIZTONSÁG ÉS INFORMATIKAI BIZTONSÁG KAPCSOLATRENDSZERE

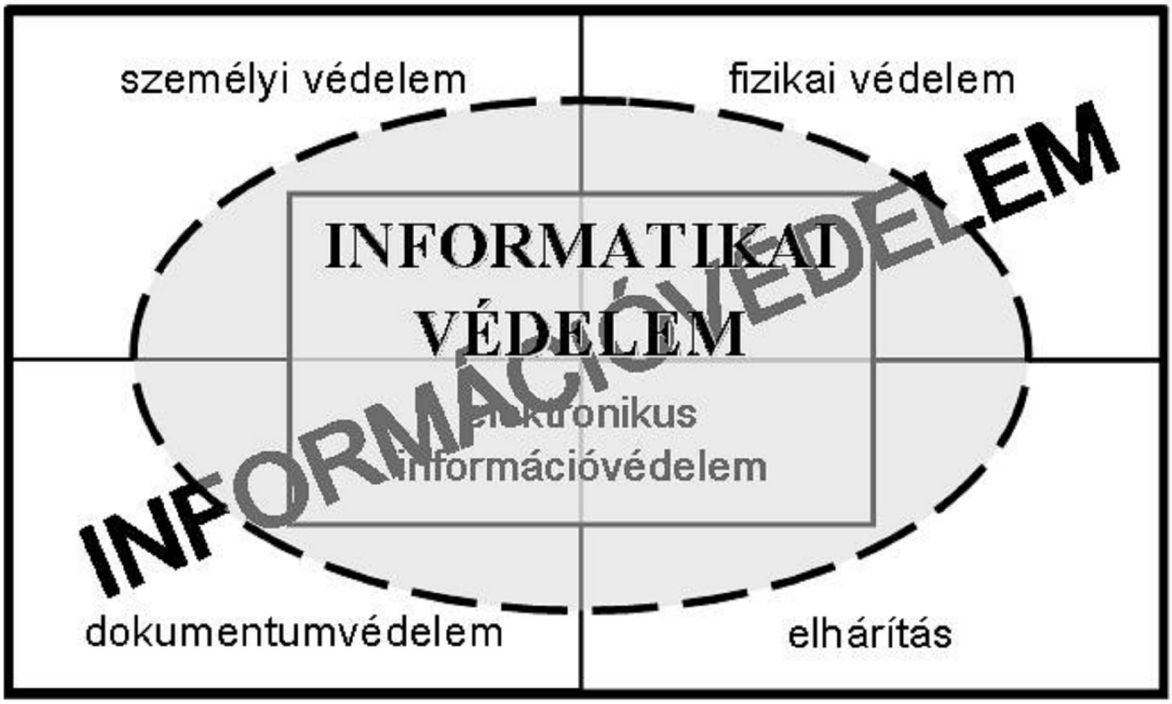
A következőkben az informatikai biztonság és az adatbázis-biztonság kapcsolatát vizsgáljuk meg, amit a témához szorosan kapcsolódó fogalmak értelmezésével kezdünk. Az informatikai biztonság és az információbiztonság kifejezéseket még ma is gyakran összekeverik, felcserélik, egymás szinonimájaként használják. A két fogalom helytelen használata mögött az angol terminológia nem-egyértelműsége jelentős szerepet játszhat, ugyanis az angol nyelvben az 'information security' kifejezés írja le mind az informatikai biztonságot, mind pedig az információbiztonságot. Az angol dokumentumok magyar nyelvre történő fordításakor feltétlenül figyelembe kell venni a szövegkörnyezetet, ami alapján a helyes magyar terminológiát megválaszthatjuk.

Az információbiztonság és informatikai biztonság kapcsolatáról több tudományos cikkben is olvashatunk. Munk Sándor [13] a következő értelmezés szerint tárgyalja a fogalmakat. Az informatikai biztonság jelentése az informatikai rendszerek és az általuk kezelt adatok biztonságához kötődik, az információbiztonság pedig a tetszőleges módon hordozott (pl. papíron, fejben, adatbázisban, elektronikus dokumentumban) információ védelmével kapcsolatos, ugyanakkor nem tartalmazza az informatikai rendszereknek a biztonságát. Az információbiztonság és az informatikai biztonság egymáshoz való viszonyát a szerző a következő ábrával szemlélteti:



1. ábra. Információ biztonság és informatikai biztonság [13] alapján

Muha Lajos [14] az információvédelem és informatikai védelem kapcsolatát vizsgálja a NATO védelmi előírására [15] alapozva, mely szerint: „Az információvédelem az általános védelmi rendszabályok és eljárások alkalmazása, az információ megsemmisülésének vagy kompromittálódásának megelőzése, felfedése ellen és helyreállítása céljából”. Az informatikai védelmet az információvédelemnél szűkebb, de önállóan is működtethető szakterületként jellemzi, amibe csak az informatikai rendszer védelme szempontjából szerepet játszó információvédelmi részterületek tartoznak. A két fogalom kapcsolatát Muha Lajos a következő ábrával szemlélteti:



2. ábra. Információvédelem és informatikai védelem kapcsolata [14] alapján

Az informatikai rendszer fogalmának értelmezésére szintén különböző megközelítések léteznek. A NATO szabályozókat megvizsgálva például a következő releváns fogalmakkal találkozunk: ’information system’, ’communication system’ és ’communication and information system’ [16]. Általában az informatikai rendszer egységesen elfogadott sajátossága, hogy információs tevékenységeket támogat, összetevőit technikai eszközök, programok, adatok, illetve szükség esetén a működtető személyzet alkotják, illetve eleget tesz a rendszer fogalom követelményeinek is. (Tehát nem nevezhető informatikai rendszernek egy egyedi eszköz vagy akár több, egymással kapcsolatban nem álló eszköz összessége sem.) [17]

A legszűkebb értelmezés a számítógépes rendszereket, egy ennél bővebb a számítógépes és kommunikációs rendszereket, a legtágabb pedig az információ feldolgozással kapcsolatos rendszereket sorolja ide. A továbbiakban informatikai rendszer alatt az információs tevékenységet támogató eszközök, programok, adatok, valamint a működtető személyek együttesét értjük, mely a következő elemekből épül fel [17]:

1. az informatikai rendszer fizikai környezete és a működéséhez szükséges infrastruktúra;
2. hardver;

3. szoftver;
4. kommunikációs eszközök és hálózat;
5. adathordozók;
6. dokumentumok és dokumentáció;
7. személyek.

Informatikai rendszerek közé a következő rendszerek tartoznak [14]:

1. a számítástechnikai rendszerek és hálózatok, ide értve az internet szolgáltatást is;
2. a vezetékes, a mobil, a rádiós és műholdas távközlés;
3. a vezetékes, a rádiófrekvenciás és műholdas műsorszórás;
4. a rádiós vagy műholdas navigáció;
5. az automatizálási, vezérlési és ellenőrzési rendszerek;
6. az előbbiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

Az informatikai biztonság és az informatikai védelem egymáshoz szorosan kapcsolódó fogalom. Az informatikai biztonságnak a szakirodalomban megtalálható meghatározásai különböző nézőpontból közelítik meg a fogalmat, az eltérő hangsúlyok jöhetnek többek közt (1) a védelem, (2) a biztonság, mint állapot, (3) a biztonság ellenőrzése és (4) a védendő tulajdonságok oldaláról. [18].

Az említett különböző hangsúlyok megjelennek például a hálózati munkacsoport egyik releváns RFC dokumentumában [19], melyben az informatikai biztonság fogalmát három pontban foglalják össze. A meghatározás magában foglalja egyrészt azokat az intézkedéseket, melyek az informatikai rendszer védelmére irányulnak, másrészt az informatikai rendszernek azt az állapotát, mely a védelmére létrehozott és fenntartott intézkedések hatására jön létre, harmadrészt pedig a rendszer erőforrásainak olyan állapotát, mely mentes a jogosulatlan hozzáférésektől, a jogosulatlan vagy véletlen változtatásoktól, tönkretételektől és veszteségektől.

Az ISO 27001:2005-ös szabványban [12] ’information security’ fogalom alatt az információk bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzését értik, megjegyezve azt, hogy még egyéb tulajdonságok védelmére is szükség lehet, mint a hitelesség, elszámoltathatóság, letagadhatatlanság és megbízhatóság.

A témánkat érintő, egy másik széles körben elterjedt szabványban, a NIST 800-30-ban [20] az informatikai biztonságon az informatikai rendszer tulajdonságát és működési folyamatait értik, melyek logikailag és fizikailag átszövik a rendszert. Az öt biztonsági cél pedig a sértetlenség, rendelkezésre állás, bizalmasság, elszámoltathatóság és garancia (mely az előző négy kritérium teljesítésére vonatkozik).

Az Amerikai Egyesült Államok hadseregében a biztonság alapfogalma a 'security' (biztonság, védelem) helyett az 'assurance' (garancia, garantált védelem) kifejezésre épül. Az ’information assurrance’ fogalmát következőképpen határozzák meg: mindazon intézkedések összessége, amelyek rendeltetése az információk és az informatikai rendszerek megóvása és védelme, rendelkezésre állásuk, sértetlenségük, hitelességük, bizalmasságuk és letagadhatatlanságuk biztosításával, beleértve az informatikai rendszerek helyreállítására irányuló védelmi, figyelési/észlelési és reagálási képességeket is. [21]

Munk Sándor által javasolt biztonság alapmodellje [13] szerint az informatikai biztonság meghatározásához szükséges feltárni a biztonság alanyát, ennek sebezhetőségeit, védendő tulajdonságait és a fenyegetéseit. Az informatikai rendszer biztonságát fenyegetések veszélyeztetik, ami alatt olyan potenciálisan káros, vagy meg nem engedett hatást értünk, mely a védendő rendszer valamely összetevőjét károsan, egy megengedett mértéknél jobban befolyásolja. A fenyegetések bekövetkezését az informatikai rendszer hiányossága vagy gyengesége, azaz sebezhetősége teszik lehetővé. A veszélyeztetés jellegét tekintve megkülönböztetünk fizikai, információs vagy tudati szinten jelentkező hatást [13].

Az informatikai biztonság értelmezése tekintetében Magyarországon a következő meghatározás terjedt el: Az informatikai biztonság az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. [14]

Teljes körű védelem esetén a védelmi intézkedések a rendszer összes elemére kiterjednek. A védelem zárt, ha az figyelembe veszi az összes releváns fenyegetést. Folyamatos a védelem, ha az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul. Kockázattal arányos a védelem, ha egy kellően nagy időintervallumot vizsgálva a védelem költségei arányosak a potenciális kárértékkel. A védelem akkor kielégítő mértékű, ha rá akkora összeget és olyan módon fordítanak, hogy ezzel egyidejűleg a kockázat az érintett fél számára még elviselhető szintű vagy annál kisebb. [22]

Célszerű a biztonságot egy állapotként, a védelmet pedig tevékenységek rendszereként értelmezni. Az informatikai védelem az informatikai biztonság kialakítására és fenntartására — a biztonság összetevőinek érvényesülésére — irányuló tevékenységek és rendszabályok összessége [23]. A védelem feladatai közé tartozik a megelőzés, az észlelés, a reagálás és az esemény- vagy válságkezelés. [14]

Napjainkban egy szervezeten belül az informatikai biztonság gyakorlata a következő alapintézkedéseket tartalmazza [9]:

1. az informatikai biztonságpolitika dokumentumainak elkészítése;
2. az informatikai biztonság felelősségeinek kiosztása;
3. informatikai biztonságtudatosság, képzés és oktatás;
4. helyes adatfeldolgozás az alkalmazásokban;
5. műszaki sebezhetőség kezelése;
6. működésfolytonosság irányítása;
7. az informatikai biztonsági incidensek menedzsmentje.

Ha az informatikai biztonság meghatározását megvizsgáljuk, akkor észrevesszük, hogy az két alapterületet foglal magában. Egyrészről az informatikai rendszerben kezelt adatok sértetlenségének, bizalmasságának és rendelkezésre állásának elvesztését kívánja megakadályozni. Másrészről pedig magának az informatikai rendszernek a megbízható működését jelenti, ami magába foglalja a rendszer elemeinek sértetlenségét és azok rendelkezésre állását. Az informatikai biztonságot veszélyeztető fenyegetések elsősorban az adatok biztonságát veszélyeztetik, de gyakran nem közvetlenül, hanem az azokat kezelő rendszerelemeken keresztül érvé-

nyesülnek.

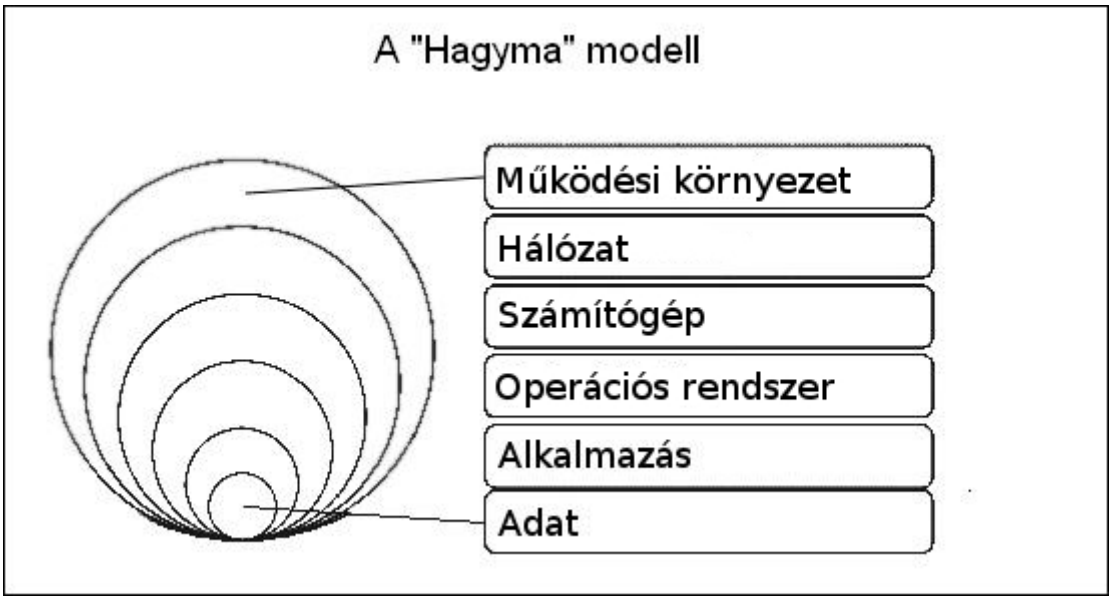
Ha az informatikai biztonság és az adatbázis-biztonság kapcsolatát szeretnénk feltárni, akkor meg kell vizsgálnunk mindkét esetben a biztonság alanyát, illetve annak védendő tulajdonságait. Az informatikai biztonság alanya az informatikai rendszer és az abban kezelt adatok halmaza, az adatbázis-biztonság esetében pedig az adatbázis-kezelő rendszer és az adatbázisokban tárolt adatok. Az informatikai rendszerek által kezelt adatok egyik leggyakoribb tárolási módját az adatbázisok alkotják, az adatbázis-kezelő rendszerek pedig az informatikai rendszerek részét képezik, vagyis az adatbázis-biztonság alanya az informatikai biztonság alanyának a része. Az előző fejezetben felvázolt adatbázis-biztonságot érintő tulajdonságok – sértetlenség, rendelkezésre állás, megbízhatóság, letagadhatatlanság, hitelesség – az informatikai biztonság esetében is lényeges szerepet játszanak. Ebből az is következik, hogy az adatbázis-biztonságot érintő sérülékenységek, illetve fenyegetések az informatikai biztonságra is lényeges hatással vannak. Ezek alapján megállapíthatjuk, hogy az adatbázis-biztonság az informatikai biztonság részét képezi, köztük rész-egész viszony áll fenn.

ADATBÁZIS-BIZTONSÁG HELYE, SZEREPE

Mivel az adatbázisokban koncentráltan található érzékeny, kritikus információ, az adatbázisok védelme fontos feladattá vált. Az adatbázisok az architektúra legutolsó pontján, tűzfalak védelmével ellátva helyezkednek el, ezért sokáig ezek védelme az informatika biztonsági feladatok között nem szerepelt prioritásként. Mára a helyzet megváltozott. Egyrészt a webes alkalmazások elterjedtével támadásuk könnyebbé vált, a behatolók ellen kevésbé vannak elrejtve, másrészt integritásuk megsértése bizonyos esetekben helyreállíthatatlan vagy nagyon problémásan helyreállítható helyzetet teremtene, illetve törvényi előírások is létrejöttek az adatok védelme érdekében.

Az informatikai rendszerek fejlődésével, elterjedésével az informatikai biztonság szakterülete is bővül, fejlődik, egyre több speciális részterülete alakul ki. Az informatikai rendszerek biztonságának kialakításában mára a ’mélységi védelem’ (angolul defense in depth) stratégiája egy meghatározó iránnyá vált, melyben a védelmet több rétegbe szervezve kívánják elérni (ez az elv megtalálható például az USA haderejének informatikai védelmi direktívájában is [21]). A rétegek kategorizálása több szempontrendszerre épülve történhet, például az informatikai rendszerek különböző komponenseinek vezérfonala alapján.

Ha az alábbi ábrán található ’hagyma modell’ szerint vizsgáljuk az informatikai biztonságot, akkor megkülönböztethetünk adatbiztonságot, operációs rendszer biztonságot, alkalmazás biztonságot, hálózat biztonságot és működési környezet biztonságot. Mivel az informatikai rendszerekben az adatok tárolására az egyik legelterjedtebb módszer az adatbázisokban történő tárolás, a ’hagyma modell’ szerinti informatikai biztonság legbelső területének részét képezi az adatbázisokban tárolt adatok biztonsága.



3. ábra. Az informatikai biztonság hagyma modellje [24] alapján

Az adatbázis-biztonság az informatikai biztonság részét képzi, csakúgy, mint a hálózat biztonság, operációs rendszer biztonság, alkalmazások biztonsága vagy a fizikai biztonság. Az adatbázis-biztonságot az informatikai rendszer többi elemével egységben, csak komplex módon lehet megvalósítani, ugyanakkor célszerű és létjogosult, mint az informatikai biztonság egy különálló területét kezelni, ami hangsúlyosan érvényes a kritikus információs infrastruktúra védelem tekintetében.

Az előbbi gondolatot támasztja alá az USA Védelmi Minisztériuma által kiadott, a vezérlő rendszerek biztonságával foglalkozó egyik dokumentum is [25], melyben az informatikai biztonságot érintő egyik legkritikusabb támadási módszerként elemzik a vezérlő rendszerek adatbázisait érintő támadásokat. A következőket olvashatjuk: „Adatbázis alkalmazások a vezérlő rendszerek és a kapcsolódó naplózó rendszerek alkalmazás komponenseinek egyik leglényegesebb elemét adják.” „Az adatbázisokban található információ értékes célponttal bír a támadók számára. Az értékes adatokat tartalmazó adatbázisokba való behatolás messzire kihatható következményekkel járhat, különös tekintettel a vezérlő rendszerek környezetében, ahol az adat pontosság és integritás kritikus mind az üzleti, mind a működési döntési folyamatokban.”

Az adatbázis-biztonság és védelem az adatbázis-kezelő rendszerek megjelenése és elterjedése utáni években egészen mást jelentett, mint manapság. A hagyományos adatbázis védelem a hitelesítés (authentication), jogosultság kiosztás (authorization) és hozzáférés szabályozás (access control) köré csoportosul. Ezek megfelelő használata ma is a biztonságos működés szükséges feltétele. Az adatbázisok elterjedésével, elérésük módjának kiszélesedésével, illetve a különböző támadási módszerek megjelenésével az adatbázis-biztonság fogalomköre is tágult. A támadások számának növekedésével és a törvényi szabályozások bevezetésével a biztonsági megoldások bővültek. Új igények, szükségletek jelentek meg az adatbázis-biztonságimegoldások területén, mint például az adatbázisokban történő adattitkosítás, a felhasználók hitelesítésének és jogosultság kiosztásának a komplex informatikai rendszeren belüli egységes kezelése, az adatok biztonsági besorolását figyelembe vevő jogosultság kiértékelés, az adatbázis rendszerek monitorozása vagy a kiváltságos felhasználók jogainak korlátozása.

Az adatbázis-biztonság megvalósulásához kiemelt figyelmet kell fordítani az informatikai rendszer adatbázis rendszerekkel összefüggő összetevőinek biztonságára is. A hálózta, az adatbázis szervert futtató gép operációs rendszerének és az azon futó egyéb alkalmazásoknak (web szerver, alkalmazás szerverek, címtár szerver) megfelelő védelme szorosan összefügg az adatbázis-biztonsággal. Az adatbázist elérő alkalmazások jelentik az adatbázisok felé a legnagyobb támadási felületet. Az adatbázis-biztonság és az informatikai biztonság egyéb részterületeinek szoros kapcsolatának hangsúlyozását megtalálhatjuk az USA Védelmi Minisztériuma által kiadott Adatbázis-biztonság Technikai Megvalósítási Útmutatóban [8] is.

Feltehetjük a kérdést, hogy van-e létjogosultsága az adatbázis-biztonsággal, mint az informatikai biztonság egy meghatározott területével külön foglalkozni vagy pedig ezt az informatikai biztonság helyes kezelésével automatikusan úgyis elérjük? Mivel az adatbázis-kezelő rendszerek és az adatbázisok az informatikai rendszer egy elhatárolható részét képzik - a több rétegű architektúra modellben például egy speciális réteget alkotnak -, védelmüket egy külön egységet kezelve célszerű megtervezni és biztosítani. Ezt alátámasztja egyrészt az, hogy léteznek kimondottan az adatbázisok ellen irányuló támadási módok, másrészt pedig az informatikai biztonságot komplex módon érintő incidensek súlyos következményekkel járhatnak az adatbázisokban tárolt adatok biztonságára nézve. A következőkben néhány kritikus infrastruktúrával kapcsolatos biztonsági incidensen keresztül megvizsgáljuk azok adatbázisokat érintő hatását.

2009 decemberében számítógépes támadás érte az amerikai Nemzeti Légügyi és Űrhajózási Hivatalának (NASA) két alrendszerének informatikai központját. A támadók adminisztrációs felületeteket hackeltek meg, valószínűen demonstrációs célból. A megtámadott oldalakról készült képernyőfotókból megállapítható volt, hogy a hackerek súlyos módosításokat is végrehajthattak volna a rendszerben, amire azonban nem került sor. A támadást SQL injekciós módszerrel hajtották végre [26]. Feltételezhető, hogy a NASA informatikai rendszere erős informatikai védelemmel rendelkezik, támadások számára nem képvisel könnyű célpontot, mégis a fenti eset bekövetkezhetett. A támadás módszere arra enged következtetni, hogy a támadóknak súlyos adatbázisokat érintő módosításokat is lehetőségükben állt végrehajtani.

2009. január 19. és február 7. között két olyan incidens következett be az elektronikus kormányzatot támogató Központi Elektronikus Szolgáltató Rendszer működésében, melynek adatbázist érintő vonzata is volt [27]. A hibák utáni biztonsági ellenőrzések során megállapították, hogy az incidensek visszavezethetőek a nem kellő gondossággal letesztelt programmódosítások éles üzembe állítására, a változáskezeléssel kapcsolatos – informatikai biztonság körébe tartozó – szabályok és eljárásrendek személyi mulasztás miatt bekövetkezett figyelmen kívül hagyására.

Az első incidens során az Országos Egészségbiztosítási Pénztár (OEP) informatikai rendszere az egészségügyi szolgáltatóknál és a gyógyszertárakban olyan állampolgárok esetében is rendezetlen jogviszonyt jelzett vissza hibásan, akik ténylegesen érvényes biztosított jogviszonnyal rendelkeznek. Az incidens során nem az alapadatok, hanem a feldolgozás során újra számított adatok sérültek meg. A megsérült adatokat tartalmazó adatbázisok újraszámlálása és ellenőrzése jelentette a helyreállítás időigényének jelentős részét.

A második incidens során az ügyfélkapu beléptetési moduljának átmeneti tárában (cache) keletkezett olyan üzemzavar, amely a hiba időszakában az ügyfélkapun belépett felhasználók egy része esetében a kapcsolatok keveredését okozta. A hiba oka az új program verzió hibás konfigurációs beállítása okozta. A hiba következtében felhasználók saját adataival nem tudtak

belépni az ügyfélkapun, ugyanakkor a bejelentkezési kísérlet eredményeként másik – szintén bejelentkezni szándékozó - felhasználónak az adataival beléptek az Ügyfélkapu belső felületére. A hiba következtében a felhasználó hozzáférhetett a másik felhasználónak a Központi Rendszer által biztosított tartós tárához, törölhette annak ügyfélkapus regisztrációját, letölthette a más címére érkezett visszaigazolásokat, üzeneteket vagy átmehetett valamely szakrendszer szolgáltatásaihoz (például az APEH rendszerébe) és a szakrendszer által engedélyezett szolgáltatásokat igénybe vehette. Ez utóbbi következmény például az APEH adatbázisaiban tárolt adatok módosítását és megismerését tette lehetővé, ami a legsúlyosabb biztonsági incidenst jelenti.

Ezek a példák is szemléltetik az informatikai biztonság és az adatbázis-biztonság szoros kapcsolatát, a kimondottan adatbázis-biztonságot érintő támadások jelentőségét a teljes informatikai biztonságra, illetve tetszőleges informatikai biztonsági incidens súlyos következményeit az adatbázis-biztonságra.

A fentiek alapján megállapítható, hogy az adatbázis-biztonság az informatikai biztonság egyik fontos részterülete. Az adatbázisok védelme kiemelt figyelmet érdemel az informatikai védelmen belül, mivel az adatbázis-kezelő rendszerekben tárolt adatok tönkretétele helyrehozhatatlan problémát okozhat a teljes informatikai rendszer működésében. Az adatbázis-biztonságot az informatikai rendszer többi elemével egységben, csak komplex módon lehet megvalósítani a rendszer-elemek interdependenciája miatt, ugyanakkor célszerű és létjogosult, mint az informatikai biztonság egy különálló területét kezelni.

ÖSSZEGZÉS: AZ ADATBÁZIS-BIZTONSÁG EGY LEHETSÉGES ÉRTELMEZÉSE

Összegzésképpen megállapítható, hogy az adatbázis-biztonság értelmezése az idők folyamán megváltozott, kibővült. A szűkebb típusú értelmezés szerint az adatbázis-biztonságot a tárolt adatok biztonsága jelenti, ezen belül az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, ez a hozzáállás az adatbázis-kezelő rendszerekről nem tesz említést. Ez a szemléletmód az adatbázis-kezelő rendszerek első megjelenésétől kezdve megfigyelhető. A rendszerek fejlődésével és elterjedésével egy tágabb típusú értelmezés is megjelent, mely a tárolt adatokat és az ezeket kezelő adatbázis-kezelő rendszert tekinti a biztonság védendő objektumának. Az adatbázis-biztonságnak ezt a megközelítését találhatjuk meg például az USA Védelmi Minisztériuma által kiadott Adatbázis-biztonság Technikai Megvalósítási Útmutatóban [8]. Mivel a témát kutatásaimban a kritikus infrastruktúra védelem, illetve az informatika biztonság megvalósítása oldaláról is tanulmányozom, az adatbázis-biztonság alanyának mind az adatbázisban tárolt adatokat, mind az azokat kezelő adatbázis-kezelő rendszereket tekintem.

Az adatbázis-biztonság védendő tulajdonságai közé tartozik a bizalmasság, sértetlenség és rendelkezésre állás. Bizonyos esetekben szükség lehet a hitelesség és letagadhatatlanság tulajdonságokra is, szemléletmód kérdése, hogy ezeket külön kategóriáknak tekintjük, vagy pedig a sértetlenség tulajdonság részének. Az utóbbi időben, a törvényi szabályozások és megfelelőségi elvárások hatásának köszönhetően kialakult egy újabb védendő tulajdonság is, amit elszámoltathatóságnak vagy más néven auditálhatóságnak nevezünk. Kijelenthetjük, hogy igazából nem a kategóriák száma a fontos, hanem a mögöttük lévő tartalom és védendő értékek, illetve az adatbázis-biztonság védendő tulajdonságai konkrét alkalmazások és környezetek

esetén eltérőek lehetnek.

Adatbázis-biztonság nézőpontjából a bizalmasság annak biztosítása, hogy az adatok csak az arra jogosultak számára legyenek elérhetőek, a bizalmasság elvesztése az adatok illetéktelenek általi hozzáférését, megismerését jelenti. A sértetlenség azt jelenti, hogy a tárolt adatot, illetve az adatbázis-kezelő rendszert csak az arra jogosultak változtathatják meg, azok észrevétlenül nem módosulhatnak és nem törölhetők. A rendelkezésre állás annak biztosítása, hogy a felhatalmazott felhasználók hozzáférjenek a szükséges adatokhoz. A rendelkezésre állás megsértése azt jelenti, hogy az adatokhoz, illetve az adatbázis-kezelő rendszerhez való hozzáférés egy adott időtartamra nézve megsérül, vagy teljes mértékben megszűnik.

A letagadhatatlanság és a hitelesség biztonsági kritériumai adatbázisokkal kapcsolatban ritkábban merülnek fel, ezeket szokás a sértetlenség biztonsági tulajdonság részének is tekinteni. A letagadhatatlanság az a biztonsági tulajdonság, amely megfelelő bizonyítékokkal szolgál az adatbázis-kezelő rendszerben végrehajtott tevékenységek későbbi ellenőrizhetőségét illetően, ezt auditálhatóságnak is hívják. A hitelesség az adat forrásának, eredetének a valódiságát jelenti.

FELHASZNÁLT IRODALOM

[1] 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról.

[2] C. J. Date: An Introduction to Database Systems, 8th Edition, Addison Wesley 2004

[3] Ramez Elmasri Shamkant B. Navathe: Fundamentals of Database Systems, 5th Edition, Addison Wesley 2007

[4] Mario Guimaraes**,** Meg Murray: Using animation courseware in the teaching of database security. Proceedings of the 8th ACM SIGITE conference on Information technology education 2007

[5] Mario Guimaraes, New challenges in teaching database security, Proceedings of the 3rd annual conference on Information security curriculum development, September 22-23, 2006, Kennesaw, Georgia

[6] Mario Guimaraes, Herb Mattord, Richard Austin: Incorporating Security Components into Database Courses. Proceedings of the 1st annual conference on Information security curriculum development, October 8, 2004, Kennesaw, Georgia

[7] Dimple Arora: Introduction to Database Security and Auditing, http://cert-in.org.in/training/14Oct09/database_security.pdf (2010.03.19.)

[8] Database Secrity Technical Implementation Guide, Version 8, Release 1, 19 September 2007, Developed by DISA for the DoD

[9] Közigazgatási Informatikai Bizottság 25. számú Ajánlása, MIBA Magyar Informatikai Biztonsági Keretrendszer, 25/1-2. kötet Informatikai Biztonság Irányítási Követelmények (IBIK), 2008. június

[10] Útmutató az IT biztonsági szintek meghatározásához http://www.ekk.gov.hu/hu/emo/ekozigkeretrendszer/ek3-itbiztonsag/EKK_ekozig_ITbiztonsagiszintekmeghatarozasa_080822_V101.doc (2010.03.19.)

[11] 223/2009. (X. 14.) Korm. Rendelet az elektronikus közszolgáltatás biztonságáról

[12] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

[13] Munk Sándor: Információbiztonság vs. informatikai biztonság. – Robothadviselés 7 tudományos szakmai konferencia anyaga (2007.11.27.), Hadmérnök különszám

[14] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana. Bolyai Szemle, 2008 (XVII.)/4.

[15] Security within the North Atlantic Treaty Organisation (NATO) – C-M(2002)49

[16] AAP-31(A), NATO Glossary of Communication and Information Systems Terms and Definitions. - NATO C3 Agency, 1998.

[17] Munk Sándor: Katonai informatika II. Egyetemi jegyzet. Budapest 2006, ZMNE

[18] Vicente Aceituno Canal: On Information Security Paradigms http://www.issa.org/Library/Journals/2005/September/Aceituno Canal - On Information Security Paradigms.pdf (2010.03.19.)

[19] Network Working Group Request for Comments: 2828 Internet Security Glossary http://www.ietf.org/rfc/rfc2828.txt (2010.03.19.)

[20] National Institute of Standards and Technology (NIST): Risk Management Guide for Information Technology Systems, Special Publication 800-30 http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (2010.03.19.)

[21] DoD Directive 8500.01E, Information Assurance (IA). – USA Department Of Defense, 2007.04.23.

[22] Bodlaki Ákos-Csernay Andor-Mátyás Péter-Muha Lajos-Papp György-Vadász Dezső: Informatikai Rendszerek Biztonsági Követelményei, Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 12. számú ajánlása. Budapest, 1996. http://www.itb.hu/ajanlasok/a12/html/a12_1.htm (2010.03.19.)

[23] Munk Sándor: Az informatikai biztonság rendszertanához Bolyai Szemle 2009. XVIII/4

[24] Budai Péter: Hogyan csökkentsük az IT-kockázatokat? http://www.microsoft.com/hun/technet/dl.aspx?id=2c4172ce-c0f2-4dc5-9a11-583345d58663 (2010.03.19.)

[25] Control Systems Cyber Security: Defense in Depth Strategies http://csrp.inl.gov/Documents/Defense in Depth Strategies.pdf (2010.03.19.)

[26] Ifj. Zettner Tamás: Meghackelték a NASA-t
http://itcafe.hu/hir/nasa_hacker_tamadas.html (2010.03.19.)

[27] Miniszterelnöki Hivatal, Informatikai biztonsági felügyelő: Részletes jelentés a Központi Elektronikus Szolgáltató Rendszer egyes szolgáltatásainak üzemzavarairól. Budapest, 2009. február 24.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Inkovics Ferenc
ferenc.inkovics@gmail.com

HANGALAPÚ KOMMUNIKÁCIÓS RENDSZEREK

Absztrakt

Az emberi társadalom fejlődésével párhuzamosan a különböző kommunikációs technikák is fejlődtek. Az emberek egymás közötti kommunikációjában meghatározó szerepet játszik a hangalapú kommunikáció. A cikk röviden bemutatja a kommunikáció fejlődését, majd felsorolja a 4 főbb hangalapú kommunikációs megoldást és azok működését.

Parallel with the evolution of the mankind society different communication techniques also developed. The voice-based communication plays a specific role in the communication among people. This article briefly introduces the development of the communication then enumerates the main 4 voice-based communication solutions and their operation.

Kulcsszavak: *telefon, mobiltelefon, VoIP, műholdas telefon ~ telephone, mobile phone, VoIP, satellite phone, satphone*

Bevezetés

A szociális fejlődést erősen befolyásolta és a jövőben is befolyásolni fogja a társadalom kommunikációképessége. Kezdetben az emberek csupán gesztusokkal, arckifejezésekkel, egyszerű szavakkal tudtak egymással kommunikálni. Ily módon az egyik barlang vadászai csak nehezen tudták megértetni magukat egy másik horda vadászcsapatával. A nyelv fejlődése lehetővé tette, hogy a családok, törzsek népekké, nemzetekké váljanak. Ha aztán egy közös jelkészletben megegyezés született, a fejlődés következő állomása az üzenetek gyorsabb továbbítása volt. Például mind az aztékok, mind a római hódítók kiváló úthálózatot építettek ki, amin a futárok már gyorsan tudták a leveleket szállítani. Ez segítette a birodalmak irányítását, összetartását. A helyzet 1440-ig (a sajtó feltalálásáig) gyakorlatilag változatlan maradt. A korábbi korlátok drasztikus változását okozta a nyomtatás megjelenése, miáltal nagymennyiségű információ vált elérhetővé nagy területen, de különösen a telegráf és a telefon (1844-1876) szélesítette ki a lehetőségeket. Ettől kezdve a nagytávolságú és gyors kommunikációval lehetővé vált az országok, sőt a kontinensek közötti gazdasági együttműködés. [1]

A kommunikációs technikák fejlődését az ösztönözte, és ösztönzi a továbbiakban is, hogy egyre nagyobb adattömeg átvitelére van szükség egyre rövidebb idő alatt. A három legfontosabb paraméter, amivel a kommunikáció fejlődését is jellemezhetjük: sebesség, a

hatótávolság és az adattömeg (A fejlődés oda vezetett, hogy a sebesség és az adattömeg helyett egy új paramétert, az adatátviteli, vagy információátviteli sebesség fogalmát vezették be). A kommunikációs rendszerek tervezése során használatos még néhány további paraméter is. megbízhatóság, ár, kényelem. A társadalomi haladás és jólét, nagymértékben függött az alkalmazott kommunikációs technikától. Az információ átvitele - ezeken az alkalmazott technikákon - sokféle módon történt. Néhány mérföldkő ezekből a technikákból: a hegytetőről felszálló füstjelek, futárposta, újságkihordás, telefon, telex, rádió és TV műsorszórás, számítógép-hálózatok, fax, műholdas és száloptikai kommunikáció.

Az kommunikációra használt átviteli utak technikai megvalósítása szerint két csoportot különböztethetünk meg: vezetékes illetve nem vezetékes (vezeték nélküli), sugárzó eszközökkel megvalósított összeköttetések. A vezetékes rendszerek lehetnek modern üvegszálas, valamint hagyományos fémes kábelek, amely kategóriába a tábori nehéz- és könnyűvezetékek, több eres kábelek sorolhatók. A sugárzó eszközök kategóriájába a különböző rövid-, és ultrarövid hullámú rádiók, mikrohullámú relék, troposzféra állomások, műholdas és cellás rendszerű telefonok tartoznak. [2]

A vezetékes telefon

A telefon az egyik olyan kommunikációs eszköz, ami nagytávolságú és gyors kommunikációt tesz lehetővé. Ezt az eszközt az emberi hang felismerhető módon történő átvitelére tervezték. A telefon (a telefonközpont) a világ legnagyobb automatája és földrajzi méreteit tekintve is a legnagyobb rendszer. A világ telefonhálózata kb. 1 milliárd vezetékes telefont és kb. 400 millió mobiltelefont foglal magába. Mindezek ellenére az emberiség felének még nem volt lehetősége telefont használni. [3]

A telefon működéséhez azt használjuk fel, hogy hang hatására változik a szénmikrofon ellenállása. A membránon levő szénrészecskék változó mértékben préselődnek össze a hanghullámok hatására. Az áramkörbe bekötött szénmikrofonon keresztül átfolyó áram a hang frekvenciája és erőssége szerint változik. A hang visszanyeréséhez ezt a változó erősségű áramot egy elektromágnes tekercsére vezetjük rá, melynek mágneses ereje egy vasanyagú membránt hoz rezgésbe, mely hallható hangot fog kibocsátani. Ez a megoldás csak egyik irányba való hangtovábbításra használható, ezért a másik irányú átvitelhez duplázni kell az áramkört. Ahhoz hogy 2-nél több állomás tudja felhívni egymást már egy telefonközpont szükséges. Kezdetben a telefonközpontos kollégák kapcsolták össze a két hívót, de ma már automata végzi ezt a feladatot, a hívó fél által küldött vezérlő információ (ez tartalmazza a hívott állomás azonosítóját) alapján. Technikailag megoldható lenne, hogy minden egyes készülék egy óriási telefonközponton keresztül legyen összekapcsolva, de a valóságban egy többszintű hierarchikus rendszer épül fel sok kisebb telefonközpontból. Ebben a rendszerben az egyes készülékek egy-egy vezetékpárral kapcsolódnak az adott helyi telefonközponthoz. [4]

Két telefonkészülék közötti hívás felépítésénél a helyi telefonközpontok, távhívó központok és a hierarchia rendszer egyéb szintjein elhelyezkedő központok is részt vehetnek a hívás felépítésében. A rendszernek csak azon elemei vannak bevonva a kapcsolat felépítésébe, amik a feltétlenül szükségesek. Amennyiben két telefonkészülék azonos helyi központhoz kapcsolódik, akkor nem szükséges egyéb központ beiktatása a kapcsolathoz. Az helyi központok több vezetékpárral, helyközi trönkkel, vannak összekötve a távhívó központtal. A távhívó központok pedig szintén több vezetékpárral kapcsolódnak a hierarchiában magasabb szinten elhelyezkedő kapcsoló központokhoz. [4]

A mobiltelefon

Az első mobiltelefonálási kísérletekre a XX. század elején sor került, és már az 1920-as és 1930-as években kedvező eredmények születtek. Pl.: A new yorki tűzoltók az 1930-as években már használtak mobiltelefont. Ezek a kezdetleges mobiltelefon-központok vezetékes irányba még nem voltak automaták, ezért a vezetékes hálózatokat csak telefonközpontos segítségével tudták hívni. Az első teljesen automatikus mobiltelefon-központot az Ericsson alkotta meg az 1950-es években. Ez a hálózat még 160 MHz-s volt, és közel 40 évvel később 1990-ben jelent meg a 450 MHz-es hálózat, ami csak néhány évig volt a legelterjedtebb. A mobiltelefónia fejlődése ekkortól ugrott meg. Eleinte évente majd később évente többször is vezettek be új szolgáltatásokat, technológiákat. [5]

Európában minden ország fejlesztette a saját analóg celluláris telefon rendszerét, melyek a többi rendszerrel inkompatibilis volt, mind felszerelés, mind működés tekintetében. A mobiltermékek a nemzeti határokon belülre korlátozódtak, és emiatt az egyes mobiltermékekre csak korlátozott piac alakult ki. Ezt korán felismerve, az európaiak alakítottak egy vizsgálati csoportot GSM (Groupe Spécial Mobile) néven, egy páneurópai nyilvános földi mobilrendszer kifejlesztéséhez. Az alábbi feltételeknek kellett megfelelnie az új rendszernek [6]:

- Jó hangminőség;
- Alacsony kezelőfelület és szolgáltatási költség;
- Nemzetközi roaming támogatása;
- Kézi kezelőfelületek támogatásának képessége;
- Új szolgáltatások bevezetésének támogatása;
- Sávszélesség hatékony kihasználása és;
- ISDN kompatibilitás.

A GSM csoport szabványa olyan sikeres lett, hogy a csoport neve rajta maradt a szabványon. A sikertől kezdve nem a csapatot, hanem a rendszert rövidítette a GSM (Global System for Mobile Telecommunications) betűszó. A GSM rendszert kitaláló csapat ma is folyamatosan dolgozik a rendszer továbbfejlesztésén, hogy a technika fejlődési ütemével lépést tudjunk tartani. Kb. évtizedenként kell 1-1 fejlettebb megoldást kidolgozni. [7]

A GSM rendszer négy egymásra épülő rendszerből áll:

- Mobil telefonok (SIM): olyan készülék, ami egy telefonkészülék és egy rádió adó-vevő berendezés ötvözete
- Bázis állomások (BTS): állandó helyű rádió adó-vevő berendezés, mely átjátszóként működik a mobiltelefon és a kapcsolóközpont között
- Telefonközpontok (BSC): feladata a hagyományos telefonközpontoknál megszokott hívási és kapcsolási feladatok ellátása
- Felügyelő rendszer (MSC): nevéből adódóan ellenőrzi és szabályozza a teljes rendszert

A hordozhatóság mellett még lényeges különbség a hagyományos távbeszélő hálózatok és a rádiótelefon-rendszerek között, hogy a vezetékes hálózatoknál kábeleket szinte korlátlan mennyiségben telepíthetünk, addig a rádiótelefon-rendszerek által felhasználható frekvenciák száma korlátozott. A 900 MHz-es tartomány 890MHz-től 960MHz-ig terjed, amelyet 2 db 25 MHz-es frekvenciasávra bontottak (az egyiket a bázisállomás a másikat pedig a mozgó állomás adási frekvenciájaként használják), és mindkettőben 124 db 200 KHz-es csatorna lett kialakítva. Ez a csatorna darabszám azért van, mert ha kisebbek lennének csatornák, akkor az egyes csatornák között áthallás lenne. Ma már létezik 900, 1800 és 1900 MHz-es GSM hálózat is.

Ahhoz az igényeket megfelelően ki lehessen szolgálni, statisztikát kell készíteni, hogy egyszerre mennyien telefonálnak, és meg kellett oldani, hogy egy adott csatornát többen is

használhassanak egy időben. Az utóbbi megoldására született a cellás kialakítás. A szolgáltatással lefedendő területet hatszögletű cellákra osztják és minden egyes cellának van egy bázisállomása. Amennyiben úgy osztjuk ki a csatornákat, hogy a szomszédos cellákban nincs kiosztva ugyanaz a csatorna akkor 2 cellával arrébb felhasználható ugyanaz a frekvencia. Egy-egy cella mérete 500m-től 30-35 km-ig is terjedhet. Ott ahol kevés az ügyfél nagyobb a cellaméret, ahol pedig sok ott kisebb.

Egy hívás kezdeményezésekor a telefon felméri a szabad csatornákat és kiválasztja a legnagyobb térerejűt. A kiválasztott csatorna lefoglalása után létrejött a kapcsolat a központ és az előfizető között, és a felhasználó hívásokat kezdeményezhet. Előfordulhat, hogy egy folyamatban lévő beszélgetés során lép át a felhasználó egy másik cellába. A mai rendszereknél már megoldott, hogy az összeköttetés ne szakadjon meg. A hívás automatikusan átadódik a következő cella egy csatornájára, persze ennek előfeltétele, hogy a fogadó cella rendelkezzen szabad csatornával. [6]

A csatornakijelölési módszereknek négy típusa van:

- Fix csatornakiosztás: A jelenleg működő rendszerek fix csatornakijelöléssel dolgoznak. A fix kijelölés a csatornákat úgy rendeli hozzá az egyes cellákhoz, hogy ezen a kiosztáson a későbbiek során már nem változtat. Előnye, hogy a kiosztást csak egyszer kell elvégezni, hátránya, hogy nem tud az egyes cellák forgalmi ingadozásaihoz alkalmazkodni. Ha a fix kiosztású rendszerben egy cellában minden csatorna foglalt, a hívás letiltódik. Ennek elkerülésére vezették be a csatornakölcsönzést. Ekkor a szomszédos cellák valamely szabad csatornája fogja kiszolgálni a hívást, ha a kölcsönzés nem zavarja a már folyó beszélgetéseket. Az eljárás hátránya, hogy nehéz forgalmi feltételek mellett a kölcsönzés további kölcsönzések sorozatához, végül a későbbi hívások letiltásához vezethet. Egyszerű kölcsönzés esetén egy csatorna csak akkor adható kölcsön, ha egyidejűleg szabad mindhárom legközelebbi azonos csatornájú cellában.
- Dinamikus csatornakiosztás: Ez az eljárás az igényeknek megfelelően rendeli a csatornákat a cellákhoz az igény kiszolgálásának időtartamára. Bármelyik csatornát bármelyik cella megkaphatja, feltéve, hogy a csatorna újrafelhasználási távon belül lévő más cella az adott pillanatban nem használja a kiosztandó csatornát. Előnye, hogy rugalmasan alkalmazkodik a forgalom ingadozásaihoz. Hátránya, hogy nagy terhelések esetén nem lehet teljesíteni a sűrű csatornakiosztást. Ez újrarendezéssel csökkenthető: az egymástól távolabbra kiosztott csatornákat, amikor lehet, úgy rendezik át, hogy az azonos csatornákat használó cellák a megengedhető legkisebb távolságra legyenek egymástól.
- Hibrid csatornakiosztás: A hibrid módszer átmenet a fix és a dinamikus csatornakiosztás között. A csatornákat két csoportba sorolják. Az egyik részt fix módon megkapják az egyes cellák, a másikat pedig dinamikus kiosztásra fenntartják.
- Adaptív csatornakiosztás: Az adaptív eljárásnál a csatornakiosztás csak egy adott hosszúságú időintervallumban érvényes. Az időintervallumok elején a csatornák például fix módszerrel kerülnek kiosztásra a forgalmi igények pillanatnyi területi eloszlása alapján.

A műholdas telefon

A műholdas telefon felfogható egyfajta mobiltelefonnak is, ez a megoldás nem földi bázisállomásokkal fedi le a szolgáltatási terültet, jelen esetben a Földet, hanem űrben keringő műholdakkal. Előnye pontosan az, hogy a földi bázisállomásokkal nehezen lefedhető területeken, pl.: havas hegycsúcsokon, homokos sivatagban vagy akár a viharos óceánokon is

lefedettséget nyújt. Hátránya, hogy az alkalmazott technológia miatt ez a legdrágább. A legismertebb műholdas rendszerek [8]:

- Inmarsat: elsősorban az arab világban elterjedt szolgáltató, de szolgáltatásaival lefedi Afrika és Eurázsia nagy részét is. A műholdja geostacionárius pályán levő műholdakat használ.
- Thuraya: 66 földközeli műholdjával lefedi a teljes Földet. Alacsony pályája és a műholdak kommunikációja miatt a geostacionárius pályán levő megoldásokhoz képest késedelem nélküli megbízható hang- és adatátvitelt biztosít.
- Iridium: 48 műhold kering földközeli helyzetben. Afrika nagy részét és a sarkköri részeket kivéve lefedi a Földet a szárazföldek környezetében.
- Globalstar: 3 db geostacionárius pályára helyezett műholddal a sarkköröket kivéve lefedi a Földet.

Tudnunk kell, hogy a műholdas átvitel késleltetése a földi mikrohullámú illetve a vezetékes rendszerekhez képest jelentős a nagy lehet távolság miatt, akár 250-300 ezredmásodperc. [4]

VoIP

Egyik legújabb megoldás a beszédalapú kommunikációban az internet protokoll alapú beszédátvitel, vagyis a VoIP (Voice over Internet Protocol). Több változatban lelhető fel. Az egyik, amikor a az emberek a PC-re telepített szoftver, illetve mikrofon és hangszóró segítségével az interneten keresztül beszélnek egymással. A szakemberek azonban ezt nem tekintik a telefonnal egyenértékű szolgáltatásnak. A VoIP továbbfejlesztett változatában az előfizető már saját, hagyományos telefonszámot kaphat, és az internetre bárhol (akár egy hotspot1 körzetében) csatlakozva bármilyen más telefonszámot felhívhat. Erre a "nem helyhez kötött" szolgáltatásra a szabályozó hatóságok a 21-es "körzetszámot" (prefixet) jelölték ki. [8]

A jelenlegi IPv4 nem tudja garantálni a szolgáltatás minőségét. Ezt a csomagok megérkezésének sorrendje és ideje okozza. A szolgáltatás minősége függhet a beszélgető partnerek hálózatbeli távolságától és a hálózat leterheltségétől is.

Általánosságban elmondható, hogy az IP-alapú beszélgetés olcsóbb a hagyományos tábeszélőn folytatott beszélgetésnél. Az internet hozzáféréssel rendelkező felhasználók a saját sávszélességük egy részét használják fel a VoIP beszélgetésekhez. Ebből következik, hogy nincs szükség egy különálló hálózat kiépítésére és fenntartására. Ez pedig költségmegtakarítással jár. Másik nagy előnye a VoIP-nek a hordozhatóság. Persze ez nem feltétlen, mert a beszélgetéshez előfeltétel egy internetes vonal megléte. VoIP szolgáltatás nyújtó nagyobb szolgáltatók közül néhány:

- Skype;
- MSN;
- VoIPCheap;
- stb.

A VoIP használatához szélessávú internet szükséges. Míg a ma elterjedt DSL szolgáltatás aszimmetrikus le és feltöltési sebességed nyújt, a VoIP szolgáltatáshoz mindkét irányban azonos sávszélesség szükséges. Azonban e különbségek ellenére is a ma elterjedt DSL szolgáltatások leggyengébbike is elégséges a VoIP szolgáltatás igénybe vételére.

A hagyományos telefonáláshoz képest több hibalehetőség van a VoIP-nél. Ilyen lehet a VoIP szolgáltató, az Internet szolgáltató, a csatlakozás szolgáltató vagy esetleg saját eszközünkkel kapcsolatban fellépő probléma vagy hiba. Azonban a vonalhiba az alternatív csatlakozás illetve útvonalak választásával orvosolható.

[1] egy nyilvános, vezeték nélküli internet hozzáférési pont

A segélyhívások ma már VoIP technológián is üzemelnek, azonban mivel nem helyhez kötött a szolgáltatás, ha a hívó fél nem tudja a pontos helyzetét, akkor nem lehetséges a segélyszolgáltatás biztosítása.

Sokan úgy gondolják, hogy a VOIP egy olyan kommunikációs csoportot jelent, mint a SKYPE vagy MSN, akik nagyon is vigyáznak rá, hogy szolgáltatásuk ne legyen kompatibilis mással, értékes ügyfeleiket, zárt körben, csak maguknak tartsák meg, és szinte teljesen elszigeteljék más lehetőségektől. Szerencsére a gyors fejlődésnek köszönhetően újabb és újabb protokollok születnek, melyek kinyithatják és szabványosíthatják (elsősorban a SIP) az internetes telefonálást. A SIP protokollnak köszönhetően többek között a szolgáltatók közötti hívásátadás is egyszerűvé vált. Ez egy hirtelen versenyhelyzetet teremtett, melynek köszönhetően a telefonálás percdíja nagyon nagymértékben lecsökkent, egyedül a mobiltelefon szolgáltatók tudták megőrizni a magas percdíjaikat Ők ugyanis továbbra is drágán veszik át a hívásokat. [9]

A VoIP szolgáltatók jobban szeretik az úgynevezett prepaid (előre fizetett) konstrukciókat, mivel a nem helyhez kötött felhasználás a hagyományos telefonvonalaknál több visszaélési lehetőséget biztosítanak.

Következtések

A globalizációt nagymértékben elősegítette és segíti továbbra is a kommunikációs technológiák fejlődése. Az újabb és újabb szolgáltatások megjelenése közelebb hozza az egymástól távol élő embereket. Mindegyik megemlített technológiában van még bőven kiaknázatlan terület, fejlesztési lehetőség.

A kommunikációs technikák fejlődése hozzájárul ahhoz is, hogy az információ egyre gyorsabban jutnak el a kívánt helyre, és ezzel egy időben a feldolgozandó adatmennyiség logaritmikusan növekedik. Ugyanakkor a jelenleg legelterjedtebb kommunikációs technológia, a vezetékes telefónia csak az emberiség feléhez jutott el. Az adatmennyiség növekedése és a technikák elterjedésének aránya újabb kihívások elé állítják korunkat, melyekkel szembe kell nézni, és erre felkészülni csak megfelelő szakértelemmel lehetséges. Ehhez a jövő szakembergárdáját már most el kell kezdeni felkészíteni.

Ugyanakkor a jövő veszélyeket is rejt. Ezeket a technikai vívmányokat használva abba a csapdába eshetünk, hogy a személyes szemtől szembeni kommunikációt minimálisra csökkentjük, és ez teljes egészében megváltoztathatja a társadalmi szokásokat is. Szembe kell néznünk a kibertérben megjelent bűnözés folyamatos növekedésével, a digitális azonosítókkal való visszaélésekkel, a digitális terrorizmussal stb-kel is. Ezek mind olyan kihívások melyekkel szemben fel kell lépni, harcolni kell ellenük.

Irodalmi hivatkozások

[1] A kommunikáció rövid története. http://www.szgti.bmf.hu/opto/1_KommTort.htm. letöltve: 2009-11-05

[2] Kerti András: Átviteli út biztonság. http://www.hadmernok.hu/archivum/2007/4/2007_4_kerti.pdf. letöltve: 2009-11-05

[3] Szám Norbert: A telefon története. http://mobil.nik.bmf.hu/tantargyak/fitk/hallgatoi_projektek/a%20telefon%20t%F6rt%E9nete%20i-szam_norbert.pdf. letöltve: 2009-11-05

[4] Kónya László: Számítógép-hálózatok. LSI Informatikai Oktatóközpont Alapítvány. http://e-oktat.pmmf.hu/halozatok (2001)

[5] Ilyenek voltak az első mobiljaink. http://www.origo.hu/techbazis/mobil/20070910-mobiltelefontorteneti-tarlat-a-mobil-shown.html. letöltve: 2009-11-15

[6] A GSM története. http://www.mobilport.hu/fokuszban/20030810/a_gsm_tortenete/. letöltve: 2009-11-15

[7] A GSM rendszer működése. http://www.rentit.hu/cikkek/47.aspx. letöltve: 2009-11-15

[8] Alternatív telefonos technológiák. http://www.kabelinfo.hu/kabelinfo/tudasbazis.php?cikk=tel_alternativteltechnologiak. letöltve: 2009-11-16

[9] Mit jelent a VoIP? http://voip.itt.ma/. letöltve: 2009-11-05

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Kassai Károly
kassai.karoly@hm.gov.hu

AZ ELEKTRONIKUS INFORMÁCIÓVÉDELMI FELADATOK ÉS A FELELŐSSÉG

Absztrakt

Az elektronikus adatkezelés szabályozottsága, a szükséges mértékű védelmi rendszabályok a honvédelmi szervezeteknél biztonsági menedzsment kialakítását és fenntartását követelik meg. A védelemből adódó jellegzetességek miatt (időtényező, személyi és egyéb erőforrás igények, szervezeti problémák) ennek a követelménynek van néhány szervezeti szempontból negatívnak tekinthető hatása, így célszerű a biztonsági menedzsment kérdések vizsgálata, a fontosabb feladatok azonosítása. Jelen cikk az elektronikus adatkezelő rendszerek menedzseléséhez szükséges feladatok azonosítását célozza annak érdekében, hogy a rendszer életciklusnak megfelelően érthetőbbek legyenek a védelemmel kapcsolatos követelmények.

The regularization, appropriate level security measures of the electronic information handling at the military organisation requires establishing and permanently upgraded security management.

This requirement has some negative organisation impact because of the nature of security (time, additional human and other resources, and organisation problems) so should be useful to observe the security management issues and identify the important tasks.

This article identifies the tasks of electronic information handling security management for the understandable security requirements according to the system life cycle.

Kulcsszavak: *információbiztonság, információvédelem, személyi biztonság, biztonsági menedzsment, biztonsági követelmények ~ information security, protection of information, personal security, security management, securiry requirements*

Bevezetés

A honvédelmi szervezetek elektronikus adatkezelésének biztonsági kérdései alapvetően két kategóriára bonthatók: a *felhasználók által végzendő védelmi feladatokra* és a *biztonsági menedzsment feladatokra*.

Jelen cikk az *elektronikus információbiztonsági menedzsment végrehajtói szintű szakfeladataira koncentrál*, de figyelembe veszi azt a tény, hogy egyes rendszerek vagy helyszín esetében ezek a szakfeladatok élesen nem határolhatók el a fizikai-, személyi vagy dokumentumbiztonsági kérdésektől.

Az átfogó jellegű jogszabályi megfogalmazások mellett szükség van a végzendő feladatok részletesebb azonosítására és ezzel a honvédelmi szervezeteknél a rendszer-specifikus és a szervezeti típusú felelősségi körök meghatározásának támogatására, így e területen a cikk közvetlenül támogatja biztonsági dokumentumokban és munkaköri leírásokban történő megfogalmazásokat.

Jogszabály minősített elektronikus adatkezelő rendszer esetében határoz meg a védelmi feladatok ellátását végző személyek kijelölésére vonatkozó követelményt a rendszerbiztonsági felügyelő/felügyelet formájában [1.]; mely feladatkör alapesetben nem tartalmazza a rejtjelzéssel kapcsolatos feladatokat (de nem is zárja ki azon feladatok együttes végzését sem).

A nemzeti és nemzetközi szabványok [2, 3, 4.] és a vonatkozó kormányzati ajánlás [5.] szintén határoznak meg feladatokat a biztonságért felelőssé tehető személy azonosítása érdekében.

A honvédelmi tárca információ biztonságpolitikája az általános követelmények és ajánlások szerint a honvédelmi szervezeteknél az elektronikus információvédelmi feladatok ellátása érdekében szervezethez és rendszerhez köthető felelősöket azonosít [6.], amely kötelezettséget a korábbi kiadású informatikai szabályzat is azonosít. [7.]

Az előbbi követelmények, illetve ajánlásoknak megfelelően a honvédelmi szervezeteknél *a szervezeti és adatkezelési sajátosságok figyelembe vételével* az elektronikus adatkezelés biztonsági kérdéseit a következő általános szempontokat specializálva célszerű megoldani.

A szervezeti szintű elektronikus információvédelmi szakfeladatok

A szervezethez köthető elektronikus információbiztonságért felelős személy (vagy szervezeti elem) az elektronikus adatkezelő rendszerektől függetlenül, az egész szervezetre vonatkozó szakfeladatokat végez a kijelölt vezető beosztású személy szakmai vezetésével. Az ebbe a körbe tartozó feladatok:

a) a szervezetnél található elektronikus adatkezelő rendszerek (eszközök) nyilvántartása, azok biztonsági besorolása;
b) a rendszer szintű kockázatelemzés irányítása, a folyamatos kockázatkezelési tevékenység felügyelete;
c) a szervezeti szintű elektronikus információvédelmi rendszabályok azonosítása, helyi szabályozás kialakítása, jóváhagyatása és időszakos felülvizsgálata;

d) a szervezetnél végzendő helyi képzési, továbbképzési feladatok és biztonsági tudatosságot segítő programok szervezésével és végrehajtásával kapcsolatos tevékenység;
e) a rendszer-specifikus felelősök szakmai felügyelete, támogatása;
f) a szervezetnél található elektronikus adatkezelő rendszerek védelmének szabályozásához szükséges jogszabályok, állami irányítás egyéb jogi eszközei körébe tartozó szabályozók szabványok, ajánlások nyilvántartása, rendelkezésre állásuk biztosítása;
g) a szakmai kapcsolattartás az együttműködő szervekkel és szervezetekkel;
h) a rendszerek kialakítása, fejlesztése során a projekt tevékenységben való részvétel és a szervezet elektronikus információvédelmi képviselete;
i) az elektronikus adatkezelő rendszerek biztonságával kapcsolatos ellenőrzési tevékenység szervezése, ellenőrzések végrehajtása, a biztonsági incidensek kivizsgálása (annak irányítása) és a szükséges korrekciós lépések felügyelete.

Annak eldöntése, hogy a védelmi rendszabályok felügyelete elvégezhető-e egy fővel, vagy szervezeti elemet kell kialakítani, a szervezet és adatkezelés elemzése után történhet meg. Ugyanígy további eldöntendő kérdés, hogy a biztonsági feladatokat önálló beosztásban vagy megbízással kell ellátni az adott honvédelmi szervezetnél.

Napjainkban egyértelműen érzékelhető az elektronikus adatkezelés terjedése, bonyolultságának növekedése, illetve az ezzel kapcsolatos fenyegetések és sebezhetőség bővülése. Emiatt *egyre nagyobb az alkalmazandó ismeretanyag, egyre bonyolultabb tevékenységeket kell kialakítani és fenntartani*, így a jövő vélhetően az önálló beosztások formájában történő felügyelet lesz, de az ehhez vezető út hosszú és rögös a honvédelmi szervezetek életében.

Az elektronikus adatkezelés rendszer-specifikus felügyelete

A honvédelmi szervezetnél alkalmazott elektronikus adatkezelő rendszerek, eszközök valamint a kezelt adatok mennyisége, bonyolultsága, a szervezeti és alkalmazása sajátosságok alapján eldöntendő kérdés a védelmi rendszabályok felügyeletéért felelős személyek számának és feladatainak meghatározása.

Egyszerűbb esetben a szervezeti szintű felügyelet elláthatja ezt a feladatot, de a gyakorlatban az a jellemző, hogy a rendszer-specifikus szakfeladatokat megbízás alapján tevékenykedő személyek látják el a terhek jobb elosztása érdekében.

Alapelv, hogy az *összeférhetetlenségre vonatkozó követelmény alapján* a biztonsági menedzsment úgy legyen kialakítva, hogy a felügyeleti feladatok *az adatkezelési helyekhez kötötten minél kevesebb erőforrást igényeljenek, a problémák megoldási ideje a lehető legrövidebb legyen*.

Az elektronikus adatkezelő rendszerek elektronikus információvédelméért felelős személy feladatainak meghatározásakor a következő általános követelményeket célszerű rendszer-specifikusan alkalmazni.

Az elektronikus adatkezelő rendszer kialakítása során végzendő szakfeladatok

Az egyik legfontosabb feladat a hadműveleti követelmények, a rendszerre vonatkozó általános biztonsági követelmények azonosítása, illetve az ezzel kapcsolatos változások

naprakész ismerete. Ennek alapján végezhető a kezdeti kockázatelemzés, *az elfogadható kockázatok (acceptable risk) azonosítása, és jóváhagyatása*.

A kockázat értékelés és a jóváhagyott elfogadható kockázatok alapján történhet meg a rendszer-specifikus biztonsági követelmények meghatározása, majd jóváhagyatása, és annak alapján a szükséges védelmi rendszabályok bedolgozása a tervezési folyamat során.

A BIZALMAS vagy magasabb minősítésű elektronikus adatkezelés esetén a tervezéshez elengedhetetlenül szükség van az üzemeltetési környezet kompromittáló kisugárzás elleni védelmi zónázására, és az eszközökre, kábelvezetésre, árnyékolásra, biztonsági távolságokra, földelésre vonatkozó követelmények azonosítására, amely feladat a későbbiekben láthatóan önálló beosztás vagy megbízás formájában végezhető.

Az üzemeltetés előkészítéseként az egyik legtöbb gondot okozó feladat *az üzemeltetéshez szükséges állomány és a felhasználók kijelöltetése és a minősítési szintnek megfelelő személyi biztonsági adminisztráció elvégzése*. A későbbi problémák megelőzése érdekében ebben a fázisban végre kell hajtani a hozzáférési joggal rendelkező személyek általános biztonsági oktatását is.

Az üzemeltetési környezet kialakításakor a biztonsági kérdések felügyelete, illetve a kockázatelemzés pontosítása a soros feladat.

Hazánkban a NATO, EU követelményektől eltérően a korábbi és a jelenleg hatályos jogszabály önálló akkreditálást határoz meg a fizikai-, személyi- és dokumentum biztonsági követelményeknek való megfeleltetés érdekében, így az elektronikus adatkezelő rendszerek kialakításakor e feladatokat is figyelemmel kell kísérni. Ezzel párhuzamosan haladhat a biztonsági követelmények alapján *a rendszer-specifikus biztonsági dokumentumok elkészítése*, valamint az üzemeltetési és egyéb dokumentumokba (szervezeti szintű vagy funkcionális szabályozók) a szükséges védelmi rendszabályok bedolgozása. Ennek során szükségessé válik az akkreditáláshoz, jóváhagyáshoz szükséges *biztonsági tesztre vonatkozó követelmények meghatározása*, majd a teszt végrehajtásának szakmai támogatása.

Napjainkban közvetlenül érzékelhető a missziós tevékenységek, gyakorlatok illetve az állandó rendszerek esetében is *az adatcserére, újabb kifejezéssel az adatmegosztásra vonatkozó fokozott igény*. Az ezzel kapcsolatos technikai, szervezési, együttműködési szakfeladatokat nem szükséges külön kiemelni, de fontos annak megjegyzése, hogy *főleg nemzetközi környezetben és minősített adatmegosztás esetén az ezzel kapcsolatos feladatok a tervezés és üzemeltetés során többlet feladatot jelentenek* a biztonsági dokumentumok, az engedélyezés, a technikai és menedzsment szintű együttműködés területén.

A rendszerbeállítás érdekében elkerülhetetlen, gyakran több körös feladat *az akkreditáláshoz, jóváhagyáshoz szükséges dokumentumok elkészítése* az hatósági követelmények szerint. Az ekkor már rendelkezésre álló részletes adatok alapján az üzemeltető és felhasználó állomány számára a szükséges tájékoztatási, képzési feladatok maradéktalanul elvégezhetők, valamint lehetővé válik *az üzemeltetési szakasz képzési, továbbképzési feladatainak azonosítása*.

A telepítés során jellemzően végzendő feladat a biztonsági funkciók kialakításának felügyelete, a biztonsági beállítások ellenőrzése, a rendszer szintű, az üzemeltetés és biztonság szempontjából *kritikus hozzáférésekre vonatkozó felügyeleti lehetőségek kialakítása*, illetve általánosan fogalmazva *a telepítés teljes körű biztonsági felügyelete, dokumentálása*.

A rendszerbeállítás előtt az akkreditáláshoz, jóváhagyáshoz szükséges adminisztratív feladatokat kell elvégezni, illetve *a megfelelő szintű biztonság hitelesíthetősége érdekében az eljárás során szükség van adatok, bizonyítékok szolgáltatására*.

Az akkreditálás, jóváhagyás során üzemeltetési és biztonsági területű hiányosságok merülhetnek fel, amely esetben szükség lehet a felszámolásukhoz szükséges eljárás kialakítására.

Amennyiben az akkreditálás, jóváhagyás során az üzemeltetés engedélyezése korlátozással történik, *a korlátozások érvényesítéséhez szükséges eljárásokat be kell dolgozni a biztonsági és üzemeltetési dokumentumokba*, és a változásokról tájékoztatni kell az érintetteket (felhasználók, üzemeltetők, vezető állomány, együttműködő szervezetek).

Az elektronikus adatkezelő rendszer üzemeltetése során végzendő szakfeladatok

Általános feladat a biztonsági dokumentumok naprakészen tartása, meghatározott időszakonként történő felülvizsgálata, illetve a jogosultak felé történő rendelkezésre bocsátása. Ennek részeként kiemelendő az időszakos kockázatelemzés végrehajtása, az elfogadható kockázatok azonosítása és jóváhagyatása, szükség esetén kiegészítő védelmi rendszabályok kidolgozása, mert az üzemeltetési szakaszban történő változások negatív hatással is lehetnek az elektronikus adatkezelő rendszer biztonságára.

Logikailag ide tartozik a rendszer életútja során keletkező ellenőrzési jegyzőkönyvek, biztonságot is érintő dokumentumok, jelentések áttekintése, értelmezése és értékelése, a tapasztaltak alapján a szabályozásban szükséges változtatások tervezése és végrehajtása.

Szervezeti vagy rendszer-specifikus feladatként egyaránt megjelenhet az illetékes szervek és szervezetek felé tájékoztatási, adatszolgáltatási kötelezettség teljesítése.

Szintén általános feladatként fogalmazható meg a biztonsági dokumentumokban foglaltak pontos betartása és betartatása, a biztonsági incidensek jelentése, szükség szerint közreműködés a helyreállításban, kivizsgálásban, a felhasználók és az üzemeltetők időszakos továbbképzése illetve munkájának folyamatos támogatása, a biztonsági tudatosságot erősítő feladatok végzése.

Hosszú távú, ismétlődő feladat az időszakos újra-akkreditáláshoz, jóváhagyáshoz szükséges feladatok végzése, az elektronikus adatkezelő rendszer *hardver és szoftver konfiguráció időszakos ellenőrzése*, az elektronikus adatkezelő rendszer használatának biztonsági felügyelete, naplófájlok és meghatározott paraméterek ellenőrzése, *az adathordozók kezelésének ellenőrzése*, a rendszer szintű, az üzemeltetés és biztonság szempontjából kritikus hozzáférésekre vonatkozó rendszabályok betartatása, valamint *a biztonsági mentésekre vonatkozó tevékenység ellenőrzése*.

A folytonossági és helyreállítási rendszabályok érvényesülésének ellenőrzése (szükséges állomány megléte, képzettség, gyakorlás, dokumentumok pontossága), illetve a tevékenységhez szükséges tervezési és változáskezelési feladatok végzése olyan további rendszer-specifikus feladat, melyet a hadműveleti követelményekben meghatározott rendelkezésre állási paraméterek, valamint a fenyegetettség és sebezhetőség alapján kell végezni.

A változáskezeléshez tartozó feladathalmaz a rendszer változtatásának előkészítése, kockázatelemzés végzése, a változások biztonsági hatásainak vizsgálata, szükség esetén közreműködés a biztonsági teszt kialakításában és végrehajtásában, a konfiguráció változtatás, vagy rendszer kiterjesztésének engedélyeztetésével kapcsolatos adminisztratív feladatok végzése és az esetleges hatósági eljárások előkészítése, a változtatások átvezetése a biztonsági dokumentumokban, illetve részvétel a meghatározott képzéseken, továbbképzéseken és biztonsági tájékoztatókon.

A rendszerből történő kivonás során végzendő szakfeladatok

A kezelt adatokra vonatkozó követelmények alapján a rendszerből történő kivonáshoz azonosítani kell a szükséges adatmentési, továbbítási, archiválási követelményeket. *Pontosítani kell az információs műveletek védelméhez szükséges rendszabályokat*, illetve érvényre kell azokat juttatni.

Amennyiben olyan kivonás történik, melynek következtében később a mentett felhasználói adatok, vagy rendszeradatok olvasása nem biztosított, az üzemeltető állománnyal együttműködve gondoskodni kell a szükséges információs környezet kialakításáról és fenntartásáról, ami gyakran beruházást, telepítést, képzést és fenntartási feladatok rendszerbe állítását is jelenti.

A rendszerből történő kivonás során azonosítani kell a szükséges törlési és megsemmisítési eljárásokat, ki kell alakítani a végrehajtás feltételeit és felügyelni kell a végrehajtást.

Az üzemeltető esetenként nem képes (vagy nem jogosult) a kezelt felhasználói adatok, üzemeltetési adatok megőrzési idejéről vagy törölhetőségéről nyilatkozni, így esetenként az adathalmozódásból adódó bonyolult ügyek eldöntése több adatgazda és egyéb felelős személyek együttműködését igényli.

Utolsó feladatként a szükséges konfigurációváltozási feladatok, a törlés vagy megsemmisítés dokumentálása, jelentése azonosítható.

A kompromittáló kisugárzás elleni védelem menedzselése

A minősített adatkezelésnél az idén megjelent jogszabály a korábbihoz lényegesen megfoghatóbban határozza meg a kompromittáló kisugárzás elleni védelem (TEMPEST) szakfeladatait [8.].

A honvédelmi tárca információbiztonsági politikája ezt a szakfeladatot a rendszer biztonságáért felelős személy feladatai közé sorolja, vagy önálló beosztásként (vagy megbízásként) fogalmazza meg.

Ennek megfelelően a BIZALMAS, vagy magasabb minősítési szint esetén a TEMPEST szakfeladatokért való felelősséget a szervezeti szinttől, a felügyelt rendszertől, valamint az üzemeltetési környezettől függően (röviden *a TEMPEST védelmi rendszabályok bonyolultsága szerint*) kell specializálni.

A szakterület biztonsági követelményeire és védelmi rendszabályaira vonatkozó kérdések a továbbiakban csak az általános feladatok szintjén azonosíthatók.

A szakfeladatokat végző személynek ismernie kell a kompromittáló kisugárzás elleni védelemre vonatkozó általános követelményeket, ami megköveteli a szükséges szabályozók rendelkezésre állását és alkalmazói szintű ismeretét.

Az általános követelmények alapján irányítani kell a létesítmény zónázással, a TEMPEST eszközökre vonatkozó követelmények meghatározásával kapcsolatos feladatokat, valamint képesnek kell lenni - önállóan vagy szakirányítási segítséggel - *az üzemeltetési környezet kialakításához szükséges kiegészítő követelmények meghatározására* (biztonsági távolságok, földelés, árnyékolás, szűrés) illetve a kockázatelemzés során a szakterületi támogatás biztosítására.

A kialakításhoz köthetően *a védelmi rendszabályokat be kell dolgozni a rendszer-specifikus biztonsági dokumentumokba*, illetve ki kell alakítani azt a *nyilvántartási rendszert, ami támogatja a TEMPEST feladatokkal kapcsolatos azonnali tájékozódást és tájékoztatást*. Ugyanígy a kialakítással kapcsolatos feladat a védelmi rendszabályok megfelelőségének igazolásához szolgáló dokumentumok vagy tanúsítványok kialakítása, illetve beszerzése.

Az elektronikus adatkezelő rendszer bonyolultsága függvényében nem elhanyagolható feladat az üzemeltető, biztonsági és a felhasználói állomány TEMPEST védelmi rendszabályaival való megismertetése és a helyi feladatok meghatározása.

A TEMPEST szakfeladatokat felügyelő személynek a rendszer beüzemelése érdekében közvetlenül támogatnia kell az akkreditálási folyamatot.

Az üzemeltetési szakaszban fő feladatként azonosítható a TEMPEST ismeretek naprakészen tartása (szabályozók pontosítása, képzéseken és továbbképzéseken való részvétel, az ellenőrzések során tapasztaltak hasznosítása).

A védelmi megoldásokat a meghatározott rendben ellenőrizni kell, a rendszer üzemelésével kapcsolatos személyek ismereteit szinten kell tartani, a védelmi rendszabályok megfelelőségét a technikai követelményeknek megfelelően mérésekkel és ellenőrzésekkel kell fenntartani, illetve a rendszer újra-akkreditálása, illetve hatósági ellenőrzése során be kell mutatni *a védelmi rendszabályok megfelelőségét bizonyító adatokat*.

Az adatkezelő rendszerek ezen életút szakasza tartalmazza a karbantartások, javítások és módosítások, fejlesztések témakörét is, ami bonyolultabb esetben épületgépészeti, erős- és gyengeáramú kérdések rendezését igényli. Itt figyelemmel kell lenni a rendszabályok, a környezet, esetleg a minősítési szint változására, különben beruházások futhatnak zátonyra. A „múltkor is így akkreditálta a hatóság”, vagy „ez ugyanolyan megoldás” típusú tartalmas szakértői érveléseknek tűnő megnyilvánulások veszélyes csapdákat hordozhatnak, téves vezetői döntéseket eredményezhetnek.

A rendszerből történő kivonás a kompromittáló kisugárzás esetében különös feladatokat nem igényel, csak a szükséges figyelmet kívánja meg. Mivel a kompromittáló kisugárzás elleni védelmi rendszabályok egy része az infrastruktúrához köthető, így *fontos annak pontos megértése, hogy mely megoldások, infrastrukturális elemek használhatók a létesítményben kialakított új elektronikus adatkezelő rendszer védelmére, és milyen átalakításokat, kiegészítéseket kell elvégezni a szabályos üzemeltetés érdekében.*

Az üzemeltetéshez szükséges biztonsági feladatok

Meghatározott helyszínhez, elektronikus adatkezelő rendszer hálózati elemeihez és adatkezelő eszközeihez rendelt üzemeltetésért felelős személy (pl. rendszeradminisztrátor, üzemeltető mérnök, technikus) vagy szervezeti elem információvédelmi feladatait a következő követelmények szerint kell rendszer-specifikusan meghatározni.

A kialakítás során végzendő feladatok

Az üzemeltetőnek szükség szerinti részt kell vennie a rendszer kialakításának tervezésében, illetve a kezdeti kockázatelemzésben, majd a rendszer-specifikus biztonsági dokumentum kidolgozásában, valamint az ehhez szükséges képzéseken. Ezek után feladat az üzemeltetési rendszabályok kialakítása, beleértve a folytonossági tervezésre és helyreállításra vonatkozó folyamatok tervezését és a tevékenység szabályozását.

Az új képesség sajátossága szerint részt kell venni a telepítésben, vagy a rendszer kialakítására vonatkozó szabályozás szerint a rendszert telepítés és beüzemelés után át kell venni (konfigurálása, biztonsági funkciók kialakítása, biztonsági beállítások telepítése vagy

ezek ellenőrzése és üzemeltetési felelősségének átvétele, beleértve az azonosításra és hitelesítésre vonatkozó adatok változtatását), valamint tanúsítani kell a védelmi rendszabályok megismerését és tudomásul vételét.

Ki kell alakítani a szükséges konfiguráció nyilvántartást, vagy ellenőrzés után át kell azt venni. Itt érdemes megjegyezni, hogy nem csak az anyagi elszámolásról van szó, mert például *a dokumentációhoz képest az eszközben lévő több memória nem jó üzleti érzéket, hanem a dokumentáció pontatlanságát, az átvétel felszínességét mutatja*, esetlegesen a működés során is paraméterek változtatását okozhatja. A felhasználó számára történő rendelkezésre bocsátás érdekében ki kell alakítani a szükséges hozzáférési profilokat, a hozzáférési jogosultság igénylésére vonatkozó hiteles eljárásokat.

A hadműveleti (alkalmazói) követelmények kielégítése érdekében ki *kell alakítani a folytonossági és helyreállítási terveket és a végrehajtásukra szolgáló szabályozást* a rendszer biztonságáért felelős személy által meghatározott biztonsági paraméterek szerint.

A rendszer használatba vétele érdekében *segíteni kell a felhasználók képzését, a védelmi rendszabályok elsajátítását*.

Az akkreditálás, jóváhagyás érdekében biztonsági teszt tervet kell kialakítani a rendszer biztonsági felelős személy szakmai támogatásával, majd dokumentáltan végre kell hajtani a tesztet.

Az előbbi feladatok elvégzése és az esetleges problémák elhárítása után utolsó feladat az akkreditáláshoz, jóváhagyáshoz szükséges adminisztrációban *a rendszer biztonságért felelős személy szakmai támogatása, illetve az eljárásban való részvétel*.

Az üzemeltetés során végzendő feladatok

A rendszer életének e szakaszában az üzemeltető feladata az üzemeltetési dokumentumok naprakészen tartása, meghatározott időszakonkénti felülvizsgálata, illetve a dokumentáció rendelkezésre bocsátása.

Gyakorlati feladat a rendszer folyamatos üzemeltetése, a szoftverkarbantartással kapcsolatos feladatok folyamatos ellátása (vírusvédelmi, anti-spam és egyéb védelmi szoftver frissítések, az operációs rendszerek frissítése, a szükséges kiegészítő programok telepítése és dokumentálása), valamint kapcsolattartás a rendszer biztonsági felelőssel, rejtjelzővel, összekapcsolás esetén a csatlakozó rendszer üzemeltető állományával.

Az üzemeltetési kérdések egyik legproblémásabb feladata *a rendszer felhasználói és rendszer biztonsági felelősi tevékenységének szakmai támogatása*, illetve technikai oldalon a rendszer hardver és szoftver konfigurációjának naprakészen tartása.

A rendszer átalakítás, továbbfejlesztése során egyedi feladat a rendszer biztonságáért felelős személy biztonságra vonatkozó hatásvizsgálatának támogatása.

Konfiguráció változtatáskor, vagy a rendszer kiterjesztésének engedélyeztetésekor el kell végezni a szükséges adminisztratív feladatokat, elő kell készíteni a változtatások engedélyezéséhez szükséges hatósági eljárásokat, majd a műveletek elvégzése után a változtatások át kell vezetni az üzemeltetési és a biztonsági dokumentumokban.

Ismétlődő feladat az időszakos kockázatelemzésben, az elfogadható kockázatoknak megfelelően *a kiegészítő védelmi rendszabályok kidolgozásában való részvétel*, illetve az újraakkreditáláshoz, jóváhagyáshoz szükséges üzemeltetési feladatok ellátása.

Mindenkori feladatnak kell tekinteni a biztonsági incidensek jelentését, majd szükség szerint közreműködést a helyreállításban, kivizsgálásban.

Ugyanígy folyamatos feladatnak kell tekinteni a felhasználók képzését és továbbképzését. A biztonsági tudatosságot erősítő feladatok során lapvető szakmai követelmény a rendszer biztonsági felelős szakmai támogatása.

Az azonosított feladatok nyilvánvalóan naprakész információkat igényelnek, melynek érdekében követelmény a meghatározott szakmai képzéseken, továbbképzéseken és biztonsági tájékoztatókon való részvétel.

A rendszerből történő kivonáskor végzendő feladatok

Az elektronikus adatkezelő rendszer, eszköz életútjának végén az eddigiekhez hasonlóan találhatók olyan feladatok, melyek félreértése, elhanyagolása vagy figyelmen kívül hagyása későbbi szervezeti hátrányokat okozhat kompromittálódás, vagy meglévő de alkalmazhatatlan, esetleg hiányzó adat formájában. Emiatt a felszámolási műveletek előkészítésének alapvető feltétele a helyzet megértése és a végzendő feladatok pontos tervezése.

Ennek része lehet a szükséges adatmentési, továbbítási, archiválási feladatok tervezése és végrehajtása, és az információs műveletek védelméhez szükséges rendszabályok pontosítása és érvényre juttatása.

Gyakran elfelejtett követelmény, hogy az adatkezelő rendszereknek nem csak a felhasználói adatait, hanem az elektronikus adatkezelő rendszer napló adatait is a minősítéssel illetve az adatok érzékenységével arányos követelmények szerint kell tárolni, archiválni.

Amennyiben olyan kivonás történik, melynek következtében a jövőben a mentett felhasználói adatok, vagy rendszeradatok olvasása nem biztosított, a szükséges információs környezet kialakításával kapcsolatos tervezői és végrehajtói feladatokat is a kivonáshoz kell számolni.

A rendszerből történő kivonás során általános feladat az adatok érzékenységével arányos törlési és megsemmisítési eljárások azonosítása és a szükséges eljárásrend kialakítása.

A rendszerből történő kivonás utolsó feladata a konfiguráció változási feladatok dokumentálása, jelentése.

Összefoglalás, következtetések

Az előzőek rávilágíthattak arra, hogy az életciklus szemlélet segíthet az elektronikus adatkezelő képességek biztonsági kérdéseinek azonosításában.

Fontos annak hangsúlyozása, hogy a szervezeti feladatok közötti eltérések, a rendelkezésre álló elektronikus adatkezelő szolgáltatások jelenleg nem teszik lehetővé a minden helyzetben érvényes rendszabályok kialakítását.

A fenyegetések és sebezhetőség megértése, a szükséges szabályozók alkalmazás szintű ismerete, a változások nyomon követése egyre nagyobb figyelmet kíván a végrehajtó személyektől.

A nemzetközi szakirodalom egy része magyarul nem áll rendelkezésre, a NATO, EU adatkezelő rendszerekre vonatkozó követelmények is angol nyelvűek, így nyilvánvaló az a szakmai követelmény is, hogy az elektronikus biztonsági kérdésekért felelős személyek képesek legyenek az angol nyelvű kommunikációra, ismerjék a szakkifejezéseket és azok pontos tartalmi jelentését. A korábbi jogszabályokban található „biztonsági megbízott”, a „Rendszer Biztonsági Utasítás”, a „rendszer üzemeltetés biztonsági felelős”, vagy a „megerősített iroda” már mint nem használatos kifejezések mutatják *a szakmai nyelv szükségszerű fejlődését*, *amit honvédelmi területen még ki kell egészíteni a katonai szakkifejezésekkel is.*

Az információvédelmi szakfeladatok üzemeltetési szakaszra érvényes meghatározása mellett kiemelt fontosságú annak megértése, hogy *az információvédelmi szakfeladatokra*

történő kiválasztással, kijelöléssel, képzéssel, illetve a kinevezés (vagy megbízás) visszavonással kapcsolatosan az életciklus különböző szakaszaihoz köthetően számtalan feladat azonosítható még.

A biztonsági menedzsment feladata, hogy az elektronikus adatkezelő képességek védelméhez szükséges *biztonsági feladatkörök azonosításakor a honvédelmi szervezeteknél átfedések, illetve felügyelet nélküli területek ne legyenek.*

A fentiek rámutatnak arra is, hogy a bonyolultabb elektronikus adatkezelő képességekkel rendelkező honvédelmi szervezeteknél *a biztonság kérdések kézbentartása előrelátást igénylő, bonyolult, erőforrás és időigényes tevékenység.* A honvédelmi szervezetek vezetői, biztonsági vezetői ezt a kihívást csak *a biztonsági kérdések komplex kezelésével, a szükséges ismeretekkel és jártassággal rendelkező személyekre támaszkodva menedzselhetik.*

A honvédelmi szervezetek szakirányú támogatását az át és továbbképzések rendszerében fokozatosan továbbfejlesztett szakmai követelmények szerint évek óta végzi a Zrínyi Miklós Nemzetvédelmi Egyetem. Az oktatott tananyag *gyakorlat centrikusan, a NATO és EU követelményekre támaszkodva készíti fel a honvédelmi szervezetek biztonsági és üzemeltető állományát.* A képzés eredményessége *a hatósági ellenőrzések és akkreditálási eljárások, NATO biztonsági ellenőrzések eredményein keresztül közvetlenül jelentkezik.*

Hivatkozások

[1.] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 9-10. §.

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

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

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

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

[6.] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról, 5. §. (3) és 6. §. (1)

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

[8.] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 49-51. §.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Kuris Zoltán
Zoltan.Kuris@irm.gov.hu

AZ EGYSÉGES DIGITÁLIS RÁDIÓRENDSZER (EDR) ALKALMAZÁSÁNAK LEHETŐSÉGEI A RENDÉSZETI SZERVEKNÉL

Absztrakt

Jelen közleményben az EDR rendészeti alkalmazásának gyakorlati tapasztalatai kerülnek kifejtésre. A publikáció néhány olyan problémára is rávilágít, amelyek alapvető kockázatokat rejtenek magukban. Ha ezeket a problémákat nem kezelik megfelelő súllyal, akkor azok (előbb vagy utóbb) rendelkezésre állási anomáliákat is okozhatnak a készenléti szervek feladat végrehajtásával összefüggésben.

In this paper the author explains the practical experiences of applying the EDR enforcement. Through the publication the attention also raised regarding some problems/difficulties, which have the chance for hidden risks. In case we do not make efforts to manage these problems/difficulties by adequate force, then they might cause (in shorter or longer time-period) availability anomalies linked to execution of the tasks of the defense police forces.

Kulcsszavak: *EDR, TETRA, kockázatok, rendelkezésre állás, készenléti szervek ~ EDR, TETRA, risk, availability anomalies, defense police forces*

BEVEZETÉS

Az információs társadalom kialakulása, a kritikus infrastruktúrákat veszélyeztető fenyegetések (természeti katasztrófák, balesetek, nemzetközi terrorizmus, szervezett bűnözés) egyre nagyobb kihívások elé állítják a különböző nemzeti és nemzetközi készenléti szolgálatokat. Ahhoz, hogy ezek a szervezetek minél hatékonyabban lássák el feladatukat szükséges, hogy a kommunikációs hálózatuk is megfeleljen a mai kor magas követelményeinek. De a civil szférának (szállítmányozás, közlekedés, építőipar) is szüksége van korszerű mobil kommunikációs rendszerekre, ezzel is fokozva versenyképességüket, hatékonyságukat.

A fentiekkel összefüggésben – a kutatási témámhoz kapcsolódóan – a releváns tudományos közlemények felhasználásával célszerű, a kritikus információs infrastruktúra egy infokommunikációs elemének pragmatikus elemzését végrehajtani.

A hazánkban működő készenléti szolgálatokat ellátó kommunikációs hálózatok többségében elavultak voltak, nyílt egycsatornás analóg - többségében URH - rádiórendszereket alkalmaztak, melyek továbbfejleszthetősége nem volt megoldott és nem nyújtottak megoldást a közvetlen és nagysebességű adatátvitelre (pl. adatbázisok lekérése).

Az operatív műveletek, melyek zömmel nagyvárosi környezetben, nyílt terepen zajlanak, megkövetelik a megfelelő valós idejű kommunikációt, koordinációt és eszközkövetést. A hazai rádiórendszereknél a fenti követelmények kielégítése nem volt megoldott úgy, mint a külföldön már bevált, fejlettebb trönkölt rádiórendszereknél.

Az igények kielégítésére az Egységes Digitális Rádió-távközlési rendszer – továbbiakban EDR – megvalósítására született határozat. Az EDR egy olyan kizárólag az ország érdekeinek és szabványainak megfelelő és annak készenléti szerveinek szolgálatába állított, valamint az Európai Unió által előírt Schengeni-kritériumoknak is megfelelő rendszer, amely alkalmas arra, hogy az Uniós csatlakozást követően is hatékonyan képes együttműködni a többi tagország készenléti rádiórendszerével. Ez a rendszer a mai kornak megfelelő technikai megoldásokkal és bővült szolgáltatásokkal segíti az ügyeleti – és járőrszolgálati munka elvégzését. Egyszerre hivatott felváltani az ügyeleti – és járőrszolgálati és szimplex rádiórendszereket, valamint használatban lévő a rádiótelefon (MRKB, Edacs) rendszereket.

Az értékelő elemzés tudományos célja, hogy a releváns közlemények és a gyakorlati tapasztalatok szintéziseként, objektív képet adjon arról, hogy ezek a rendszerek miként, – és ha nem akkor milyen hiányosságokkal – elégítik ki a különböző készenléti szolgálatok igényeit. Milyen fizikai és technikai megoldásokat használnak működésük során, és hogyan valósítják meg a velük szemben támasztott követelményeket. Ezt követően annak elemzését célszerű végrehajtani, hogy a személy és rendezvénybiztosítással összefüggésben, milyen – a biztonságos kommunikációt biztosító – megoldások alakultak ki, illetve váltak ismeretessé.

AZ EDR HAZAI MŰKÖDTETÉSÉNEK JOGSZABÁLYI ÉS MŰSZAKI KERETEI

Az Egységes Digitális Rádiórendszer, hazánkban 2007. február 1-től teljes kiépítettségében üzemel. A rádiórendszer működését és kötelező használatát az alábbi jogszabályi háttér teszi lehetővé.

A 109/2007. (V. 15.) Korm. rendelet az egységes digitális rádió-távközlő rendszerről, az alábbiakat írja elő.

„4§. (3) A Felhasználók mobil csoportkommunikációs távközlésüket - a honvédelemért felelős miniszter által felügyelt tábori (katonai) rádió-távközlő rendszerek kivételével - csak az EDR hálózati infrastruktúráján keresztül folytathatják [1]

7. § (1) Ez a rendelet a (2) bekezdésben foglalt kivétellel a kihirdetését követő 8. napon lép hatályba.

(2) A rendelet 4. §-ának (3) bekezdése 2008. július 1-jén lép hatályba.” [2]

1053/2005. (V. 26.) Korm. Határozat az egységes digitális rádió-távközlő rendszer (EDR) kialakításával, valamint az EDR szolgáltatás vásárlásával kapcsolatos feladatokról, rendelkezik.

„8.§. Az EDR szolgáltatás országos üzemszerű működésbe állásától számított három hónapon belül a Magyar Honvédség tábori (katonai) mobil rádiótávközlése kivételével valamennyi állami szerv készenléti mobil rádiótávközlésének kizárólagosan az EDR- re kell átállnia. Ennek érdekében fel kell gyorsítani a jelenlegi távközlési működtetési feladatot ellátó személyek és szervezeti egységek kiszervezését, a KVI bevonásával ki kell alakítani az infrastruktúra felhasználható elemeinek hasznosítására vonatkozó konstrukciót. Az azonos funkciójú, az államháztartáson kívül nem hasznosítható párhuzamos rendszereket le kell bontani.” [1]

A jelenlegi szabályzók szerint, az EDR használatára jogosult és kötelezett szervezetek [3]

- polgári titkosszolgálatok;
- katonai titkosszolgálatok;
- Igazságügyi és Rendészeti Minisztérium;
- Országos Rendőr-főkapitányság és alárendelt szervei;

- Országos Katasztrófavédelmi Főigazgatóság;
- Büntetés-végrehajtás Országos Parancsnoksága;
- Vám és Pénzügyőrség Országos Parancsnoksága;
- Honvédelmi Minisztérium;
- Magyar Honvédség;
- A Kormány kizárólagos rádió távközlő rendszerei üzemben tartásáért felelős állami szervek;
- Országos Mentőszolgálat.

Az EDR rendszer védelmi vezetéstechnikai tervezésének és gyakorlati alkalmazásának vizsgálatával összefüggésben célszerű tisztázni azt, hogy melyek azok az „üzemmódok" amelyeken keresztül a szolgáltatás megvalósul és a különböző funkciók elérhetővé vállnak, a felhasználók részére.

Közvetlen üzemmód (DMO): lehetővé teszi a tagállomások (terminálok) számára, hogy szimplex üzemmódban, minden infrastruktúra nélkül kommunikáljanak. Ez a képesség kiemelt fontosságú, mert olyan területeken teszi lehetővé a kommunikációt, amelyeket az infrastruktúra nem fed le (alagutak, hegyvidék, nagyobb kiterjedésű lakatlan területek, stb.) és elkerüli annak megterhelését kis körzetekre (5-10 km sugarú kör) kiterjedő üzemeltetés esetén. A készenléti szolgálatok bármely ágazati szerve kb. n x 10 db csatornát igényel. Tapasztalati tények viszont azt igazolják, hogy ezek az elvárások, túlzónak bizonyultak és a „különleges" operatív feladatokat ellátó egységek vezeték nélküli kommunikációjának tekintetében a közvetlen üzemmód alkalmazására alapozott híradás tervezése kommunikációs zavarokat okozhat.

Relézett üzemmód: ebben az esetben az állomások egyetlen hordozható csatornaismétlőn keresztül kommunikálnak. A relézett üzemmódot a közvetlen üzemmód helyett alkalmazzák viszonylag nagykiterjedésű területeken (30-40 km sugarú körben a frekvenciától, az antenna magasságtól függően). Ez a megoldás különösen bonyolult és kapacitás hiányos kommunikációs helyzetben teszi lehetővé az infrastruktúra egyszerű megerősítését. Ezzel kapcsolatosan az a gyakorlati tapasztalatok azt igazolják, hogy a „mozgó bázis állomás" igénybevétele hazánkban igen drága és nehézkes. Gyakorlatilag napokkal előtte kell igényelni a szolgáltatótól. Ez egy gyors reagálású rendészeti egységet figyelembe véve – különösen a rádiókommunikáció „alsó hálójában" - zavarokat okozhat. A csatornaismétlők alkalmazására DMO üzemmódban is van lehetőség. Ez ugyan megoldás lenne a helyi „alsó háló" kommunikáció biztosítására, de gyakorlatban azt tapasztalható, hogy ezek a (jelenleg elérhető) eszközök nem alkalmasak a probléma megoldására. Ugyanis nem homogén (városi épületen belüli és kívüli) környezetben kioltják egymást, vagy nem biztosítják a kellő lefedettségi paramétereket, gyakran a „hálózat nem elérhető" hibajelenséggel szakítják meg a kommunikációt.

Azonos idejű kisugárzás (simulcast): igen jó megoldást kínál a spektrumhatékonyság szempontjából egyes vidéki körzetekben, ahol a felhasználó-sűrűség nagyon csekély és a nyitott csatornák gyakran több adáshelyet szolgálnak ki.

A fent leírt üzemmódok biztosítják a különböző szolgáltatások elérését. A rendszer szolgáltatásai között található az alapvető beszéd alapú szolgáltatás. Ezt tekinthetjük a rendszer alapvető funkciójának is.

Az alapvető beszédalapú szolgáltatáson túl az EDR további beszédalapú szolgáltatásokra is képes. Ilyen szolgáltatás például a vészhívás, ahol elsődleges prioritást élvez a hívás, egy közvetlen kapcsolattal a diszpécserközpont, vagy kitüntetett csoport felé.

A másik ilyen szolgáltatás például a „Hook of" hívás, ahol előre meghatározott azonosítók, hívószámok használatával vagy a saját hálózatban, vagy egyéb külső hálózatba (PSTN, PABX, PBX, GSM) hívás kezdeményezhető.

Természetesen a digitális szolgáltatási mód adottságait kihasználva, más – az analóg rádiózáshoz képest - egyértelmű funkció kiterjesztést jelentenek a különböző adattovábbítási szolgáltatások.

Az adattovábbítási szolgáltatások közül az alábbiak emelhetők ki.

Adatüzenet továbbítása (Pl. SDS), ahol a felhasználó által bevitt rövid üzenetek küldhetőek a hálózaton belül.

Státuszüzenetek, előre definiált vagy egyénileg szerkeszthető szöveges üzenetek, melyek a felhasználó állapotáról tájékoztatnak (például: intézkedem, mentést hajtok végre, súlyos sérültet látok el, utasítást várok. stb.).

Csomagkapcsolt adatátvitel, ahol a hagyományos csomagkapcsolt üzenetküldési módon a lehető leghatékonyabb erőforrás felhasználással történik az adatforgalmazás.

A készenléti szolgálatok esetében az üzemi rendelkezésre állásnak kiemelkedően magas szintűnek kell lennie, mivel a hálózatokat a nap 24 órájában, az év 365 napján megszakítás nélkül üzemeltetik. Az alrendszerek ellenőrzési lehetőségeit maximális hatékonyságúra kell tervezni, nagyfokú hibatűréssel párhuzamosan. Szükséges a tartalék üzemmódok kialakítása is mivel a javítások, karbantartások során a kommunikáció nem szakadhat meg, a paraméterek csak minimális mértékben romolhatnak. A készenléti szolgálatoknál nagy tömegben kézi terminálokat használnak. Ebből az következik, hogy az operatív (különleges, rejtett VIP, vagy személyvédelmi, épületen belüli tűzoltási, stb.) feladatokat ellátó készenléti egységek vezeték nélküli kommunikációs lehetőségei jelenleg korlátozottak! Ugyanis hazánkban a szolgáltató országos lefedettséget kézi terminál vonatkozásában, nem köteles és nem is tud biztosítani! A jelenlegi helyzetet tovább bonyolítja, hogy az adatüzenet továbbításának fokozódó igénye nagy kihívások elé fogja állítani az infrastruktúrát és a szolgáltatót is. Ugyanis az adattovábbítással kapcsolatos (egyre fokozódó) igények igen súlyos kapacitás (egyben rendelkezésre állási) problémákat eredményezhetnek akkor, ha a szolgáltató nem hajtja (vagy nem tudja végrehajtani) a megfelelő kapacitásbővítést a jelenlegi infrastruktúrán.

Ugyanakkor, a rendszer biztonsági követelményei rendkívül széleskörűek, melyek kiterjednek a jogosultság-megállapítás, rendelkezésre állás, biztonságot érvényesítő funkciók, adatkezelés területeire. A hagyományos rendszerekkel összehasonlítva a készenléti szolgálatok hatékonyságával szemben jóval magasabb szintű követelményeket kell támasztani, például a Rendőrség és a Köztársasági Őrezred esetében. A biztonsággal kapcsolatos területek többsége – *a védelem fokozása okán* – nem írható le nyilvános szabványban, ugyanakkor a rögzítésnél a közcélú hálózatok jellemzőit is igénylik. Ilyen terület például a titkosítás, mely többek között a rendőrség esetében végponttól-végpontig kell (kellene), hogy megvalósuljon, szemben a hagyományos, polgári felhasználás elvárásaival. Ugyanis jelenleg ez a szolgáltatás (funkció) nem része a működő rendszernek, ezért például a prioritáskezelési funkciókhoz hasonlóan ezt a szolgáltatást a készenléti szolgálatok nem tudják igénybe venni, bár ezzel összefüggésben konkrét igények fogalmazódnak meg!

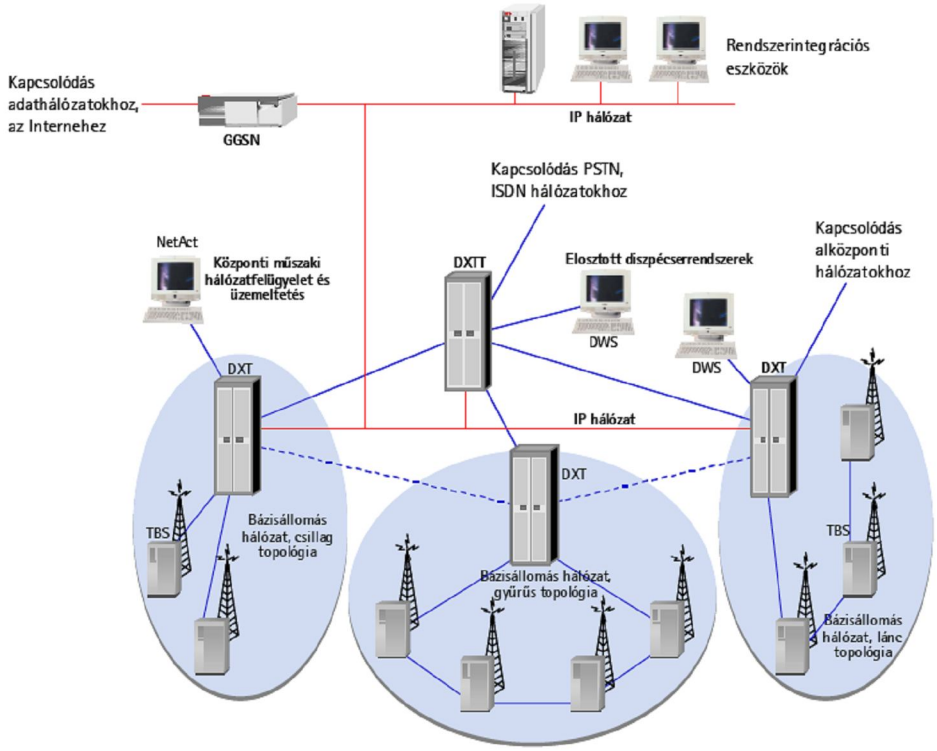
Az elvárásokat és követelményeket összefoglalva az újonnan létesítendő vezeték nélküli kommunikációs hálózatoknak az alábbi fő tulajdonságokkal kell (kellene) rendelkezniük.

- jó rádióellátottság, teljes körű (legalább 95%-os felszíni) lefedettség kézi terminál szinten;
- adattovábbítási lehetőség;
- könnyen ki- és átalakítható csoportkonfiguráció;
- a rádiócsatornákhoz történő gyors hozzáférés (optimális hívás felépülési idő);
- közvetlen üzemmódú működés, még épületen belül is legalább 1 Km-es körzetben;
- az infrastruktúra gyors telepíthetősége és felszerelhetősége;
- megbízható és a környezeti viszonyoknak ellenálló kézi - és mobil rádiókészülékek, utóbbiak gépkocsiba, vízi – és légi járműbe szerelhetőek legyenek;

- esetleges műszaki meghibásodás, természeti csapás vagy egyéb rendkívüli esemény esetén is a rendszerből kiesett, de még önálló kommunikációra képes átviteli elemek ellássák feladatukat.

AZ INFRASTRUKTÚRA BEMUTATÁSA

Az egyes felhasználói szervezetek az EDR rendszer használatában egy közös infrastruktúrán osztoznak, azonban minden szervezet, saját hálózati struktúráját szabadon, a többiektől függetlenül képes kialakítani és használni. Látszólag úgy viselkedik, mintha „saját" magánhálózata lenne és nem egy mindenki által használt közös hálózaton, kommunikálna. Ezt a tulajdonságot nevezzük virtuális magánhálózatnak, azaz VPN-nek (Virtual Privat Network). Minden egyes VPN a szervezeti struktúrának és alkalmazásnak megfelelően, hierarchikusan épül fel. A legnagyobb az „EDR VPN" az, amely magában foglalja a rendőrséget és a büntetés-végrehajtást is. Minden készüléknek önálló hívószáma van. A hívószámok hét jegyűek.



1. ábra A TETRA hálózat architektúrája és a hálózati elemei. [4]

Az objektumok védelmének vezeték nélküli kommunikációjára a védett személyek és [5] objektumok vonatkozásában az EDR rendszer megfelel a vele szemben támasztott követelményeknek, a működtetéssel probléma nem fordult elő. Nagyon jól érzékelhető a minőségi különbség az analóg rádiórendszerekhez képest. A védett objektumok őrszemélyzete önálló forgalmi csoportba rendezve, csak a saját forgalmazásukat hallják, más objektumokat ezzel nem zavarnak.

A személyvédelmi (operatív) tevékenység vezeték nélküli híradó biztosítása kapcsán elsősorban kézi terminálokkal történik a kommunikáció.

A Személyvédelmi feladatok ellátásához a hatvanas évek végén kiosztott 2 m-es analóg, keskenysávú FM frekvenciákat használták és használják a mai napig is. A személy-, és helyszínbiztosító állomány kézi és mobil rádió adó-vevőkkel kommunikál a hatótávolságon belül.

A szolgáltatók egy országban sem garantálják. hogy a digitális rádiórendszereik az ország mindenegyes pontján biztosítja a kézi terminálok működéséhez szükséges rádiófrekvenciás lefedettséget.

Magyarországon, azokon a lakott településeken ahol rendőrkapitányság működik, valamint az egy számjeggyel jelölt főutak mentén, illetve a határsáv 20 km-es körzetében garantált a kézi terminálok üzemeltetéséhez megfelelő lefedettség.

Mobil (gépkocsiban üzemelő, tetőantennával szerelt) terminál számára kisebb térerő is elegendő, jelen kiépítésben mobil terminálokat kb. Magyarország területének 94-96%-án lehet használni. A beszéd csoportban, egy időben csak egy felhasználó beszélhet. A sürgős szolgálati utasítást kiadó tagállomás nem tudja az üzenetet eljuttatni a többi tagállomásnak.

Az adási jogosultság megszerzéséhez az adás gomb folyamatos nyomva tartásával kell várakozni. Ha többen is várakoznak ilyen módon, akkor a beszédjogot a készülékek előre definiált prioritásának megfelelően, /jelenleg Magyarországon nem működik/ illetve a kéréseket sorba állítva osztja ki a rendszer. Ebből következik, hogy szélsőséges esetben hosszú másodperceket kell várakozni egy sürgős közlemény leadásához.

Az éppen folyó csoport forgalmazás megszakítására két lehetőséget nyújt az EDR rendszer. A kézi készülékek segélyhívó gombjának használata, melyre rendeltetéséből adódóan csak rendkívüli esetben kerülhet sor.

Az előjogos /preemptív/ hívásra jelenleg csak a diszpécsereknek van jogosultsága. A kézi terminálokon ezt az üzemmódot csak a még hiányzó prioritáskezelő szoftver biztosítaná.

Ha a hálózati szoftver a hazai EDR hálózaton rendelkezésre állna, akkor a pillanatnyi kommunikáció megszakítására az EADS gyártmányú THR880 típusú kézi terminálokon, egy külön nyomógomb szolgál, melynek megnyomása után az adás gomb használatával lehetne forgalmazni, egy külön nyomógombnak a konspiratív kezelőn történő működtetése nem megoldott.

A Magyarországon rendszeresített SEPURA gyártmányú kézi terminálóknál az adásgomb egyben a preemptív hívó gomb, ami csak a hálózati szoftver megvásárlása után lenne használható.

A Direct Mode Operation /DMO/ üzemmód lehetőséget nyújt preemptív hívásra. A SEPURA kézi terminálok úgy is programozhatóak, hogy a preemptív megszakításkérő gomb egyben az adásgomb. Jelenleg az ORFK részére erre a kommunikációs üzemmódra öt frekvencia lett kijelölve, három saját, kettő együttműködési.

Ha hálózati üzemmódról át kell állni DMO üzemmódra, akkor relatív nagy besugárzott terület esetén - például az objektumokban magas házak tetőire szerelt nagy nyereségű antennával forgalmazva -, problémaként jelentkezik, hogy ha a hatókörzeten belül az ORFK másik szervének csoportja forgalmaz ugyanazon a DMO frekvencián, akkor adás kezdeményezésekor a terminálok LCD kijelzőjén a „csatorna foglalt” felirat jelenik meg, az idegen tagállomás nem hallható, és nem kapcsol adásra a készülék.

EDR biztonság

Technológiájában az EDR, a világszerte mintegy 650 működő implementációval bíró Tetra rendszer Nokia – jelenleg EADS szállítású - hazai megvalósulása, mely technológia a felhasználók közötti zárt és biztonságos kommunikációval, nagyságrendekkel és minőségileg magasabb hatékonyságot, biztonságot, információvédelmet, egymástól való biztonságos csoport kommunikáció elkülönítést eredményez.

A bevezetett, készenléti és rendvédelmi rádió kommunikációs rendszer megakadályozza a korábbiakban tapasztalható illetéktelen hozzáférést, jogosulatlan lehallgatást, a bizalmasság, letagadhatatlanság sérülését, az illegális információ és adatfelhasználását.

Az EDR rádió-távközlő rendszerrel szemben különleges biztonsági követelményeket támasztottak a felhasználók és a megrendelő, elsősorban a felhasználói kör, az általuk végzett

szakmai feladatokkal kapcsolatos információk érzékenysége (annak ellenére, hogy minősített információk továbbítását a rendszerben nem tervezték), a rendszerben tárolt adatok védelmének, sérthetetlenségének, rendelkezésre állásának megőrzése érdekében.

Az EDR hálózat védelméhez alapvető nemzetbiztonsági érdek fűződik, ezért az EDR biztonságát szolgáló biztonsági követelményeknek való megfelelés egységes egyenszilárdságú rendszert alkot, mely kiterjed a rádiórendszeren túl a befogadó és működtető infrastruktúrára, az üzemeltető személyzetre, a szabályozási környezetre, a rendszerhez tartozó dokumentumokra és az iratok kezelésére is.

Hálózatbiztonsági szempontból felhasználói oldalon az azonosításai eljárások (csak ezen eljárás kötelező lefuttatása után vehet részt terminál a hálózat kommunikációjában) biztosítják az illetéktelen hozzáférés kizárását. Szolgáltatói szinten az informatikai rendszerek biztosítják a hálózati események helyének, idejének, módszerének, naplózását, visszakereshetőségét.

Információvédelem szempontjából az EDR rendszer származtatott, gyakran változtatott kulccsal védett kommunikációt valósít meg a terminálok és bázisállomások, a terminálok és a terminálok, terminálok és diszpécser munkaállomások között, a rendszerben alkalmazott, szabványosított rádiós interfész titkosítási algoritmussal (sem a titkosítási kulcs, sem az algoritmus hozzá nem férhető). A Nokia Tetra rendszer a világon elsőként kapta meg azt a szigorú biztonsági tanúsítást, miszerint biztonsága az automatikusan generált dinamikus rejtjelező kulcsokkal, megfelel a kormányzati és készenléti szervek által támasztott követelményrendszernek. Ez a titkosítási mechanizmus egyesíti a rádióterminálok hitelesítését a tartalom végponttól végpontig terjedő szabványos titkosításával.

A NOKIA terminálok belső funkcióihoz való hozzáférés elleni védelméről, az úgynevezett hardver kulcs és a benne lévő védett szoftver gondoskodik.

A hardver kulcs alkalmazása biztonsági kockázatot jelent, mivel nem kellően körültekintő védelme, felhasználása, illetéktelen jogosulatlan birtokolása a terminálok feltörését, a készülékek jellemzőinek megismerését eredményezheti. A terminálok, és a benne tárolt adatok biztonsága megköveteli, hogy a felprogramozott, adatokat tartalmazó, a hálózat használatára feljogosított terminál csak úgy kerüljön átadásra pl. javításra, hogy annak memória tartalma törlésre kerül. Javítást követően az újraprogramozásnál a biztonsági szabályokat kötelezően be kell tartani.

Az átviteli hálózat oldaláról a fő hordozó felület az optikai összeköttetés, alternatív független nyomvonalak tartalékként való biztosításával.

A hálózat felügyelet központosított, mely magas rendelkezésre állást biztosító felületen a hálózat konfigurálása, a riasztások kezelése, a műszaki, üzemeltetési adatok gyűjtése valósul meg.

Az EDR rendszerben kiemelt védelmet igényelnek a felhasználókhoz köthető, forgalmi adatok, a monitoring rendszerhez tartozó információk a jogosultságokat tartalmazó adatbázisok.

A rádió hálózat biztonsága mellett az EDR informatikai rendszer biztonsága is magas szintű követelményrendszernek felel meg a megfelelő informatikai biztonsági szabályozással, az informatikai felelősségek, jogosultságok, hozzáférések meghatározásával, az informatikai biztonság menedzselésével és tervezetten rendszeres auditálásával, az informatikai adatvagyon osztályozásával, az események naplózásával, visszakereshetőségével.

Mindenképpen ki kell térni az EDR infrastruktúrájának, a bázisállomások, a kapcsolóközpontok, a központi hálózatvezérlés biztonságára is.

Az EDR helyiségek kialakítását meghatározó biztonsági követelményrendszer, a szabotázsvédett, magas rendelkezésre-állású, folyamatosan működő, elektronikus behatolás jelző, beléptető, video megfigyelő és jelző, tűzjelző rendszer, a fizikai – mechanikai védelem és élőerős védelem összessége szolgálja a titok és vagyonvédelmi követelményrendszer megvalósulását.

Fentiek működését, felügyeletét a hálózat biztonsági infrastruktúrájának rendelkezésre állását menedzselő, a bekövetkező biztonsági eseményeket rögzítő és a szükséges intézkedéseket végrehajtó biztonság felügyeleti központ hivatott biztosítani.

A HÁLÓZATI LEFEDETTSÉG KITERJESZTÉSÉT TÁMOGATÓ, RÁDIÓFREKVENCIÁS ESZKÖZÖK

A DMO GATEWAY

A személyvédelmi alkalmazásban - DMO üzemmódban – a gateway gondoskodhat, akár az ország másik felén üzemelő vezető tagállomással való rádió összeköttetésről.

A tesztelés eredményei alapján megállapítható, hogy az egyes gyártók DMO getaway-i csak a saját gyártmányú kézi terminálokat támogatja. Az EADS nem gyárt gateway-t, a SEPURA kézi terminálok a repeater hatótávolságában automatikusan felkapcsolódnak a repeaterre. A Motorola terminálok tesztelésére eddig nem nyílt lehetőség.

A DMO REPEATER

A repeater feladata a DMO hatótávolság növelése. a Repeater a gateway-hez hasonlóan csak a saját gyártmányú kézi terminállal kompatibilis. Az EADS nem rendelkezik repeaterrel, a SEPURA eszközzel a saját terminálok összekapcsolódnak. A motorola repeater tesztelésére eddig nem nyílt lehetőség.



2. ábra. SEPURA SRG 3500 DMO repeater és gateway [6]

MOBIL BÁZISÁLLOMÁSOK

Előfordulhat, hogy katasztrófa helyzetben, vagy előre tervezhető rendezvények, nagygyűlések, esetleg előre nem tervezett demonstrációk biztosítása kapcsán, nagyszámú EDR terminál üzemeltetésére kerül sor egy helyen, egy időben.

A magyarországi szolgáltató a Pro-M Zrt. a hálózati lefedettség, vagy a hálózat kapacitásának kiterjesztésére - igény szerint - ideiglenes bázisállomásokat telepít. A Mercedes kamion alvázra szerelt mobil bázisállomás órákon belül kitelepülhet, a meglévő mikrohullámú és optikai gerinchálózaton keresztül becsatlakozhat a legközelebbi kapcsolóközpontba, ám ennek igen jelentős költségvonzata van.

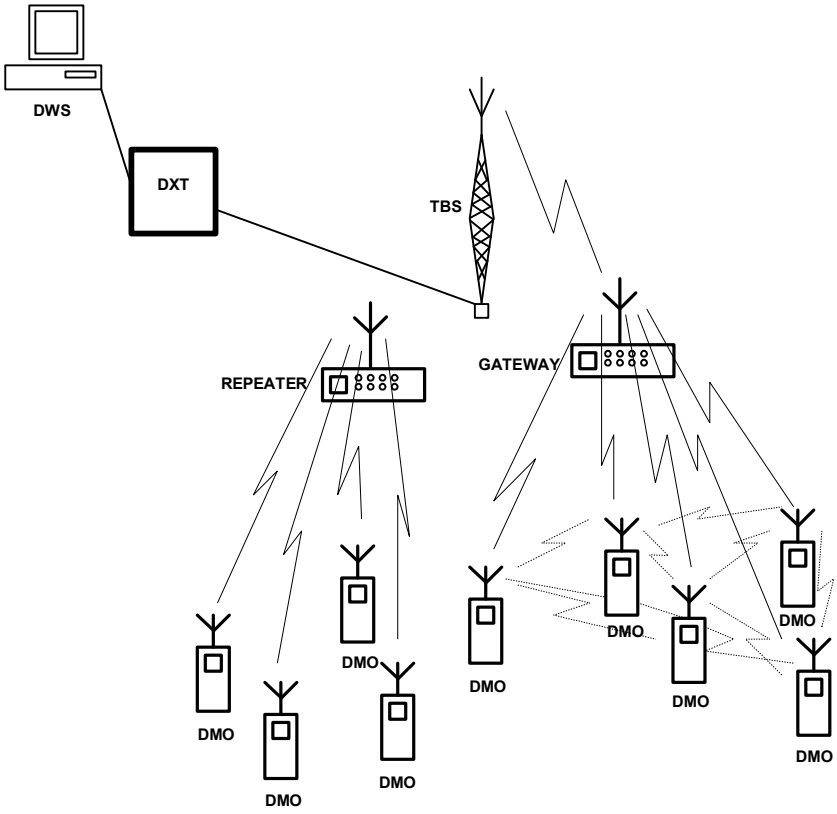
HÁLÓZATI HORDOZHATÓ REPEATER

A hálózati lefedettség kiterjesztésére a készenléti szervek a szolgáltatótól be tudnak szerezni hálózati repeatereket. Ezek a gépkocsiba telepített vagy hordozható berendezések egy közeli bázisállomás besugárzott területét terjeszti ki. Ezzel a megoldással hálózat lefedettsége növekszik, de a rendszer nagyobb területen tud, de csak ugyanannyi terminált kiszolgálni.

A DMO REPEATER ÉS GATEWAY EGYÜTTES HASZNÁLATÁNAK TAPASZTALATAI, A HÁLÓZATI LEFEDETTSÉGET KIBŐVÍTŐ RÁDIÓFREKVENCIÁS ESZKÖZÖK ALKALMAZHATÓSÁGA

A repeater és a gateway telepítésénél nagyon figyelmesen kell az eszközök pozícióját meghatározni annak érdekében, hogy minden kézi terminál elérhesse őket és igénybe tudja venni a szolgáltatást.

Ha egy helyszínen és egy időben kívánjuk alkalmazni SEPURA repeater-t és gateway-t akkor azt tapasztaljuk, hogy a kézi terminálok a számukra nagyobb térerővel rendelkező eszközzel összekapcsolódnak, és csak annak a szolgáltatását veszik igénybe. A problémát fokozza, hogy az így kettéosztott tagállomások egymással nem képesek kommunikálni.



3. ábra. A DMO repeater és gateway együttes használata (Kuris Zoltán)

AZ ANALÓG - EDR ÁTJÁTSZÁS LEHETŐSÉGE

A személyvédelmi feladatok kommunikációjában másodlagos, de nem nélkülözhetetlen a vezető tagállomással, és a biztosításban részt vevő rendészeti szervekkel való rádiófrekvenciás beszéd kommunikáció alapú együttműködés.

A gyakorlatban a személy, és helyszínbiztosító állomány, a tűzszerészek, - megfelelő digitális rádióháló hiányában- a hagyományos analóg rádiókat kénytelenek használni.

A biztosításban részt vevő gépjárművek ennek megfelelően analóg, és EDR rádiókkal is rendelkeznek. A rendészeti szervek napjainkra teljesen áttért az EDR használatára. A vezető tagállomás ezért egy időben kénytelen az analóg és az EDR rendszert is használni.

A két rendszer közötti átjárhatóság képes biztosítani a társszervekkel való együttműködést és a vezető tagállomással való kommunikációt. A helyi rádió forgalmazás rögzítéséről az EDR rendszer automatikusan gondoskodik, de azt átjátszóba beépítet korszerű hangrögzítővel is megoldható.

Az átjátszó berendezés feladata a biztosítási helyszíneken folyó analóg 2 m-es VHF rádió forgalmazás átjátszása egy tetszés szerinti védelmi szektorban üzemelő EDR / TETRA / forgalmi csoportra és vissza. A készülék felhasználási területe Magyarország. A készülék antennája lehetőség szerint kétsávos, duplexerrel közösített. Az antenna a gépkocsira könnyen telepíthető.

A szolgáltató Pro-M ZRt. igény esetén biztosít egy olyan mobil bázisállomást, amely V-SAT műholdas kapcsolat beiktatásával országon kívül is teljes értékű lefedettséget valósít meg egyetlen cellában. Az így telepített cella természetesen a gépjárművek követésre (AVL) is alkalmas. Az eszköz esetleges fejlesztését, és üzembe helyezését a hálózatgazdával és a szolgáltatóval együttműködve lehet, és kell végrehajtani!

Az átjátszóval szemben támasztott általános követelményeket az eddigi gyakorlati tapasztalatok felhasználásával, az alábbiak szerint célszerű összefoglalni.

- Az átjátszott hanginformáció késleltetése minimális legyen.
- Az átjátszó üzemszerű működése során a közölt hanginformáció nem veszhet el.
- A berendezés mobil kivitelű legyen, és kezelő személyzet nélkül gépkocsiba, vagy stabilan telepítve autonóm módon üzemeljen.
- Az antennák csatlakoztatására külön csatlakozó aljzatokon keresztül történjen.
- A tápellátás saját 12 V-os akkumulátorral legyen megoldva, melynek folyamatos töltése hálózati töltő berendezéssel, vagy a gépkocsi tápellátásáról történjen.
- Elvárt követelmény a pornak, párának, rázkódásnak, ütésnek ellenálló kivitel,

Nyilvánvalóan az analóg oldali követelmények sem hanyagolhatók el az átjátszó elem védelmi vezetéstechnikai rendszervezés folyamatában, melyeket az alábbiak szerint célszerű csoportosítani.

A készülék legyen alkalmas:

- a meghatározott frekvencia sávban szimplex összeköttetés biztosítására (4,5- 4,6 MHz duplex frekvenciatávolság kezelésére),
- CTCSS kóddal történő zavarvédelemre (enkóder, dekóder)
- üzemi frekvenciatartomány: 136-174 MHz,
- csatorna sávszélesség: 12,5/25 KHz,
- modulációs mód: F3 frekvenciamoduláció
- löketkorlát: 2,5 KHz (12,5 KHz raszter), 5 KHz (25 KHz raszter)
- programozható csatornák száma: min 5, a programozás 10 ; 12,5; 25 kHz-es raszter távolságokra legyen lehetséges.
- RF teljesítmény min. 20 W (programozható)
- Kis mechanikai méret
- Por, pára, rázkódás, ütés álló kivitel
- Time-out Timer funkció (adásidő korlátozás) programozható legyen
- Az EU szabványoknak megfelelő szomszéd csatorna elnyomással és szelektivitással rendelkezzen.
- A vevő érzékenység min. 0,35µV 12 dB SINAD
- EU szabványoknak megfelelő frekvencia stabilitással rendelkezzen

Az EDR oldali modul alapvető követelményeit az alábbi minimum követelményrendszer tartalmazza.

- A készülék feleljen meg az EDR /TETRA/előírásoknak
- A készülék lehetőség szerint kapcsolódjon az EDR rendszer saját GPS alapú műholdas gépjárműkövető rendszeréhez /AVL/, gondoskodjon a szükséges pozíció információk feldolgozásáról és a szolgáltató felé való továbbításáról
- Szabványos csatlakozásokkal rendelkezzen az EDR és VHF antennák részére
- Az interfész kis szintű, lehetőleg két oldali hangfrekvenciás kimenettel rendelkezzen
- Kezelőszervei egyszerűek és könnyen kezelhetőek legyenek
- Az átjátszó adó oldalai a vevők vételjelzéseire működjenek.
- A feléledési idő olyan kicsi legyen, hogy a rendszerből információ ne vesszen el.

Ezen túl alapvető forgalmi követelményeket is kell támasztani az alkalmazni kívánt átjátszó rendszerrel szemben.

A készülék legyen alkalmas:

- Adáskijelzésre, a forgalmi csoport nevének kijelzésére (az EDR rádión)
- A speciális adatrögzítőre való csatlakoztatására

Az antenna helyes megválasztása és kialakítása alapvető eleme a működő rendszernek, ezért az antenna SWR (állóhullám arány) érték a 136-174 MHz sávban és az EDR sávban kevesebb, legyen mint 1,5.

Egy lehetséges analóg- digitális átjátszó

A berendezés egy Motorola GM-340 VHF és Motorola TM-800E TETRA mobil rádióval működik. A vételjelzés SEPURA készülékben nem áll rendelkezésre, ezért VOX áramkör indítja az analóg rádióadást. Az analóg -EDR irányú átjátszás jó minőségű, késleltetés-mentes, de az EDR - analóg irányú beszéd átvitel feléledési ideje 400-500 ms, a VOX áramkör miatt, így a rádióforgalmazás első néhány szótagja elvész, nem kerül átvitelre. A hiba jelenség közvetlenül nem befolyásolja a helyszíni rádió forgalmazást, a tagállomások egymás közötti kommunikációjában, passzív vevő tagállomásként üzemel.

A vezető tagállomás a DWS /dispecher work station/ hálózati terminálja és az együttműködő EDR terminál forgalmazásában a rendelkezésemre álló tesztelésre szánt átjátszó feléledése problémát okozott.

ÖSSZEGZÉS

A jelenleg rendelkezésre álló nemzetközi összehasonlítást is figyelembe véve az a végkövetkeztetés vonható le, hogy a TETRA rendszert használó országok a hálózati lefedetlen területeken DMO üzemmódot használnak. A Magyarországon elvégzett tesztek eredményei alapján az analóg rendszerrel összehasonlítva DMO kézi terminál szintű kommunikáció használhatatlannak bizonyult.

Az azonnali kommunikáció lehetősége az érintett országokban a személyvédelmi állomány részére, valószínűleg rendelkezésre áll, ugyanakkor hazánkban a beszédelemre való várakozás, - a sorban állás - a forgalmazás információ tartalmának elévülését okozhatja.

Magyarországon az összes lehetséges műszaki követelményt és a megbízható, személy-. és helyszínbiztosítás igényeit kielégítő – a rádiófrekvenciás terjedés szempontjából mostoha körülmények, pl. hálózati lefedettség hiánya - a nagy biztonságú beszédkommunikáció EDR terminálokkal való megvalósítása jelenlegi, és a már teljesen kiépített hálózati lefedettséggel, a rendelkezésére álló EDR eszközökkel, a személyvédelmi feladatok biztonságos ellátására jelenleg nem alkalmas.

A kézi terminálok számára alkalmas 100%-os kültéri és beltéri lefedettség elméletileg megvalósítható, de - a jelentős költségek miatt – ennek megvalósítása aggályos.

Optimális megoldásnak jelenleg a két rendszer (analóg és digitális) egymás melletti üzemeltetése látszik, oly módon, hogy a társszervekkel való együttműködésre, és a vezető tagállomással való kapcsolattartásra a két önálló rádió hálózatot a biztosítási helyszíneken és a védett személyek mozgásának közvetlen környezetében összekapcsoljuk. Az átjátszó kísérleti példányának feléledési késleltetése gondot okozhat, de a kommunikációt nem veszélyezteti. A végső műszaki megoldásig az analóg rádiórendszer további üzemeltetéséhez szükséges jogi feltételek átmenetileg biztosítottak. Átmeneti megoldást jelenthet, ha az eredetileg a védelmi szférának kijelölt 2 m-es frekvencia sávban engedélyezett analóg frekvenciákat használhatná a személyvédelmi feladatok ellátása során az erre kijelölt szervezet. Ettől a sávtól eltérő frekvenciák kiosztása a jelenleg használt kézi és mobil rádiók teljes cseréjét vonná maga után, a gépjárművekbe való beépítés költségeivel együtt.

Az EDR szolgáltató nyitott a saját eszközeivel megvalósítható műszaki megoldásokra, közösen további megoldások keresésére van szükség.

Összességében elmondható, hogy hazai viszonylatban a rendészeti szerveknél –normál körülményeket figyelembe véve – jól vizsgázott az egységes digitális rádiórendszer. Mobil terminál tekintetében a hálózati lefedettség jónak mondható. A kézi terminálokkal kapcsolatosan már ugyanez nem jelenthető ki és a szolgáltató jelenleg nem is kötelezett ennek biztosítására. Az üzemszerű használatbavétel az ütemezéseknek megfelelően határidőn belül megtörtént. Budapesten a használatbavétel tapasztalatai kapcsán a rendszer teljesítette az előirányzott paramétereket. Budapesten az EDR használata nem okoz különösebb problémákat.

Ugyanakkor vidéki viszonylatban és az országos hatáskörű szervezetek, valamint a különleges feladatokat ellátó szervezeti egységek vonatkozásában felmerülhetnek, az üzemszerű működést zavaró tényezők. Ezek a problémák visszavezethetőek az országos kézi terminál lefedettség hiányára, a prioritáskezelő funkció hiányosságaira, illetve a hívás felépülési idővel kapcsolatos jelenségekre.

A titkosítással kapcsolatos megoldatlan problémák ugyan, konkrétan nem akadályozzák az üzemeltetést, de – különösen az adatátviteli üzemmód – vonatkozásában csökkenthetik a rendszer egyenszilárdságát.

Ugyancsak az adatátviteli funkciókkal kapcsolatos fokozódó igények vonatkozásában merülhet fel a kapacitás hiányos működési lehetőség, amelyből következően a beszédkommunikáció is sérülést szenvedhet, amennyiben a szolgáltató nem tartja szem előtt a fokozódó és komplex igénybevételből eredő és indukálódó infrastrukturális változásokat.

Irodalom

[1] 109/2007.(V.15.) kormányrendelet az egységes digitális rádió- távközlő rendszerről (DVD jogtár 2009. 10.26.)

[2] 109/2007.(V.15.) kormányrendelet az egységes digitális rádió- távközlő rendszerről (DVD jogtár 2009. 10.26.)

[3] 103/2005. (V.26.) kormányhatározat az egységes digitális rádió- távközlő rendszer (EDR) kialakításával, valamint az EDR szolgáltatás vásárlásával kapcsolatos feladatokról (DVD jogtár 2009. 10. 26)

[4] Az EDR, mint a készenléti szervek vezetésének hatékony eszköze ˙(5. o.)

[5] http://www.kutyu.hu/content/view/1160/6/ (2009.10.26.)

[6] http://www.ok.hu/katalogus?q=SEPURA+3500+&mode=1&hol=1

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Neszveda József
neszveda.jozsef@bmf.kvk.hu

AZ APERIODIKUSAN ALKALMAZOTT KATONAI BERENDEZÉSEK ELLENŐRZŐ TESZTJEINEK HATÁSA A MEGBÍZHATÓSÁG ÁLLAPOTVEKTORRA

Absztrakt

Az aperiodikusan alkalmazott katonai berendezések üzemelési életciklusuk alatt különböző (energiamentesen tárolt, periodikus teszt, feladatvégzés) üzemmódokban működnek. Üzemmód váltásokkor e berendezések hibaaránya ugrásszerűen változik. Az aperiodikusan alkalmazott katonai berendezések megbízhatóságát feladatvégzés üzemmódban az energiamentesen tárolt üzemmódot megszakító periodikus tesztek növelik. A hibaállapot vektorok diszkrét idejű vizsgálatkor a periodikus teszt a hibaállapot vektor korrekciójaként kezelhető. Ehhez korrigált átmenet-valószínűség mátrixra van szükség.

The aperiodic used military systems work in different (stored without energy, periodic test, task) mode during running lifecycle. The failure rates of these systems dramatically change at mode relay. The periodical test increases the reliability of the aperiodic used military systems on stored without energy mode. The periodical tests can be handled like correction of the error's state-vectors. It's needed the correction of the transition matrix.

Kulcsszavak: *periodikus teszt, hibaállapot vektor, átmenet-valószínűség mátrix ~ periodical test, error's state-vectors, transition matrix*

Bevezetés

Az aperiodikusan alkalmazott katonai berendezések tényleges feladatvégzése viszonylag rövid (1 – 10 nap) időtartamú és folyamatos üzemmódú. Két feladatvégzés között az eszköz hónapokig nem működik, az irányító berendezése energiamentesen tárolt állapotban van. A haditechnikai eszközök automatikus (autonóm felderítő robotrepülőgépek, mobilrobotok, egyszer használatos rádiólokációs zavaró berendezések, stb.), vagy félautomatikus (ember által távvezérelt bonyolult légvédelmi rakéta komplexumok, radarberendezések, távvezérelt robotok, stb.) berendezései gyakran ilyenek.

A feladatvégzések között periodikusan végzett ellenőrző teszt célja az üzemelés-megbízhatóság növelése. Az eltérő üzemmódok következménye, hogy az aperiodikusan

alkalmazott katonai berendezések λ meghibásodási hibaaránya nem állandó az üzembentartás életciklus[1] alatt.

Az aperiodikusan alkalmazott katonai berendezések irányítórendszer megbízhatóság analíziséhez a diszkrét idejű Markov analízis módszert választottam. Az előző [1] cikkemben már rámutattam az 1002D hardverstruktúrájú irányítórendszer előnyeire és a hét meghibásodás állapotot tartalmazó Markov gráf alkalmasságát a berendezés megbízhatóságának vizsgálatára.

Az energiamentesen tárolt állapotot megszakító ellenőrző tesztek esetén az IEC 61508 tesztlefedettség (DC) fogalma nem alkalmazható[2], ezért a szabványtól eltérően kell értelmezni a tesztlefedettség fogalmát. Az energiamentes állapotot megszakító ellenőrző teszt során a detektált hibák kijavításra kerülnek, ezért az ellenőrzött részegységek, és a műveletek aránya befolyásolja a teszt által detektálható hibák arányát. Ennek mértékét a C_M tesztlefedettség határozza meg. Hipotézisem szerint az aperiodikusan alkalmazott eszközökre a tesztlefedettség az irányítási rendszer ellenőrzött részegységei és műveletei, valamint az összes részegység és művelet hányadosa:

$$C_M = \frac{\sum \lambda_{0D}(\text{ellenőrzött részegység} + \text{ellenőrzött művelet})}{\sum(\text{részegység} + \text{művelet})} \qquad (1.)$$

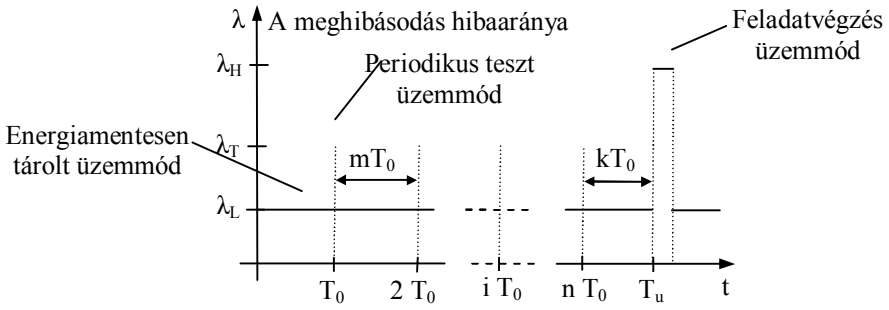
ahol a részegység a rendszer közös hibajellemzőkkel leírt része, a művelet a berendezés által a feladatvégzés üzemmódban megkívánt feladatsor, a λ_{0D} a detektált kezelhető és a detektált veszélyes hibaarányok összege.

Az állapotvektorok meghatározása diszkrét időpontokban

Legyen T_u a feladatvégzés megkezdődéséig eltelt idő:

$$T_u = (n \cdot m + k)T_0 \qquad (2.)$$

ahol T_0 a diszkrét idejű vizsgálat mintavételi ideje, „n” a periodikus tesztek száma, „mT_0” két teszt közötti energiamentesen tárolt állapot időtartama, és „kT_0” az utolsó teszt és a feladatvégzés kezdete közötti időintervallum.



1. ábra. Aperiodikusan alkalmazott katonai berendezések váltakozó hibaaránya

A berendezések hibaarányát normál üzemi körülményekre határozzák meg. Az 1. ábrán a normál üzemi körülmények a periodikus teszt üzemállapothoz tartoznak. Legyen ez a hibaarány λ_T. Szakszerű tárolás esetén az energiamentesen tárolt állapotban – a hőhatások és a

[1] Safety Lifecycle: Az IEC61508 szabvány [2] az üzembiztonság életciklus fogalma lefedi a tervezéstől, a rendszer vagy berendezés üzembe-helyezésén és üzemeltetésen át a szakszerű leszereléséig a megbízható működést szolgáló eljárások szabványos módszereit.

[2] A DC a szabvány definíciója szerint a detektált és az összes veszélyes hiba aránya.

mechanikai terhelések hiánya miatt – nagyjából egy nagyságrenddel[3] kisebb ($\lambda_L = h_L \cdot \lambda_T$) ez a hibaarány. A katonai berendezések feladatvégzés üzemelési körülményei általában megterhelőbbek a normálisénál, ezért ez a hibaarány ($\lambda_M = h_M \cdot \lambda_T$) nagyobb[4].

Amennyiben $\overline{\overline{T}}_L$ az energiamentesen tárolt, $\overline{\overline{T}}_T$ a periodikus teszt, és $\overline{\overline{T}}_M$ a feladatvégzés üzemmódhoz tartozó átmenet-valószínűség mátrix és a kezdeti hibátlan állapotot állapotvektora $\overline{S}(0) = [1 \quad 0 \quad ... \quad 0]$, akkor az első T_0 diszkrét időintervallumhoz tartozó hibaállapot vektort a 2. kifejezéssel határozhatjuk meg.

$$\overline{S}(1) = \overline{S}(0)\overline{\overline{T}}_L \tag{3.}$$

A hibaállapot vektor az első teszthez tartozó időperiódusban, amennyiben a berendezés hibamentesen üzemel teszt üzemmódban és ennek tényét sem vesszük figyelembe:

$$\overline{S}(m) = \overline{S}(0)\overline{\overline{T}}_L^{(m-1)}\overline{\overline{T}}_T \tag{4.}$$

Az előzőekhez hasonló feltételek mellett a feladatvégzés megkezdődésekor a hibaállapot vektor:

$$\overline{S}(m \cdot n + k) = \overline{S}(0)\left(\prod_{i=1}^{n} \overline{\overline{T}}_L^{(m-1)}\overline{\overline{T}}_T\right)\overline{\overline{T}}_L^{k} \tag{5.}$$

Az energiamentes állapotot megszakító tesztek célja a hibák felderítése, kijavítása, és így a meghibásodás-valószínűség csökkentése. Ezért az $(i \cdot m)T_0$ időperiódusokban a hibák felderítését és kijavítását modellező állapot-korrekciót kell megvalósítani, vagyis a 4. és 5. kifejezésekben a $\overline{\overline{T}}_L$ átmenet-valószínűség mátrix helyett $\overline{\overline{T}}_{korr}$ módosított átmenet-valószínűség mátrixot kell alkalmazni.

Bár a végső vizsgálatokhoz elegendő lenne az $\overline{S}(i)$ állapotvektorok diszkrét idejű sorozata, a 4. kifejezés korrekt meghatározása érdekében mégsem elegendő, hogy az $\overline{S}(i \cdot m)$ állapotvektort lecseréljük $\overline{S}_{korr}(i \cdot m)$ állapotvektorra. Ellenőrző tesztekkor a következő műveletsort kell végrehajtani:

$$\overline{S}(i \cdot m - 1) = \overline{S}(0)\overline{\overline{T}}_L^{(i \cdot m - 1)} \tag{6.a.}$$

$$\overline{S}(i \cdot m) = \overline{S}_{korr}(i \cdot m) = \overline{S}(0)\overline{\overline{T}}_{korr}(i \cdot m) \tag{6.b.}$$

$$\overline{S}(i \cdot m + 1) = \overline{S}(0)\overline{\overline{T}}_{korr}(i \cdot m) \cdot \overline{\overline{T}}_M \tag{6.c.}$$

A $\overline{\overline{T}}_{korr}(i \cdot m)$ átmenet-valószínűségmátrix időben változó érték és minden $i \cdot m \cdot T_0$ időintervallumban meg kell határozni. A $\overline{\overline{T}}_{korr}(i \cdot m)$ sorainak meghatározása:

- A $\overline{\overline{T}}_{korr}(i \cdot m)$ mátrix első sorának az $\overline{S}_{korr}(i \cdot m)$ állapotvektorral[5] azonos.

  Az, hogy a $\overline{\overline{T}}_{korr}(i \cdot m)$ állapotvalószínűség mátrix első sora megegyezik a $\overline{S}_{korr}(i \cdot m)$ állapotvektorral következik a 2. kifejezésből.
- A $\overline{\overline{T}}_{korr}(i \cdot m)$ mátrix második és harmadik sorai az eredeti $\overline{\overline{T}}_L$ állapotvalószínűség mátrix megfelelő sorai, de a tesztlefedettség tökéletlensége miatt az adott sornak megfelelően korrigálni kell.

[3] A közel három évtizede gyűjtött FARADIP eszköz meghibásodási adatbázis alapján.

[4] Ugyancsak a FARADIP eszköz meghibásodási adatbázis alapján, az üzemelés körülményeitől függően, kétszeres és négyszeres érték között ilyenkor a hibaarány.

[5] Az $\overline{S}_{korr}(i \cdot m)$ állapotvektor kiszámításának módszerét a következő fejezetben mutatom be.

A teszt során vagy az derül ki, hogy nincs ebben a hibaállapotban a rendszer, vagy ha mégis akkor a hiba kijavításra kerül. A tesztlefedettség tökéletlensége miatt nem áll helyre az eredeti állapot. A hibavalószínűségeket a kiindulási állapothoz képest konstans $1+(1-C_M)$ tényezővel kell felszorozni. A második sorhoz szükség van az $\overline{I2} = [0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]$, a harmadik sorhoz az $\overline{I3} = [0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0]$ segédvektorokra.

2. sor: $\overline{\overline{T}}_{korr}[2,:] = (\overline{\overline{T}}_L - \overline{I2}) \cdot (2 - C_M) + \overline{I2}$ (7.a.)

3. sor: $\overline{\overline{T}}_{korr}[3,:] = (\overline{\overline{T}}_L - \overline{I3}) \cdot (2 - C_M) + \overline{I3}$ (7.b.)

- A $\overline{\overline{T}}_{korr}(i \cdot m)$ mátrix negyedik és ötödik sorai megegyeznek a $\overline{\overline{T}}_L^{(i \cdot m)}$ mátrix negyedik és ötödik sorával.
  A hét hibaállapotot tartalmazó modellben [1] a negyedik és az ötödik állapot a kezelőszemélyzet számára felderítetlen marad, ezért a $\overline{\overline{T}}_L^{(i \cdot m-1)} \cdot \overline{\overline{T}}_L$ mátrixszorzat és a $\overline{\overline{T}}_{korr}$ korrigált állapotvalószínűség mátrix negyedik és az ötödik sora nem különbözhetnek egymástól.
- A $\overline{\overline{T}}_{korr}(i \cdot m)$ mátrix hatodik és hetedik sorai az eredeti $\overline{\overline{T}}_L$ állapotvalószínűség mátrix megfelelő soraival egyeznek meg.
  A hét hibaállapotot tartalmazó modellben a hatodik és hetedik állapot nyelő típusú. Ha az ellenőrző teszt közben a rendszer ezek az állapotok valamelyikébe kerül, akkor működésképtelenné válik, vagyis a hiba nem maradhat rejtve! Ezért a javítás utáni állapot az eredeti $\overline{\overline{T}}_L$ állapotvalószínűség mátrixnak megfelelő.

Az állapotvektor korrekció

Az energiamentesen tárolt állapotot megszakító periodikus teszt üzemmódban a hiba észlelését és javíttatását az állapot-valószínűségek korrekcióival kell figyelembe venni. A valószínűségállapotok korrekciójára, vagyis az $\overline{S}_{korr}(i \cdot m)$ hibaállapot vektorok meghatározására az egyik tanulmányomban **Hiba! A hivatkozási forrás nem található.** már a következő javaslatot tettem: a detektálható hibás állapotok korrekciója a hibaállapotok előfordulás valószínűségével súlyozottan történjen. Mivel csak statisztikai valószínűség adható meg, hogy melyik hibaállapot milyen valószínűséggel következik be, ezért a sikeres működés valószínűsége a hibaelhárítás okozta átlagos javulás mértékével emelkedjen meg és ennek megfelelően a hibás állapotok valószínűsége együttesen az átlagos javulás mértékével csökkenjen.[6]

Matematikailag ez a következőképpen valósítható meg: legyen az $\overline{S}_x$ sorvektor elemei azon állapotok, amelyekben a kezelőszemélyzet a $(m-1)T_0$ időtartam eltelte után végrehajtott teszt közben hibát észlelhet és $\overline{V}_x(i \cdot m) = \overline{S}_x(i \cdot m) - \overline{S}_x(1)$ a hibaállapotok mT_0 időpontban és az üzembe helyezéskor létező hibavalószínűségük különbségei, vagyis $\overline{V}_x$ a maximális javíthatóság sorvektora:

$$\overline{V}_x(i \cdot m) = [S_2(i \cdot m) - S_2(1) \quad S_3(i \cdot m) - S_3(1) \quad S_6(i \cdot m) - S_6(1) \quad S_7(i \cdot m) - S_7(1)] \qquad (8.)$$

[6] Megjegyzés: Az elvégzett teszt alatt csak egy konkrét hibaállapotba kerülhet az eszköz. A fenti javaslat ezt úgy veszi figyelembe, hogy a hibaállapotok az előfordulásuk valószínűségének megfelelően vannak súlyozva, vagyis azt a trivialitást feltételezi, hogy az üzemelési élettartam alatt a hibavalószínűségeknek megfelelő gyakorisággal fordulnak elő a hibák. [4]

A $\overline{V}_x(m) = \left[v_{x1} \quad v_{x2} \quad \cdots \quad v_{xx} \right]$ sorvektor x darab elemének átlagértékét (v_{xavg}) meghatározva a $v_{xavg}(m)$ átlagos javulás mértéket kapjuk meg. Az mT_0 időintervallumokban végrehajtott teszt által feltárt hibák kijavítását követően következik be a berendezés átlagos javulása. Az átlagos javulás mértéke a kezdeti állapot helyreállítását feltételezi, ezért az értékét módosítja a C_M tesztlefedettség.

$$v_{xavg}(k) = \frac{C_M}{x} \mathrm{Sum}\left\{ V_x(k) \right\} \tag{9.}$$

ahol az x azon állapotok száma, amelyben a kezelőszemélyzet hibát észlelhet.

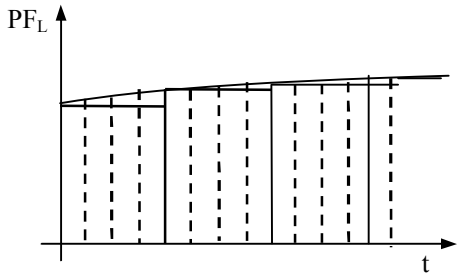
Ennek megfelelően a hét összevont hibaállapotot tartalmazó, 1002D hardver struktúrájú irányítási modell esetén a kezelőszemélyzet által kT_0 időtartam eltelte után végrehajtott teszt során észlelt $\overline{S}_x$ hibaállapot és $\overline{V}_x$ maximális javíthatóság sorvektor a következő:

$$\overline{S}_x(k) = \left[S_2(k) \quad S_3(k) \quad S_6(k) \quad S_7(k) \right] \tag{10.a.}$$

$$\overline{V}_x(k) = \left[S_2(k) - S_2(1) \quad S_3(k) - S_3(1) \quad S_6(k) - S_6(1) \quad S_7(k) - S_7(1) \right] = \\ = \left[v_{x1}(k) \quad v_{x2}(k) \quad v_{x3}(k) \quad v_{x4}(k) \right] \tag{10.b.}$$

Tekintve, hogy az irányítási rendszer energiamentes állapotát megszakító periodikus teszt rövid a két teszt közötti mT_0 időintervallumhoz képest, megfelelő időalap választással a sikeres működés illetve az állapotok hibavalószínűségének korrekciója egyetlen időintervallumban bekövetkező változásként vehető figyelembe.

A periodikus tesztekkel megszakított, energiamentesen tárolt üzemállapot több hónapig, esetleg évekig tart. A T_0 $[h^{-1}]$ időalap alkalmazásával több ezer $\overline{S}(k)$ állapotvektort kell kiszámítani úgy, hogy a $\overline{\overline{T}}_L$ átmenet valószínűségmátrix értékei nagyon kicsik. A kerekítési problémák miatt a $\overline{\overline{T}}_L$ átmenet valószínűségmátrix elemeit duplaszó formátumúra kell választani. A duplaszó formátumú, nagyon nagyméretű mátrixszal végzett műveletek komoly számítási erőforrást igényelnek.



2. ábra. Az időalap konverzió hibája

(Készítette: Neszveda József)

A PF_L hibavalószínűség diszkrét idejű kiszámítása integrálszámítás jellegű (2. ábra). Az energiamentesen tárolt állapotban nagyjából egy nagyságrenddel csökken a λ hibaarány a folytonos üzemelés üzemmódhoz képest, ezért $PF_L(t)$ időbeni változása lassúbb. Ennek következtében az 1 óránál nagyobb időlépték választás, vagyis egy napos időalapra történő időkonverzió okozta hiba elhanyagolható.

Egy nap még modulcserével megvalósítható kisebb javításokkal együtt is elegendő az időszakos teszt végrehajtására. Ez az időalap választás csökkenti a túlságosan kis számértékeknél fellépő kerekítési problémát, és egyben összhangban van az időszakos teszt egyetlen időperiódusban végrehajthatott állapot-korrekcióként való kezelésével. Ezért

vezessük be az egynapos (T_N = 24 [h]) időegységet a periodikus tesztekkel megszakított, energiamentesen tárolt állapot vizsgálatára. Az időegységváltás hatása a hibaarányra:

$$\lambda_N\left[\frac{1}{24}h^{-1}\right] = h_N \cdot \lambda_H\left[h^{-1}\right] \qquad (h_N = 24.) \tag{11.}$$

Az mT_0 időintervallumban végrehajtott teszt által feltárt hibák kijavítása következtében a [1] cikkben megadott modell hét állapotának hibavalószínűség változásait egyetlen időperiódusként kezelve a korrigált állapot-valószínűség értékek a következők:

$$S_1(m) = S_1(m-1) + v_{xavg}(m) \tag{12.a.}$$

$$S_2(m) = S_2(m-1) - v_{xavg}(m)\frac{S_2(m-1)}{S_2(m-1)+S_3(m-1)+S_6(m-1)+S_7(m-1)} \tag{12.b.}$$

$$S_3(m) = S_3(m-1) - v_{xavg}(m)\frac{S_2(m-1)}{S_2(m-1)+S_3(m-1)+S_6(m-1)+S_7(m-1)} \tag{12.c.}$$

$$S_4(m) = S_4(m-1) \tag{12.d.}$$

$$S_5(m) = S_5(m-1) \tag{12.e.}$$

$$S_6(m) = S_6(m-1) - v_{xavg}(m)\frac{S_2(m-1)}{S_2(m-1)+S_3(m-1)+S_6(m-1)+S_7(m-1)} \tag{12.f.}$$

$$S_7(m) = S_7(m-1) - v_{xavg}(m)\frac{S_2(m-1)}{S_2(m-1)+S_3(m-1)+S_6(m-1)+S_7(m-1)} \tag{12.g.}$$

A 12.a. kifejezés a sikeres működés átlagos javulását tartalmazza. A 12.d. és a 12.e. kifejezésekből következik, hogy az S_4 és S_5 állapot-valószínűség értékek nem változnak.

A 12.b., 12.c., 12.f., és 1.2.g. kifejezések tartalmazzák a meghibásodás valószínűségek súlyozott csökkenését. Ezekben a kifejezésekben szerepel az $\overline{S}_x(k)$ sorvektor sorösszege. Ezért a további számításokhoz célszerű ezt meghatározni:

$$s_x(m) = \mathrm{Sum}\left\{\overline{S}_x(m)\right\} \tag{13.}$$

Behelyettesítve az $s_x(k)$ értékét azon 12. kifejezésekbe, amelyek a korrekció következtében változnak, majd rendezve azokat a következő sorvektor elemeket kapjuk:

$$S_1(m) = S_1(m-1) + v_{xavg}(m) \tag{14.a.}$$

$$S_2(m) = S_2(m-1)\left\{1 - \frac{v_{xavg}(m)}{s_x(m)}\right\} \tag{14.b.}$$

$$S_3(m) = S_3(m-1)\left\{1 - \frac{v_{xavg}(m)}{s_x(m)}\right\} \tag{14.c.}$$

$$S_6(m) = S_6(m-1)\left\{1 - \frac{v_{xavg}(m)}{s_x(m)}\right\} \tag{14.d.}$$

$$S_7(m) = S_7(m-1)\left\{1 - \frac{v_{xavg}(m)}{s_x(m)}\right\} \tag{14.e.}$$

Az algoritmizálhatóság érdekében vezessük be a sikeres működés valószínűségének átlagos növekedését tartalmazó $\overline{V}(k)$ vektor-változót.

$$\overline{V}(m) = \left[v_{xavg}(m) \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0\right] \tag{15.}$$

A periodikus teszt állapot-konverzióját leíró 3.24.b … 3.24.e kifejezésekhez most vezessük be a hibaállapotban maradás csökkenő valószínűségét tartalmazó $\overline{W}(k)$ vektorváltozót:

$$\overline{\overline{W}}(m) = \begin{bmatrix} 1 & wa(m) & wa(m) & 1 & 1 & wa(m) & wa(m) \end{bmatrix} \quad (16.)$$

ahol a 14. kifejezésekben szereplő $wa(m) = 1 - \frac{v_{xavg}(m)}{s_x(m)}$ érték.

A végrehajtott teszt során észlelt hibák kijavítása után bekövetkező állapotkorrekció utáni $\bar{S}_{korr}(m)$ állapotvalószínűség vektor az alábbi vektorművelet formulával számítható:

$$\bar{S}_{korr}(m) = \left\{ Diag\left(\overline{\overline{W}}^{T}(m) \bar{S}(m-1) \right) + \overline{\overline{V}}^{T}(m) \right\}^{T} \quad (17.)$$

Az átmenet-valószínűség mátrix konvertálása

Amennyiben $\overline{\overline{T}}_1$ átmenet-valószínűség mátrix nem tartalmaz μ helyreállítási arányt[7], és a λ hibaarány ugrásszerű változását egy $\overline{\overline{T}}_1$ átmenet-valószínűség mátrix elemein akarjuk érvényesíteni, akkor az $\bar{\bar{I}}$ egységmátrixot kivonva a $\overline{\overline{T}}_1$ átmenet-valószínűség mátrixból a $\overline{\overline{P}}_1$ meghibásodás-valószínűség mátrixot kapjuk. Beszorozva $(\overline{\overline{P}}_1 \cdot \lambda)$ kapjuk az új $\overline{\overline{P}}_2$ meghibásodás-valószínűség mátrixot, amihez az $\bar{\bar{I}}$ egységmátrixot hozzáadva megkapjuk az új $\overline{\overline{T}}_2$ átmenet-valószínűség mátrixot.

$$\overline{\overline{T}}_2 = \left(\overline{\overline{T}}_1 - \bar{\bar{I}} \right) \cdot \lambda + \bar{\bar{I}} \quad (18.)$$

A 18. kifejezéssel megvalósítható a váltás a $\overline{\overline{T}}_T$ és a $\overline{\overline{T}}_L$ átmenet-valószínűség mátrixok között.

A számítási erőforrás igény csökkentése

A 6. kifejezés alkalmazása az $\bar{S}(k)$ állapot-vektorok kiszámításához nagy számítógépes erőforrást igényel. A számítási kapacitásigényt nagymértékben csökkenti a rekurzív formula alkalmazása.

$$\bar{S}(i) = \bar{S}(0) \overline{\overline{T}}^{i} \quad (19.a.)$$

$$\overline{\overline{T}}(i) = \overline{\overline{T}}^{i} \quad (19.b.)$$

$$\overline{\overline{T}}^{i} = \overline{\overline{T}}(i) \overline{\overline{T}} \quad (19.c.)$$

A periodikus ellenőrző tesztek gyakoriságának és a teszt lefedettségének optimalizálása, ami a folytonos üzemű technológiákra már megoldott volt [6], a 6., 17., 18., 19. kifejezésekkel és a $\overline{\overline{T}}_{korr}(i \cdot m)$ sorainak meghatározásának szabályaival megvalósítható.

[7] Ha figyelembe kell venni a μ helyreállítási arányt, akkor az $\bar{\bar{I}}$ egységmátrix helyet egy olyan $\overline{\overline{N}}$ mátrixot kell alkalmazni, amelynek főátlója csupa 1-es és a megfelelő pozíciókban tartalmazza a μ helyreállítási arányt.

Irodalom

[1] Neszveda, József: *Numerikus modell IMET eszközök megbízhatósági szintjének vizsgálatára* ZMNE, Hadmérnök, 2008. III. évf. 4. szám.

[2] IEC 61508. *Functional safety of Electrical/Electronic/Programmable electronic Safety-Related Systems*, 1998.

[3] Neszveda, József: *Safety Lifecycle of Intermittently Operated Device*, Academic and Applied Research in Military Science, Volume, Issue, 2009.

[4] Smith, David J.: *Reliability, Maintainability, and Risk: Practical Methods for Engineers*. 6th edition. Butterworth-Heinemann, 2001, ISBN: 978-0-7506-6694-7

[5] MATHWORKS, INC: "*Matlab 2008b HELP"*, 2008.

[6] Torres-Echeveria, A.C., Martorell, S., Thompson, H. A.: *Modeling and optimization of proof testing policies for safety instrumented systems,* Elsevier Journal: Reliability Engineering and System Safety, 2009.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Serege Gábor
serege@t-online.hu

A TECHNOLÓGIAI KONVERGENCIA FOLYAMATA ÉS HATÁSA A CELLÁS MOBIL HÁLÓZATOK FEJLŐDÉSÉBEN

Absztrakt

A konvergencia folyamata napjaink egyik meghatározó megatrendje. Eltérő területeket összeolvasztó hatása megkérdőjelezhetetlen tény a telekommunikáció fejlődésében. A mobil telefonálásra létrehozott rendszer képessé válik adattovábbításra, illetve az adatátvitelre kifejlesztett hálózaton is kezdeményezhetünk telefonbeszélgetést. A cellás mobil hálózatok generációin keresztül jól megfigyelhető a híradás és informatika határainak összeolvadása, amely eredményeként új szolgáltatások válnak elérhetővé. A kinyíló lehetőségekkel együtt azonban új biztonsági fenyegetések is előtérbe kerülhetnek.

The convergence is one of the main megatrend at the present. It has an undoubtful influence on connecting process in the evolution of telecommunications. The sytem has established for manage mobile phone calls is getting able to transfer data, respectively we could give a call on the network that has worked up for transferring data. Inspecting the different generations, we could realise to disappear the margin between telecommunication and informatics. This evolution both provides new facilities and risks too.

Kulcsszavak: *GSM, konvergencia, híradás, informatika, biztonság ~ GSM, convergence, communications, informatics, security*

BEVEZETÉS

A XVII. századtól vizsgálva az emberiség történelmében bekövetkezett jelentős változásokat megállapítható, hogy azok számos esetben valamilyen típusú forradalomhoz köthetők. Ez az esemény jelenthetett egy adott országhoz kapcsolódó népfelkelésekkel egybekötött, évekig elhúzódó, radikális átalakítást, esetleg egy gyors lefolyású fegyveres felkelést, vagy épp valamilyen alapjaiban megváltozó kulturális, gazdasági, informatikai megújulást. Hahner Péter tanulmánya szerint a mai értelemben használt forradalom jelentése egyenértékű a változás fogalmával. [1]

Véleményem szerint a mindennapi életünket behálózó, országokat, földrészeket összekötő telekommunikáció az információs forradalom kiemelkedő eredménye, amelyet a folytonos fejlődéssel, összetettebb rendszerekkel, előremutató változással lehet jellemezni. A magasabb technológiai szintű komplex rendszerek célja, hogy a szolgáltatások minél szélesebb körű kibővítése mellett, a felhasználói igények maximális kielégítése a kezelői környezet egyszerűsödésével valósuljon meg. A cél elérése érdekében a különböző szakterületek között a szigorúan vett határvonalak elmosódnak. A beszéd (hang) átvitelére kifejlesztett híradó hálózatok adatot továbbítanak, míg az adattovábbításra létrehozott informatikai rendszereken a hangátvitel vált elérhető szolgáltatássá. Ez a technológiai evolúciós folyamat a konvergencia. [2]

Az elmúlt két évtizedben az információs technológia a világ vezető iparágává nőtte ki magát. A fejlett társadalmakban az számít meglepőnek, ha valaki hagyományos térképpel nem GPS[1] támogatással vág neki egy hosszú útnak, találkozóit papíralapú zsebnaptárban és nem PDA[2] készüléken tartja nyilván, vagy épp nem rendelkezik mobiltelefonnal. Ezt a felsorolást hosszasan folytathatnám, amiből nyilvánvalóvá válna, hogy az információs technológia nem csak egyszerűen az életünk egy része, hanem nagymértékű elterjedtségéből, illetve gazdasági befolyásából adódóan az életünk egy meghatározó tényezője.

Az infokommunikációs technológia alkalmazásából adódó előnyök mellett nem szabad megfeledkezni a széleskörű elterjedésből és függőségből származó biztonsági kockázatokról sem. A vonatkozó jogszabály besorolása alapján a mobil kommunikációs hálózatok szerves részét képezik a Magyar Köztársaság kritikus információs infrastruktúrájának.[3] Ebből következik, hogy működésképtelenné válása vagy megsemmisülése jelentősen befolyásolná a nemzet-, illetve az állampolgárok élet- és vagyonbiztonságát.[4]

Áttekintő elemzésemben a szakterületen született írásos művek alapján kívánom bemutatni a konvergencia folyamatát és hatását a rendszer biztonsága szempontjából. Célom, hogy egy rövid betekintést nyújtsak a különböző generációk technikai fejlődésébe és az adott szinthez tartozó kockázati tényezőkbe. Továbbá követve a fejlesztési trendeket, előre kívánom vetíteni a jövő hálózatát fenyegető biztonsági kérdéseket.

A TECHNIKAI ÚJDONSÁGOK VESZÉLYÉRŐL

Az elmúlt 11 évet tekintve a magyar társadalmat is szinte robbanásszerűen hódította meg a mobil telekommunikáció. Az ezredforduló küszöbén mintegy 1,1 millió mobilkészülék talált gazdára, még 2008-ban ez az érték meghaladta a 11 milliót. [3] Természetesen az eladott készülékek mennyisége nem tükrözi pontosan a szolgáltatást ténylegesen igénybe vevők számát, azonban joggal feltételezhető, hogy a társadalom több, mint 60%-a intézi ügyeit a zsebben lapuló készülékkel. A kereskedelmi szolgáltatást gyakorlatilag bárki használhatja, aki képes megfizetni annak fenntartási költségeit, ezért érdemes végiggondolni a felhasználók lehetséges táborát. Véleményem szerint a legnagyobb csoportot a „békés civil” lakosság jelenti. Ezt követi az állami szféra dolgozóinak a szolgálati és privát jellegű felhasználói, míg a harmadik csoportba sorolnám azokat, akik a szolgáltatást illegális tevékenységek megszervezésére veszik igénybe, vagy épp a célszemélyhez (csoporthoz) kiépített infokommunikációs csatornán keresztül indítanak támadást.

[1] Global Positioning System: Globális Helymeghatározó Rendszer
[2] Personal Digital Assistant: Digitális Személyi Titkár
[3] 2080/2008. (VI.30.) Kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról
[4] A kritikus információs infrastruktúrák pontos meghatározását a 27/2004. (X.6.) IHM rendelet tartalmazza

A Szovjetunió és a VSZ széthullása megszüntette a bipoláris katonai szembenállást és ezzel együtt jelentősen csökkentette az atom-világháború veszélyét, továbbá Közép-Európát tekintve minimálisra csökkentette egy nagyméretű váratlan támadás kockázatát is. [4] Ugyanakkor lényegesen megnőtt és összetettebbé vált a kockázatok, illetve veszélyforrások köre. A Magyar Köztársaság biztonság- és védelempolitikájának alapelvei szerint növekvő kockázatot jelent a terrorizmus, a szervezett bűnözés, az illegális kábítószer- és fegyverkereskedelem.

A bűnözőcsoportok az említett tevékenységek összehangolt szervezéséhez és működtetéséhez igénybe veszik a mobil telekommunikációs szolgáltatásokat, amely tény indokolja a bűnüldöző szervezetek elhárító képességének fenntartását, továbbá folyamatos fejlesztését. A cellás mobil hálózatok megfigyelése és lehallgatása a technológiai konvergencia eredményeként egyre nehezebben megoldható feladatként jelentkezik. A felderítés során már nemcsak a vezeték nélküli beszédátvitelbe kell betekinteni, hanem az egyre inkább jellemző beszéd-adat jellegű információkat kell elemezni, ezáltal a feldolgozás során szét kell tudni választani e kétféle információ tartalmát. [5]

A terrorizmus szempontjából vizsgálva a rendszer további potenciális veszélyeket hordozhat magában, ugyanis a fejlett mobiltelefon hálózat egyaránt lehet az elkövetés eszköze és célja is. Az eszközként való felhasználására napjainkban számos példa mutatkozik, melyek közül a készülék távirányítónkénti használata csak az egyik jellemző alkalmazása.

Napjainkig tekintve nem lelhető fel olyan információ, ami arra engedne következtetni, hogy csak a hálózat bénítása lett volna a terroristatámadás kiemelt célpontja. Ez azonban nem jelenti azt, hogy a jövőben nem válhatna célponttá.

A GSM HÁLÓZATOK FEJLŐDÉSE

Az első generáció

Az első generáció kezdetét az analóg cellás rádiótelefon-rendszerek kísérleti üzembeállítása jelentette. Az első generációs hagyományos cellás telefonrendszerek elsősorban a tengerentúli területeken (így pl. Kanadában, az USA-ban, Mexikóban, valamint Közép- és Dél-Amerikában) terjedtek el, ahol még a mai napig egyeduralkodók.

Első kísérleti változatát az AT&T fejlesztette ki Chicagóban, és itt került tesztelésre az 1976-1979 közötti időszakban is. Az igazi kereskedelmi hálózat üzembe állításáig azonban 7 évet kellett várni-, amely 1983-ban indult világhódító útjára ugyancsak Chicago-ban-, majd ugyanebben az évben már kiépítették a hálózatot Washington-ban, illetve Baltimore-ban is.

A 80-as évek közepén több Európai országban is elterjedt a rádiótelefónia első generációs változata, az analóg cellás rendszer. Ezek közül a legismertebbek a következők voltak:

- NET-C Németország)
- TACS Egyesült Királyság
- IMTS Olaszország
- Radiocom 2000 Franciaország
- és talán számunkra a legismertebb Westel 06-60 NMT rendszer Magyarország

Az NMT típust a skandináv államokban indították el. Hazánk ezt a rendszert vette át, amely a 450 MHz sávtartományban üzemelt. Ezek a hálózatok más-más protokollt használtak, így egymással nem kompatibilisek.

Európa legtöbb országában már 1985/86-tól működtek analóg cellás hálózatok, ezek többsége a 90-es évek elejére elérte maximális kihasználtságát, majd elkezdtek kiszorulni a piacról, mert nem csatlakoztak a 900 MHz-es sávszélességen működő rendszerekhez a CEPT (Centre for Environmental Planning & Technology) által felügyelt alap-szabványhoz.

Összefoglalva megállapítható, hogy az AT&T vállalat alapötlete tekinthető a mobiltelefónia ősének. A benne rejlő lehetőségeket több nagyvállalat is felismerte, ezért kidolgozta az egyéni sajátosságokkal bíró rendszerét. Az egymás mellett párhuzamosan indított fejlesztési törekvések a vezető szerep megszerzésére irányultak, ezáltal meggátolták a hálózatok átjárhatóságát. A mobil hálózatok kizárólag analóg híradástechnikai megoldásokat tartalmaztak. A csatornakihasználhatóság növelésére frekvencia osztásos multiplexálás módszere került alkalmazásra.

Az inkompatibilitás egyaránt csökkentette a szolgáltatás értékét mind a felhasználói, mind a beruházói oldalról nézve. A problémát Európában ismerték fel a legkorábban, ezért itt került a leghamarább kidolgozásra egy közös szabvány, amely útjára indította a következő GSM generációt és megteremtette a konvergencia kezdeti lehetőségét.

A szolgáltatás szembetűnő problémája a titkosítás teljes hiánya volt, emiatt már egy viszonylag egyszerű berendezéssel is közvetlenül bele lehetett hallgatni a beszélgetésbe. Személyes tapasztalatom szerint bizonyos esetekben a tévékészülék segítségével is el lehetett csípni egy-egy beszélgetést.

A második (digitális) generáció

A GSM rendszer elméletéről először a 80-as évek első felében hallhattunk, majd mintegy nyolc év elteltével ez a szabvány vált meghatározóvá az európai mobil-távközlési infrastruktúra kialakításában.

A 900 MHz-es GSM rendszerek össz-európai hálózata a 90-es évek elején indult világhódító útjára. A szabvánnyá vált analóg GSM rendszerek továbbfejlesztése során a következő nagy feladat az analógról digitális technológiára való átállás volt. A digitális rendszer előnyei közé tartozik, hogy lényegesen jobb a hatásfoka, magasabb szintű az adatátvitel minősége, és új szolgáltatások igénybevételére is lehetőség nyílik, ide értve az adatbiztonságot is.

Lehetővé vált a VLSI[5] (Széles skálájú integráció) technológia használata, amely egyre könnyebb és olcsóbb árfekvésű készülékek megjelenését eredményezte. Másrészt a digitális technika elérhetővé tette egy új szabvány, az ISDN[6] megalkotását, amely a digitális GSM technológia illeszkedő rendszerévé vált.

A digitális GSM technológia legfőbb előnyei között talán a barangolási (roaming) lehetőséget említhetjük meg, továbbá az olcsóbb és kisebb méretű készülékek megjelenését. Mindezen fejlesztések a felhasználók egyre szélesebb körének folyamatos, illetve zökkenőmentes kiszolgálásával valósultak meg.

A közös szabványokon alapuló második generáció elterjedése útját állta az inkompatibilis egyedi rendszereknek. Azok a beruházások, amelyek nem követték a

[5] Very Large Scale Integration - Széles skálájú integráció
[6] Integrated Service Digital Network – Integrált Szolgáltatású Digitális Hálózat

szabványosítási tevékenység által előírt paramétereket a további fejlődési lehetőségek szempontjából zsákutcának bizonyultak.

Kijelenthető, hogy a ’80-as évek végén a mobil kommunikáció, illetve az információtechnológia meghatározó trendjének a szabványosítási törekvések tekinthetők.

Az analóg hálózat felváltása digitális technológiára, a csatorna kihasználhatóság növelése a frekvencia és időosztásos multiplexelés módszerével, illetve az ISDN kompatibilitás előírása jelentette az első nagy lépés megtételét a híradást és informatikát élesen elválasztó határvonalak elmosódásában.

A hálózat alacsony adatátviteli kapacitása (9,6 kbps), illetve a csatorna lefoglaltsága alapján számított adatforgalom problémája szükségessé tette a továbbfejlesztés igényét. Az előfizetők már nem csak telefonálni szerettek volna, hanem növekvő érdeklődést tanúsítottak a telefon kibővített szolgáltatási lehetőségei iránt is. A tisztán idő- és frekvenciaosztásos multiplexelés alkalmazásával azonban nem lehetett technikailag biztosítani a nagyobb adatátviteli képességet, illetve a tényleges adatforgalom mérését sem.

A 2,5 generációs (2,5G) Általános Csomagkapcsolt Rádiós Rendszer

Az ezredfordulóval egybeeső információs társadalom kezdetét az internet és a mobiltávközlés hihetetlen mértékű fellendülése jellemezte. Ebben az időszakban a szolgáltatók-, és általuk a gyártók is teljes mértékben az adatátviteli sebesség növelésére koncentráltak.

A felhasználói szokások gyökeres változáson mentek keresztül. A mobiltelefonok széleskörű elterjedése[7], illetve az a tény, hogy azok a nap 24 órájában a tulajdonos közvetlen környezetében találhatóak- ezzel mintegy személyes tárggyá léptek elő- magával hozták a személyre szabhatóság kérdésének feltevését is. Népszerűvé vált az egyéni háttérkép, a csengőhang, illetve a zene letöltése. A legtöbb készülék csak hálózaton keresztül volt képes ezeket az opciókat biztosítani, hiszen az infravörös (IRDA) vagy Bluetooth megoldások csak néhány magasabb árkategóriájú mobiltelefon különlegességeként volt jelen. [6]

Az áttörő hálózati megoldást a GPRS[8] technológia bevezetése jelentette. A csomagkapcsolt eljárást legelőször a korai 1970-es években használták a vonalkapcsolt adatátviteli határok kiszélesítésére, majd az elkövetkező időben tisztán „adatátvitelre” alkalmazták. A legismertebb felhasználása a hálózatba kötött számítógépek közötti kommunikációt biztosító Ethernet szabvány volt.

A ’90-es évektől már digitális alapon üzemelő elsősorban hang átvitelére kifejlesztett készülék működésében is megjelent az első, eddig kifejezetten informatikai célból alkalmazott eljárás. Ezzel a lépéssel már nem csak a „hagyományos” telefonálásra lefektetett vonalkapcsolt-, hanem a csomagkapcsolt technológia is bekerült a GSM hálózatok szolgáltatásába, mely által elérhetővé váltak olyan lehetőségek is, mint:

- a jóval nagyobb adatátviteli sebesség, amelynek elméleti felső határértéke a 171,2 kb/s –természetesen a gyakorlatban az előfizetőnek ténylegesen kiosztott sebesség ennél alacsonyabb (64-100 kb/s);
- az adathálózatok (pl.: Internet) elérési idejének csökkentése (<1s);
- az erőforrás megoszthatósága több felhasználható között, ugyanis az előfizető csak akkor használja a hálózatot, amikor éppen adatot küld, vagy fogad

[7] A BellResearch által 2007-ben végzett magyarországi felmérés alapján 3,9 millió háztartás 78%-a rendelkezett legalább egy kártyás vagy post-paid –mobiltelefon-előfizetéssel.
[8] General Packet Radio System: Általános Csomagkapcsolt Rádiószolgáltatás

- az IP alapú adatátvitel, amely biztosítja a felhasználók költséghatékony csatlakozását a nyilvános, vagy zárt (Intranet) informatikai rendszerekhez hálózati protokollok (pl.: TCP) felhasználásával;
- a helyfüggő alkalmazások kiváltása „mobil" irodával;
- az aszimmetrikus adatátvitel.

A 2.5G szolgáltatások bevezetése döntő fontosságú lépésnek bizonyult a 3G rendszer elfogadásához vezető úton. A hálózat „felruházása" GPRS szolgáltatással nem okozott nagy megterhelést a szolgáltatóknak, mert az új elemek integrálása modulszerűen történt, illetve gazdaságilag megtérülő beruházásnak számított. A GPRS-hez kapcsolt fejlesztések és bővülő szolgáltatások „filozófiája" megteremtette a harmadik generáció alapját. [7]

A konvergencia folyamatát kiemelve megfigyelhető a 2.5 generációs rendszerkialakítás legfontosabb törekvései: a felhasználók adatátviteli igényeinek a kielégítése, illetve az informatikai szolgáltatások biztosítása.

A harmadik generáció

Napjainkban a harmadik generáció felé vezető ajtó küszöbén átléptünk. A szolgáltatók nagy része már alkalmassá tette rendszerét a kibővített alkalmazások eléréséhez szükséges, elméletileg korlátlan hozzáférést nyújtó CDMA[9] használatára. A GSM és az AMPS-ből továbbfejlesztett digitális rendszerek mellett a jövőben bevezetésre terveznek új digitális rádiótávközlő rendszereket, melyek lefedve az egész Földet –az országonként különböző szolgáltatók által üzemeltett, de egymással kompatibilis hálózatok- teremtik meg egy globális, nagy sebességű infokommunikációs rendszer jövőbeni alapjait.

A harmadik generáció megnevezést egyre gyakrabban használják az UMTS[10] szinonimájaként. Ez a GSM architektúrát leváltó új technológia szélessávú mobilhozzáférést és 1-2 MBit/s adatátviteli sebességet tesz lehetővé, amely tovább fokozza a konvergencia hatását. Szemléltetésére nagyon jó példa a Vodafone Magyarország által 2006-ban kiadott prospektus, amely a következő szolgáltatásokat kínálja a 3G előfizetőknek:

- közel CD minőségű zeneletöltést a több százezres választékból;
- MobilTv és Videók használatát, amely által elérhetővé válnak TV csatornák és a speciálisan mobiltelefonra gyártott videó tartalmak. Válogatási lehetőséget az RTL legnépszerűbb műsoraiból élő- és visszatekinthető módban. Sőt a Vodafone kizárólagos opciójaként elérhetőséget kínál az UEFA Bajnokok Ligája felvett mérkőzéseihez;
- videotelefonálást, amely az élő képközvetítéssel még közelebb hozza egymáshoz a beszélgető partnereket;
- nagy sebességű vezeték nélküli Internet elérést, a hagyományos GPRS technológia hétszeres sebességével. [8] [9]

A felsorolt szolgáltatások jól tükrözik az informatika, a híradás és harmadik szereplőként a média összeolvadását. A szolgáltatások további bővítésének igénye a felhasználói oldalról továbbra is fennáll, azonban a gazdasági válság hatására világszerte mintegy 20%-os visszaesést kellett tapasztalniuk a szolgáltatóknak. [10] A fejlődés, a

[9] Code Division Multiple Access: kódosztásos többszörös hozzáférés
[10] Universal Mobil Telecommunication System – Egységes Mobile Telekommunikációs Rendszer

különböző területek összeolvadása a telekommunikáció területén, azonban nem állt le, ugyanis ez év januárjában, Stockholmban a Telina Solina vállalat bejelentette a következő negyedik generációs rendszermegoldását.

A 2-2,5 generációs készülékek az elődhöz képest már viszonylag erős csatornatitkosítást használnak, ezért a beszéd közvetlen lehallgatása a titkos algoritmusok ismerete nélkül jóval bonyolultabb feladatot jelent. Természetesen az alapkészülék által használt titkosítás nem tekinthető elégségesnek a minősített adatok közléséhez.

Elemezve a 2,5 generáció által nyújtott szolgáltatásokat megállapítható, hogy a beszédátvitel mellett egyre fontosabbá váltak a különböző „extra" szolgáltatások. A készülékek számottevő hányada képes olyan funkciók megvalósítására, mint a globális helyzet-meghatározás, a videotelefonálás, a nagy sebességű internetelérés és a különböző kódnyelvekre írt alkalmazások futtatása.

A biztonsági elemzők figyelmét szinte teljes mértékben elkerülte a készülékeken futtatatható idegen kódok lehetősége, ezért a 2004-ben megjelent Cabir malware sokkhatásként érte a mobiltársadalmat. A cseh programozók által létrehozott kódsorozat a Nokia 60-as szériába tartozó készüléken futó SymbOs operációs rendszer biztonsági hiányosságát használta ki. Szerencsére az első mobiltelefon vírus nem okozott különösebb károkat a készülékekben. A fejlesztők célja nem a károkozás volt, hanem egyszerűen be akarták bizonyítani, hogy az addig érinthetetlennek hitt telefonkészülékek a technológiai konvergencia hatására átlépték azt a határt, amelyen túl már igenis számolni kell a hasonló kódok jelenlétével.

A Cabir kódsorozata később szabadon elérhetővé vált az interneten, melynek hatására egyre több „telefon" vírus látott napvilágot. Jelenleg a számuk már meghaladja a több százat, azonban mégsem kell tartanunk tömeges terjedésüktől. Ez azzal magyarázható, hogy a kereskedelmi forgalomban kapható készülékek palettája igen széles, így az eltérő berendezések különböző operációs rendszereket használnak.

Negyedik generáció

A negyedik generáció még szélesebb szolgáltatás repertoárral, gyorsabb letöltési sebességgel, és számos teljesen új lehetőséggel káprázтatja el a leendő felhasználóit. Észak-Európában már megkezdődtek a következő technikai lépcsőfok meglépését elősegítő fejlesztések kivitelezése.

Magyarországon a „digitális" hozadékba tartozó, és a következő generációnak működési spektrumot biztosító „mobiltender" sikertelenül zárult, mert a nyertes kihirdetése elmaradt.

Véleményem szerint a világgazdasági válság hatására bekövetkező szűkülő mobilpiac nem jelenti a technológia bevezetésének teljes elvetését, csupán lassítja annak folyamatát. A rendszerspecifikációk már régóta elérhetők, így a kivitelezés jelenlegi akadályát csupán a gazdasági befektetési hajlandóság hiánya jelenti.

A negyedik generációval kapcsolatban a következő követelmények kerültek megfogalmazásra:

- legyen teljesen IP alapú csomagkapcsolt hálózat;
- rendelkezzen nagyobb kapacitással, cellánként szolgáljon ki több felhasználót;

- a világ bármely két pontja között, mozgás közben is tudja biztosítani a 100 Mbit/s adatátviteli sebességet, még ez a képesség álló helyzetben érje el az 1 Gbit/s értéket.
- legyen felülről kompatibilis a jelenlegi 2-3 generációs mobilokkal;
- valósítsa meg a globális roaming lehetőségét.

A kitűzött célokból jól tükröződik, hogy a rendszer legszembetűnőbb képessége a megnövekedett adatátviteli képesség és a teljesen IP alapú csomagkapcsolt hálózat lesz. A szolgáltatás igénybevételéhez szükséges „okos" készülékek inkább sorolhatók majd a mikroszámítógépek közé, mint a beszédkommunikációt megvalósító telefonok táborába.

Meglátásom szerint a cellás mobiltelefon hálózatok fejlődésében a negyedik generáció jelenti azt a mérföldkövet, amelynek elérésével teljes mértékben a cybertér részévé válik, és ezzel párhuzamosan még jobban felértékelődik kulcsfontosságú szerepe. Clinton elnök által felkért bizottság már 1997-ben felismerte a cybertér kiemelt fontosságát. A bizottság megállapítása alapján a cybertér a nemzeti infrastruktúra idegrendszere, illetve ellenőrző rendszere az országnak. [11] A megállapítás valóságát mi sem bizonyítja jobban, mint az Észtország ellen indított összehangolt internetes támadás, amelynek hatására néhány napra megbénult az ország.

A támadás alapját a Földet behálózó internet jelentette, amely elérése a megnövekedett sávszélesség biztosításával teljesedik ki a negyedik generációs hálózatban. Az internetre való tömeges csatlakozás pedig szabad utat nyithat a hasonló offenzívák megvalósítására.

ÖSSZEFOGLALÁS

A konvergencia helytálló besorolása az infokommunikációs fejlesztéseket jellemző megatrendek soraiba megkérdőjelezhetetlen. Hatására az eltérő ágazatokban használt technológiák közötti különbségek eltűnnek, az eltérő platformok határvonalai egymásba folynak. A vezetékes-, mobil- valamint kábelhálózati szolgáltatások összeolvadnak.

A jövőt jelentő negyedik generációs mobiltelefon hálózatokhoz tartozó végfelhasználói készülékek jellemzője a nagysebességű adatátvitelhez kapcsolható alkalmazások futtatása lesz. A továbbfejlesztett okostelefon átlépve a cybertér küszöbét egyrészt számos új lehetőséget fog nyújtani a felhasználóknak, másrészt új célpontot fog jelenteni az informatikai bűnözésnek. Feltehetően növekszik majd a készülékekre írt illegális kódsorozatok száma is, amelyek irányított használata könnyen válhat a terrorizmus eszközévé.

Hivatkozott irodalom

[1] Hahner Péter: A forradalom fogalmáról, -2008 http://epa.oszk.hu/00600/00691/00056/02.html [Letöltve: 2009. november 17.]

[2] Fekete Károly: A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei, Zrínyi Miklós Nemzetvédelmi Egyetem. Budapest. -2003. (PhD értekezés)

[3] Kőszegvári Tibor: Hadviselés a 21. században, Hadtudomány, 1999. március, IX. évf. 1. szám.

[4] http://rentit.hu/cikk/84/mobiltelefon_generaciok.aspx [letöltve: 2010. május 9.]

[5] Balog Károly: Harmadik generációs távközlési technikák és hatásuk a kommunikációs felderítésre http://www.nbsz.gov.hu/docs/3G_tavkozlesi_technikak.pdf [letöltve: 2010. május 9.]

[6] Mobil Portál: A GSM története http://www.mobilport.hu/fokuszban/20030810/a_gsm_tortenete/, [letöltve: 2009. november 18.]

[7] KommWiki: A mobiltelefon története http://p2p-fusion.mokk.bme.hu/w2/index.php/14, [letöltve: 2009. november 18.]

[8] Nokia Corporation: Introduction to WAP over GPRS, ForumNokia, 2001 http://ncsp.forum.nokia.com/csp/assets/c2/documents/WAPoverGPRS.pdf, [letöltve: 2009. november 18.]

[9] Németh András: A mobil szolgáltatók hálózatainak felhasználása, fejlesztési lehetőségei és alternatív megoldások a katasztrófavédelmi kommunikáció területén, Zrínyi Miklós Nemzetvédelmi Egyetem. Budapest. -2007. (PhD értekezés)

[10] Vodafone Magyarország: A legújabb 3G szolgáltatások a Vodafone-tól http://www.vodafone.hu/egyeni/common/vodafonerol/magyarorszagon/letoltes/pr060608_hatteranyag.pdf, [letöltve: 2009. november 18.]

[11] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, Zrínyi Miklós Nemzetvédelmi Egyetem. Budapest. -2007. (PhD értekezés)

HADMÉRNÖK
V. Évfolyam 2. szám - 2010. június

Seres György
drseres@drseres.com

Fórika Krisztina
krisztina@forika.hu

Miskolczi Ildikó
miskolczi.ildiko@gmail.com

Lengyel Piroska
l.piroska@t-online.hu

Gerő Péter
gp.projekt@gmail.com

HIPERMÉDIA AZ OKTATÁSBAN – AVAGY FELHŐPEDAGÓGIA. HOGYAN VÁLT AZ ELEKTRONIKA AZ OKTATÁS TÁRGYÁBÓL ANNAK SZÍNTERÉVÉ?

Absztrakt

A távoktatás, a XXI. század oktatási struktúrájának meghatározó szelete és a közeljövőben jelentősége és súlya egyre nő. A modern távoktatás korunk technikai vívmányait felhasználva lehetővé teszi az oktatás teljesen újszerű módjának az e-learningnek az alkalmazását. Napjainkban megjelent és rohamosan terjed – nem csak az oktatás területén – az un. felhő technológia (cloud technology, cloud computing), ami a hálózatos technológiára épít. Így az oktatásban felhő pedagógia nevet viselő új módszer(tan) legfőbb jellemzője, hogy a felhőként aposztrofált számítógépek csoportjainak teljesítményét, illetve azok egy részét a virtuális térben elérve, saját erőforrásainkat felszabadítva használhatjuk. Jelen cikkben az olvasó áttekintést kap a felhőpedagógia mibenlétéről, a szerzők által legfontosabbnak vélt tartalmi elemeiről, azok alkalmazási lehetőségeiről, hatékonyságot növelő szerepéről a távoktatásban. A cikkírók legfrissebb kutatási eredményeiket gyűjtötték össze, szemléltetve a korunk forradalmian új lehetőségeit a virtuális térben történő oktatás során.

The distance learning, the 22th century educational structure determining the near future importance and the weight growing. Using the modern distance learning our technical makes it possible for the education is completely innovative manner in the e-learning's application. Today, appeared and rapidly covered not only the field of education, the cloud technology, which builds on the network technology. This is new method in the teaching, in the practice it named

cloud-teaching. It means, that the users use the virtual space for their works and not their own computers' energy.
In this article the reader will receive an overview of cloud-teaching. The authors show the newest results of their work, wich show the content elements, the possibilities for employment, increasing efficiency on the role of learning.

Kulcsszavak: *e-learning, felhő technológia, felhő pedagógia, közösségi terek, közösségi munka ~ e-learning, cloud technology, cloud pedagogy, community spaces, community work*

BEVEZETÉS

A múlt század húszas éveiben elterjedt nyilvános rádió- és a harmincas években megkezdődött nyilvános televízióadások az elektronikát az oktatás jelentős, új *tárgyává* tették.

A negyvenes években jelentkező iskola-rádiók és az ötvenes-hatvanas évek iskola-televíziói már az oktatás közösségi *eszközévé* tették az elektronikát.

A hetvenes években a mágneses hangrögzítés, a nyolcvanas években pedig a videó rögzítők és a személyi számítógépek megjelenésével ez az új eszköz már az iskolai oktatásban is megjelent.

A nagy áttörést azonban a kilencvenes években az Internet széleskörű alkalmazása, illetve az új évezred első évtizedében – a szélessávú adatátvitel elterjedésével – a gyors Internet-hozzáférés hozta.

A digitális adat-, hang- és képrögzítés, valamint a szélessávú adatátvitel segítségével az Interneten *bármilyen* tananyagot, *bárki* számára, *bárhol* és *bármikor* hozzáférhetővé lehet tenni *reális idő* alatt.

Ezzel elérkeztünk oda, ahol az elektronika az oktatás tárgyából, majd eszközéből az oktatás és a tanulás *színterévé* vált.

Az egyre bonyolultabb felhasználói programok futtatása, az egyre nagyobb méretű adatfájlok tárolása és mozgatása, az egyre nagyobb adatfeldolgozási és adattovábbítási sebesség elérése egyre erősebb és drágább hardver- és szoftver-követelményeket támaszt a felhasználói oldalon.

Ezt felismerve, a huszonegyedik század második évtizedében született meg a számítógép-felhőnek (Cloud Computing) nevezett szolgáltatás.

Ennek lényege, hogy az adattárolási és adatmozgatási, valamint a nagy számítástechnikai feladatokat nem a felhasználók saját számítógépe végzi, hanem egy egyszerű internetes böngésző útján ingyenesen, vagy - a saját erőforrások létrehozásánál és üzemeltetésénél lényegesen kisebb - bérleti díjak fejében a számítógépfelhőben működő szolgáltatók biztosítják.

A gondolat, természetesen, nem új.

Ahhoz, hogy egy adatforrást megtaláljunk az Internet dzsungelében, már régen nem a saját gépünkről kell végigböngészni a világhálót.

Ezt a feladatot már régen a nagy erőforrásokkal rendelkező keresőszolgáltatókkal (Yahoo, Google stb.) végeztetjük el.

A korszerű, költséghatékony, interaktív tudásátadás sem oldható meg csupán a saját erőforrások felhasználásával.

Ezen a területen is igénybe vehetjük a számítógépfelhőben működő szolgáltatásokat.

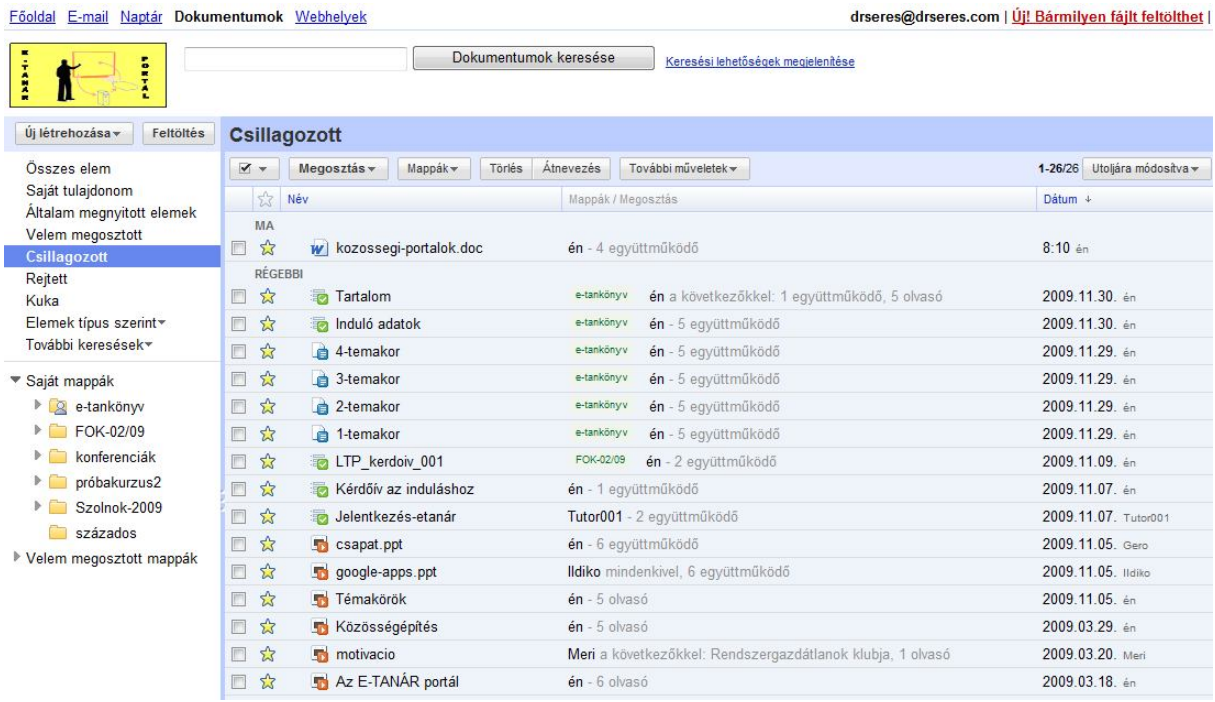
Ezekből a szolgáltatásokból mutatunk be néhány – általunk már kipróbált változatot az alábbiakban.

DOKUMENTUMOK TÁROLÁSA ÉS MEGOSZTÁSA AZ INTERNETEN

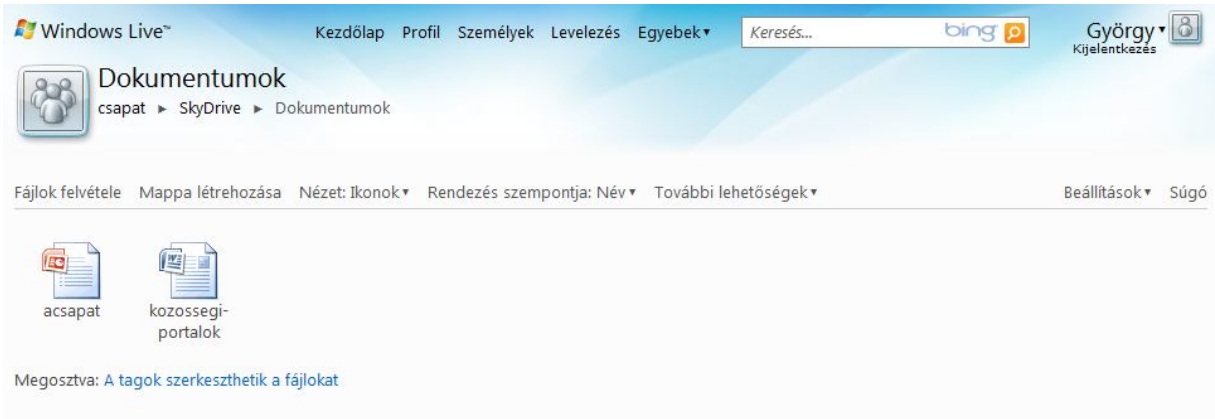
A leggyakoribb tananyagok – dokumentumok– tárolására és megosztására az Interneten nagyon sok szolgáltatót találhatunk. Ezek közül a legelterjedtebb a Google Docs[1] és a Microsoft két tárhelye, a Windows Live Sky Drive[2], és az Office Live[3].

Az első a Google Alkalmazások keretében működik – a Gmail postafiók és a Calendar naptári szolgáltatással együtt. A tároláson kívül (1. ábra) alkalmas szöveges dokumentumok, prezentációk és táblázatok online egyéni és közös szerkesztésére, miközben a szerkesztők chat-ablakban kommunikálhatnak is egymással.

A Microsoft tárhelyein a különböző dokumentumok szintén megoszthatóak, és több felhasználó által is szerkeszthetőek (2. és 3. ábra), azonban csak offline módon – a felhasználók saját irodai alkalmazásaival.

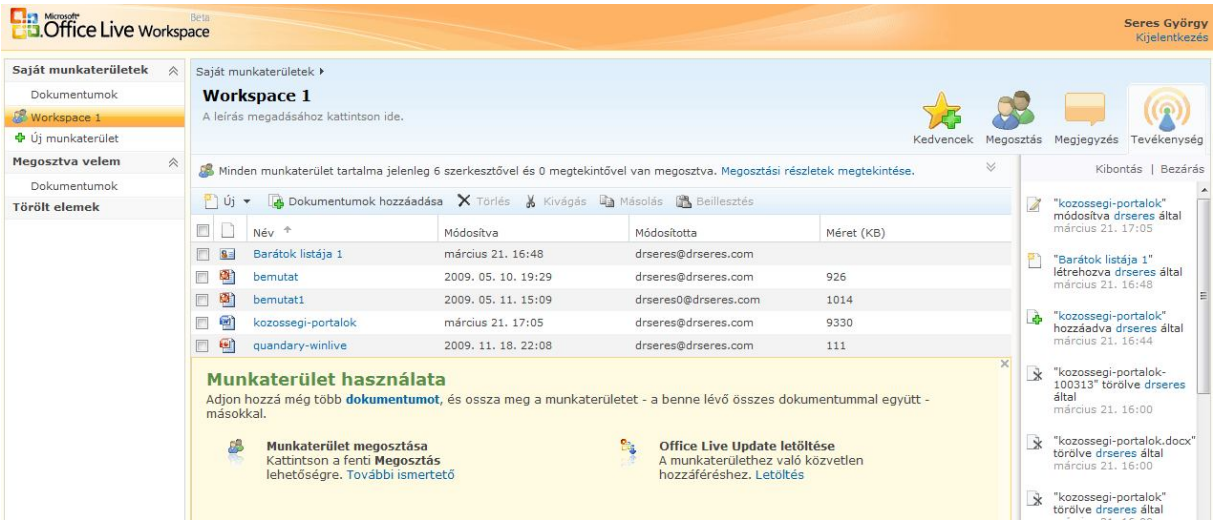


1. ábra. A Google Docs „könyvtára”



2. ábra. A Windows Live „könyvtára”

[1] http://docs.drseres.com/
[2] https://cid-0009fa821aa3c4fa.groups.skydrive.live.com/browse.aspx/.Documents
[3] http://workspace.office.live.com/#drseres/Workspace 1

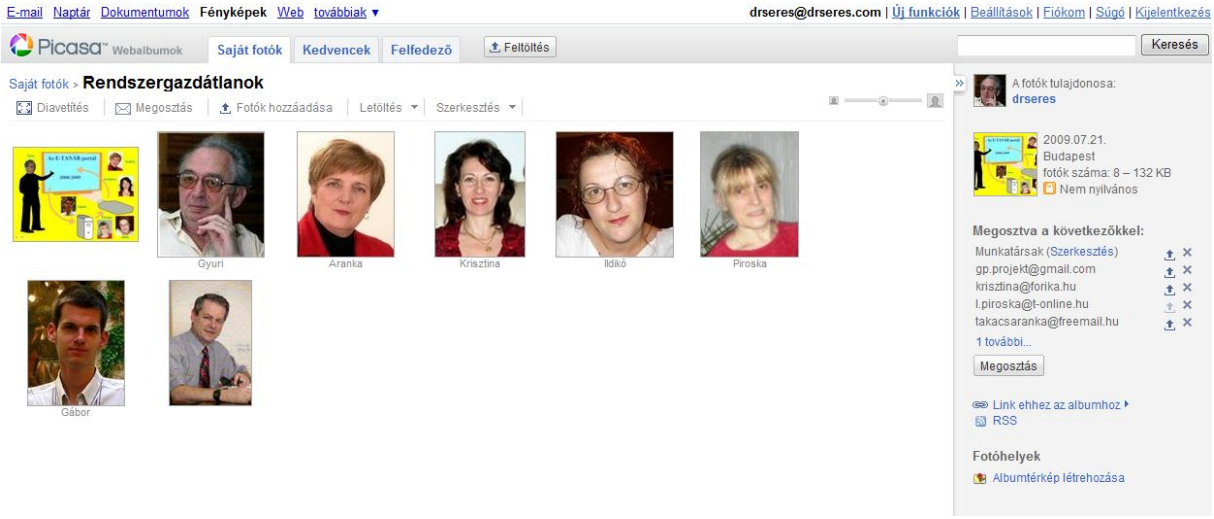


3. ábra. Az Office Live „könyvtára”

KÉPEK ÉS VIDEÓK TÁROLÁSA ÉS MEGOSZTÁSA AZ INTERNETEN

Az audió-vizuális tananyagok – fotók és videók – tárolása és megosztása az Interneten a számítógépfelhőknek (Cloud Computing) – a keresőszolgáltatások után – szinte legkorábbi szolgáltatásai közé tartoznak.

Közülük a legnépszerűbb a Picasa[4] (4.ábra) és a Youtube[5] (5. ábra), de sokan használják a Vimeo[6] (6. ábra) és a Flickr[7](7. ábra) portálokat is.



4. ábra. Portálunk fotóalbuma a Picasa portálon

[4] http://picasaweb.google.com/drseres00
[5] http://youtube.com/user/etanar1
[6] http://vimeo.com/drseres/
[7] http://www.flickr.com/photos/drseres/



5. ábra. Egy videoklippé konvertált prezentáció a Youtube portálon



6. ábra. Videoklipjeink a Vimeo portálon



7. ábra. Az Iskola Televízió archív filmje a Flickr portálon

PREZENTÁCIÓK TÁROLÁSA ÉS MEGOSZTÁSA AZ INTERNETEN

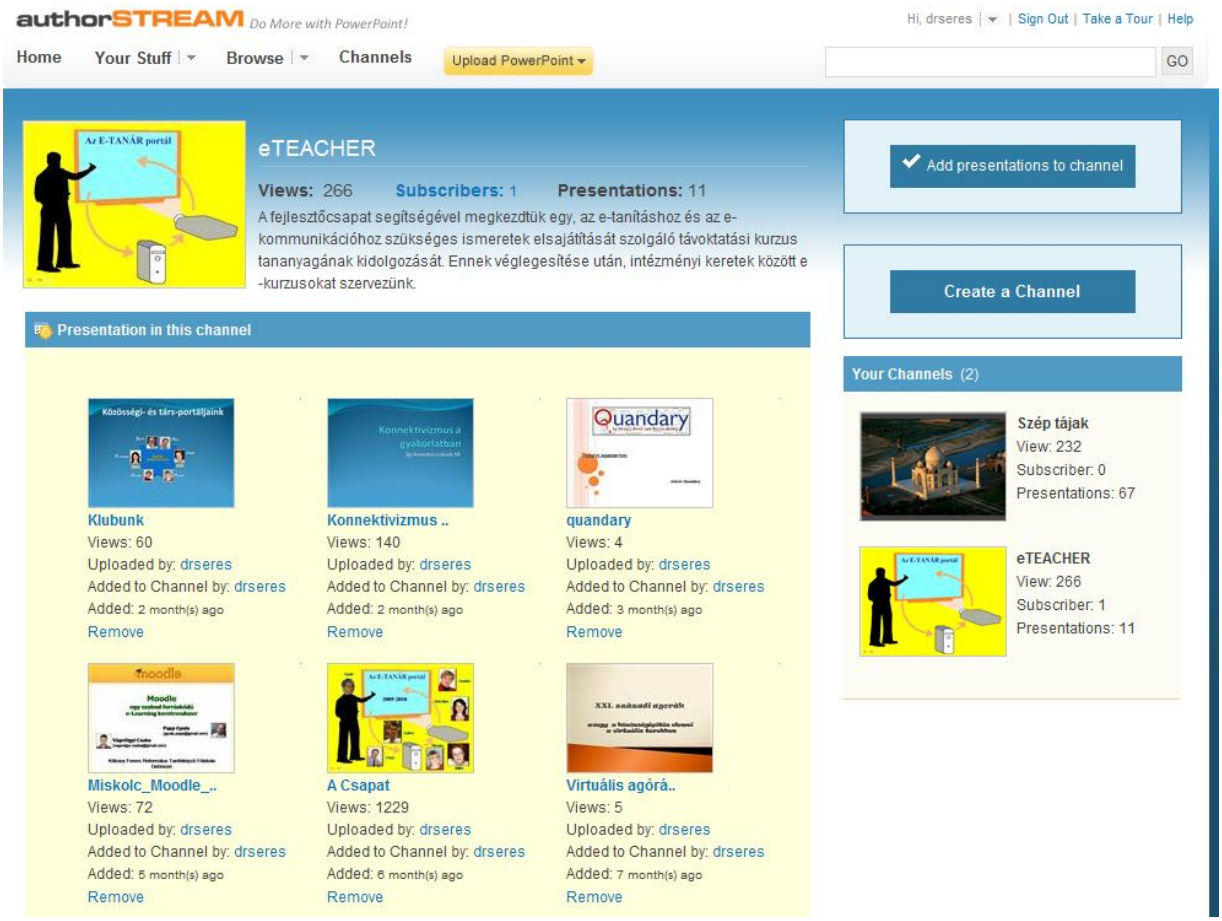
A leggyakrabban használt oktatási anyagok – a prezentációk – tárolására és megosztására az Interneten legalkalmasabbak az erre a dokumentumformára szakosodott portálok.

A prezentáció-megosztó oldalak között – tapasztalataink szerint – az authorSTREAM[8] portálon (8. ábra) tárolt bemutatók adják vissza lejátszáskor a leghívebben az eredeti prezentáció képi és hanghatásait, áttűnéseit és diaváltásait.

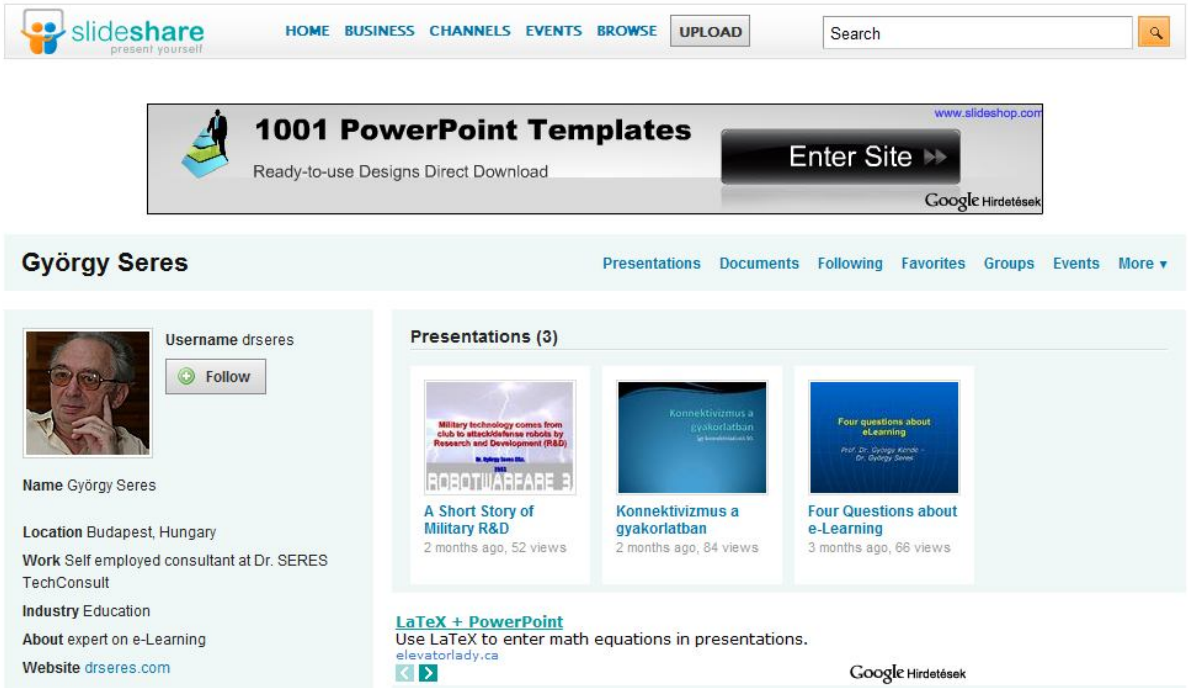
De az egyszerűbb prezentációk megosztására alkalmas a Slideshare[9] (9. ábra), és a Scribd[10] portál (10. ábra) is .

Újszerű, érdekes és látványos bemutatók online szerkesztését, tárolását és megosztását biztosítja a – magyar fejlesztők által létrehozott, de, sajnos, magyarul még nem tudó – Prezi[11] portál (11. ábra).

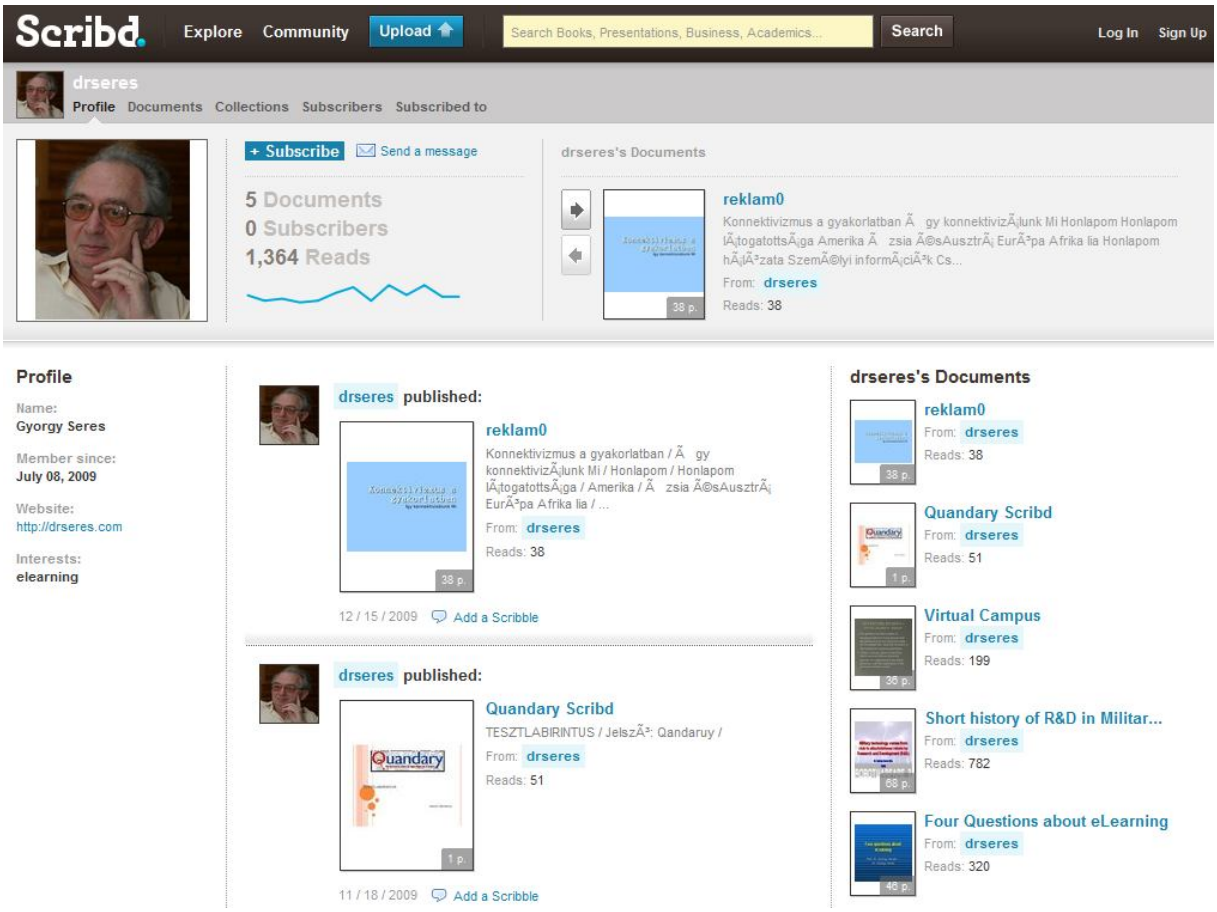
[8] http://www.authorstream.com/tag/drseres
[9] http://www.slideshare.net/drseres
[10] http://www.scribd.com/drseres
[11] http://prezi.com/ggotqqw6w5d_/



8. ábra. Prezentációink az authorSTREAM portálon



9. ábra. Prezentációink a slideshare portálon



10. ábra. Prezentációink a Scribd portálon



11. ábra. Prezentáció szerkesztése a Prezi portálon

VIRTUÁLIS TANTEREM

A Google Docs[12] (12. ábra) és az authorSTREAM[13] portálok (13. ábra) biztosítják a tárolt prezentációk nyilvános vagy zártkörű bemutatását is, a nézőkkel külön chat-ablakban folyó, párhuzamos párbeszéd mellett.

Ha az előadó és a hallgatók között beszédkapcsolatra is szükség van, akkor párhuzamosan használhatjuk a Skype, vagy a Windows Live Messenger konferenciabeszélgetés (14. ábra) szolgáltatását is.

Ennél sokkal életszerűbb online előadásokra nyújtanak lehetőséget a WiZiQ[14] (15. ábra) és a DimDim[15] (16. ábra) virtuális-tanterem portálok.

Ezek egy virtuális osztályterem valamennyi követelményét kielégítik.

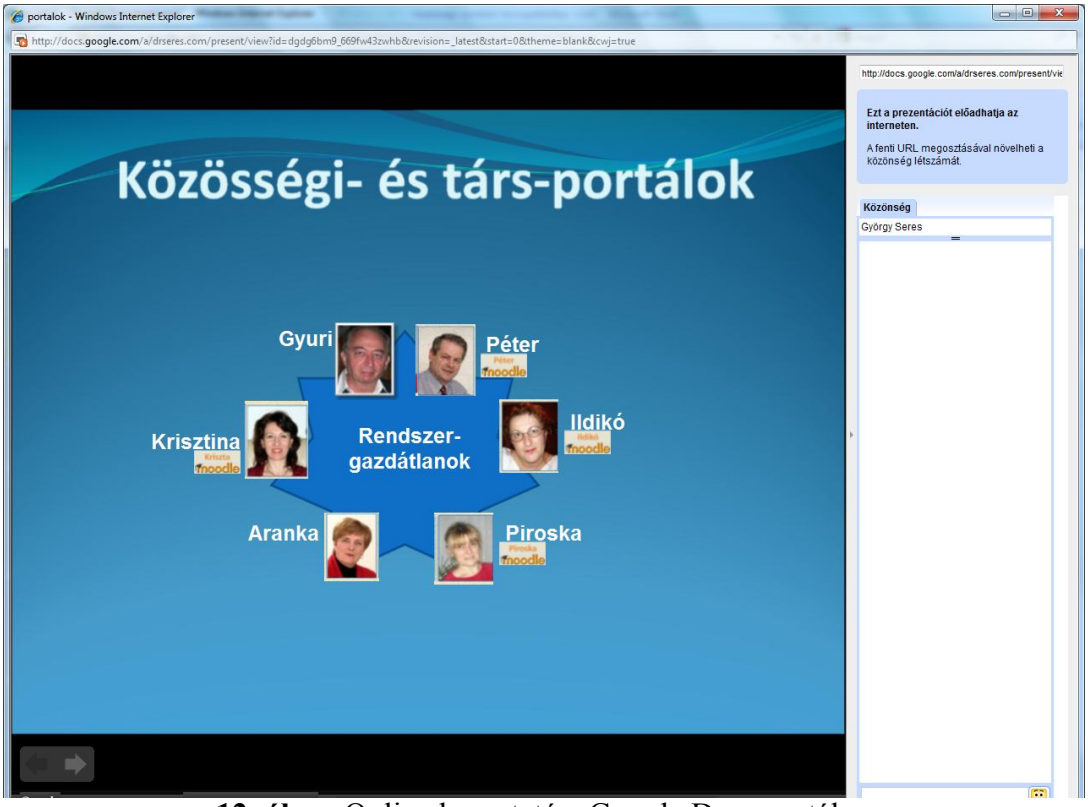
Prezentációk, képek és videók bemutatása mellett „okostábla” lehetőséget, valamint élő audio- és video-kapcsolatot biztosítanak az előadó és a hallgatók között.

Emellett, ezeknek a portáloknak kiegészítő szolgáltatásai közé tartozik a különböző témákat meghirdető tanárok, és az azokat kereső tanulók közötti kapcsolatok létrehozása is.

Érdekes online előadásokra ad lehetőséget a saját web-kameránk, illetve egyéb hang- és képanyagunk élő televíziós közvetítésére specializálódott Ustream portál[16] (17. ábra).

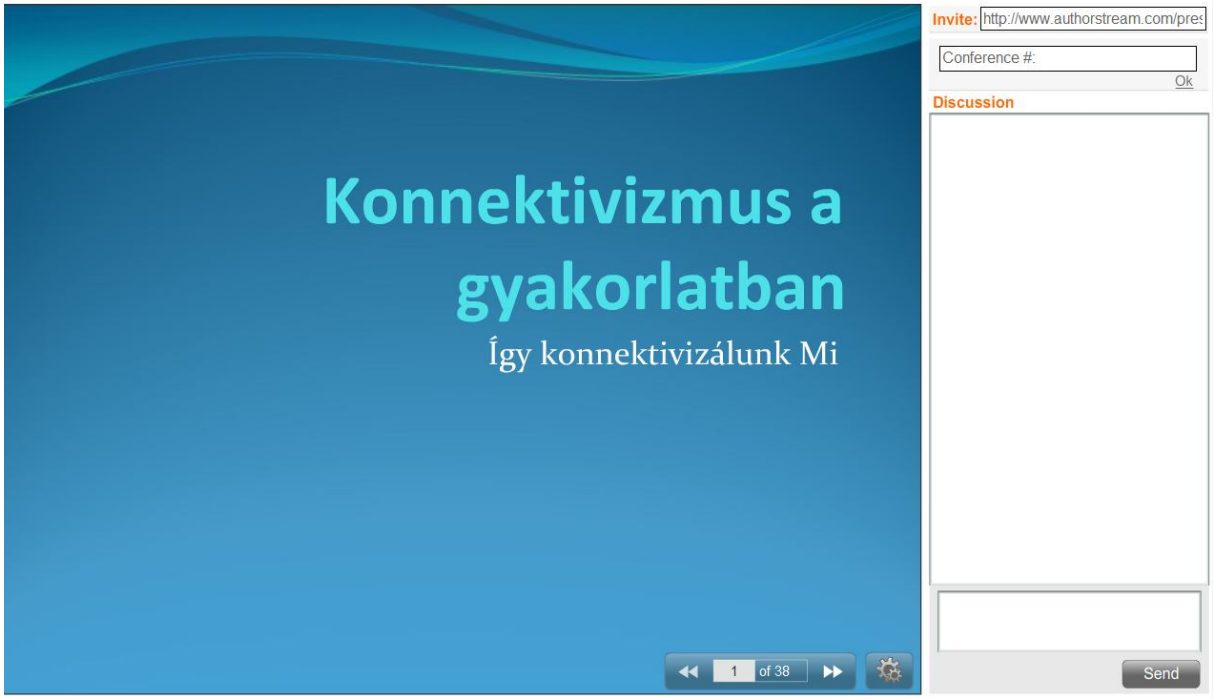
Az előadó számítógépére telepített Ustream Producer „keverőpult” (18. ábra) segítségével lehet válogatni az adásba kerülő médiaanyagok között.

A hallgatókkal – a Google Docs és az authorSTREAM portálokhoz hasonlóan – párhuzamos chat-ablakban lehet tartani a kapcsolatot.

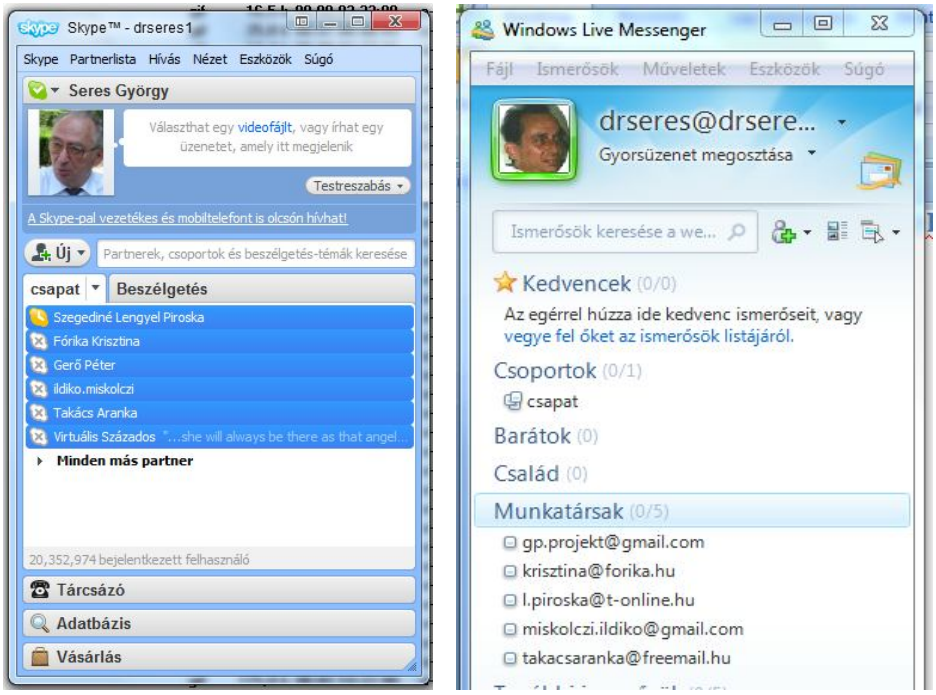


12. ábra. Online bemutató a Google Docs portálon

[12] http://docs.google.com/a/drseres.com/present/view?id=dgdg6bm9_669fw43zwhb&invite=906859995
[13] http://www.authorstream.com/presentlive/291884_633964445461711250
[14] http://www.wiziq.com/drseres
[15] http://my.dimdim.com/drseres
[16] http://www.ustream.tv/channel/drseres



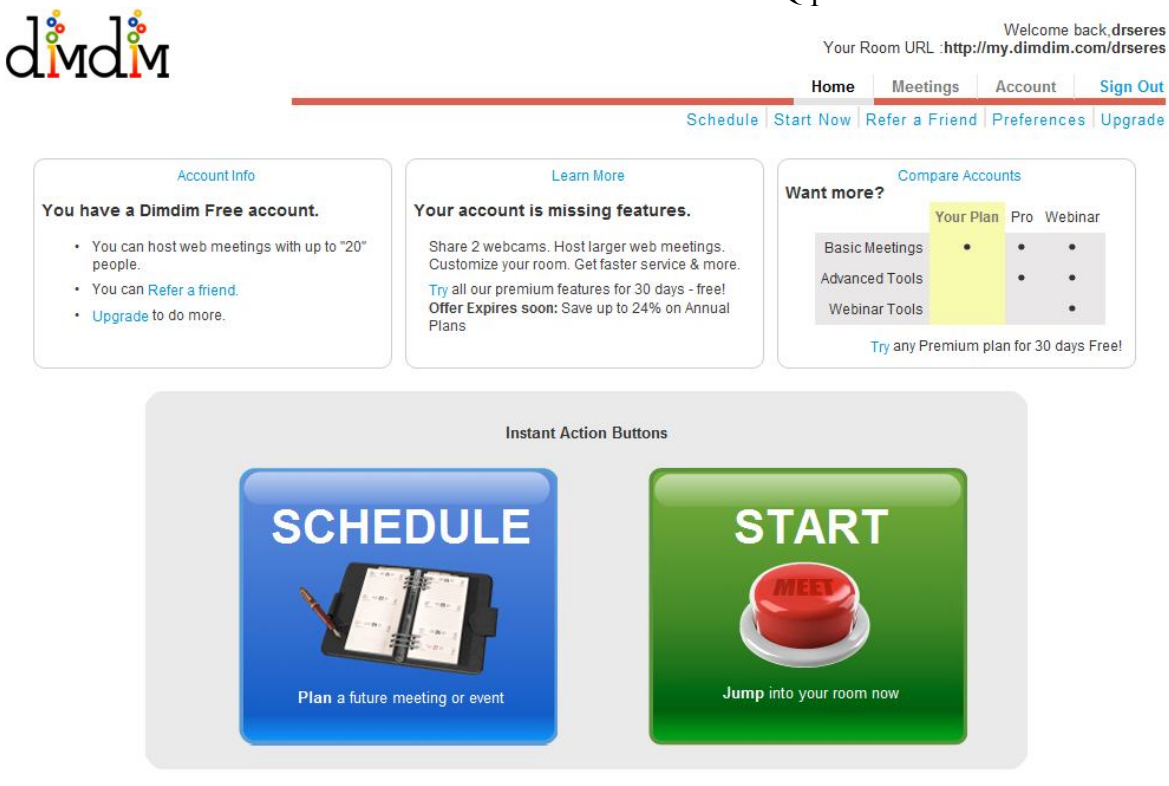
13. ábra. Online bemutató az authorSTREAM portálon



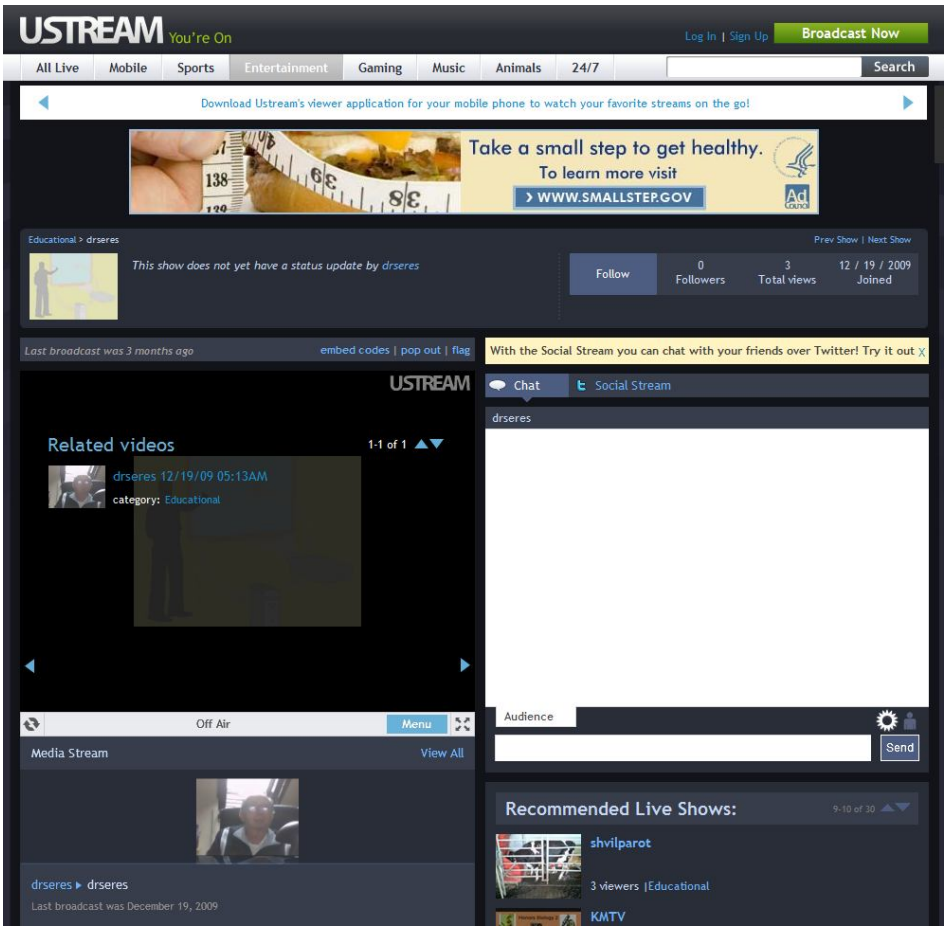
14. ábra. Konferenciahívás a Skype és a Windows Live Messenger útján



15. ábra. Online tanóra felvétele a WiZiQ portálon



16. ábra. Virtuális tanóra indítása a DimDim portálról



17. ábra. Videó előadás felvétele a Ustream portálon



18. ábra. A Ustream Producer "keverőpult"

BLOG

A számítógépfelhők legdivatosabb szolgáltatása, a blog, alkalmazható az oktatási folyamatban is – a tanárok és a tanulók is vezethetnek saját, nyilvános, vagy zártkörű internetes naplót, amelyben szabadon kifejthetik gondolataikat a tanultakról, hallgatótársaikról és tanáraikról.

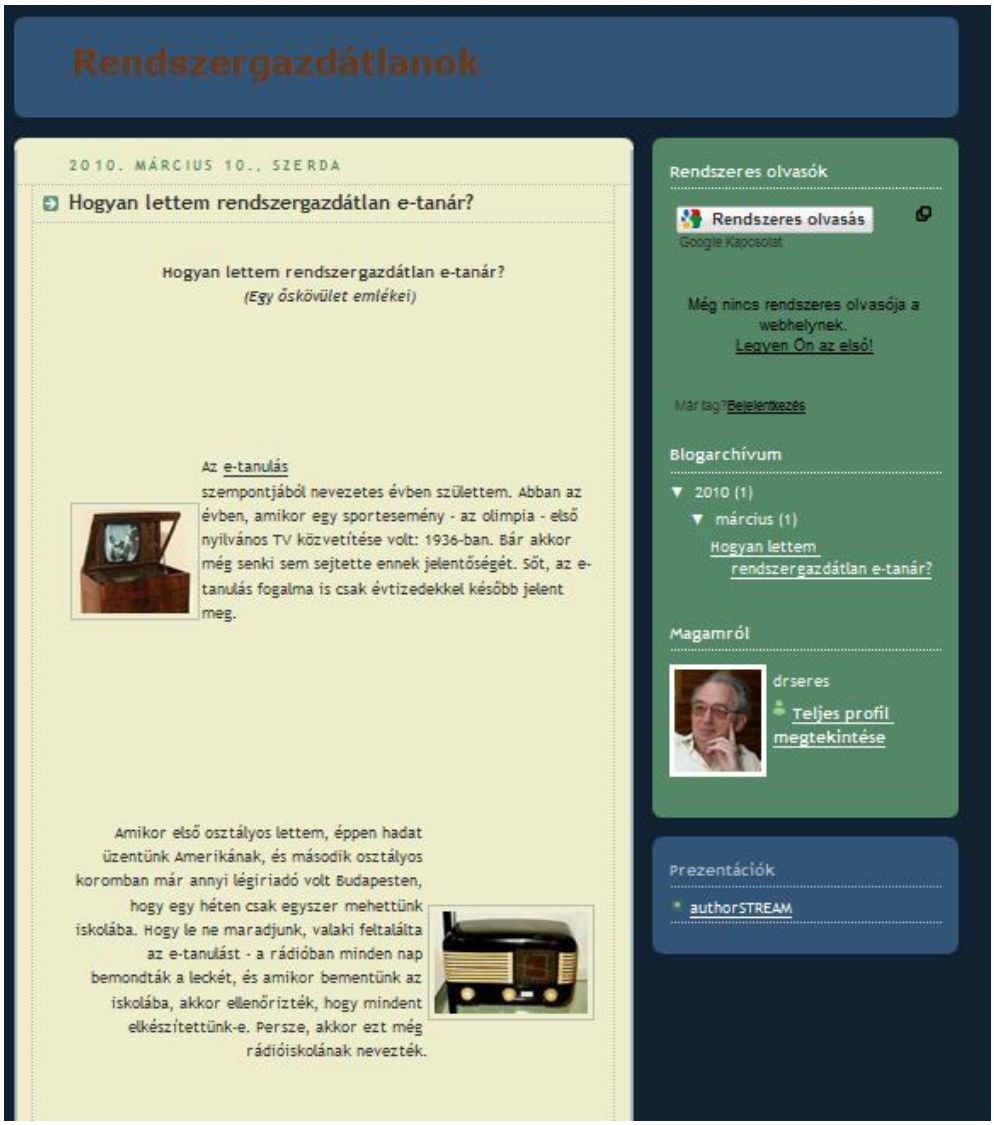
A legelterjedtebb blog-szolgáltatók, a Google által üzemeltetett Blogger[17] (19. ábra), és az önálló Wordpress[18] (20. ábra) portálokon, elsősorban szöveges – linkekkel és képekkel bővített – bejegyzések (ún. post-ok) szerepelnek

Vegyes – szöveget, képet és videoklipet tartalmazó – bejegyzések naplószerű megjelenítésére alkalmas a tumblr[19] portál.

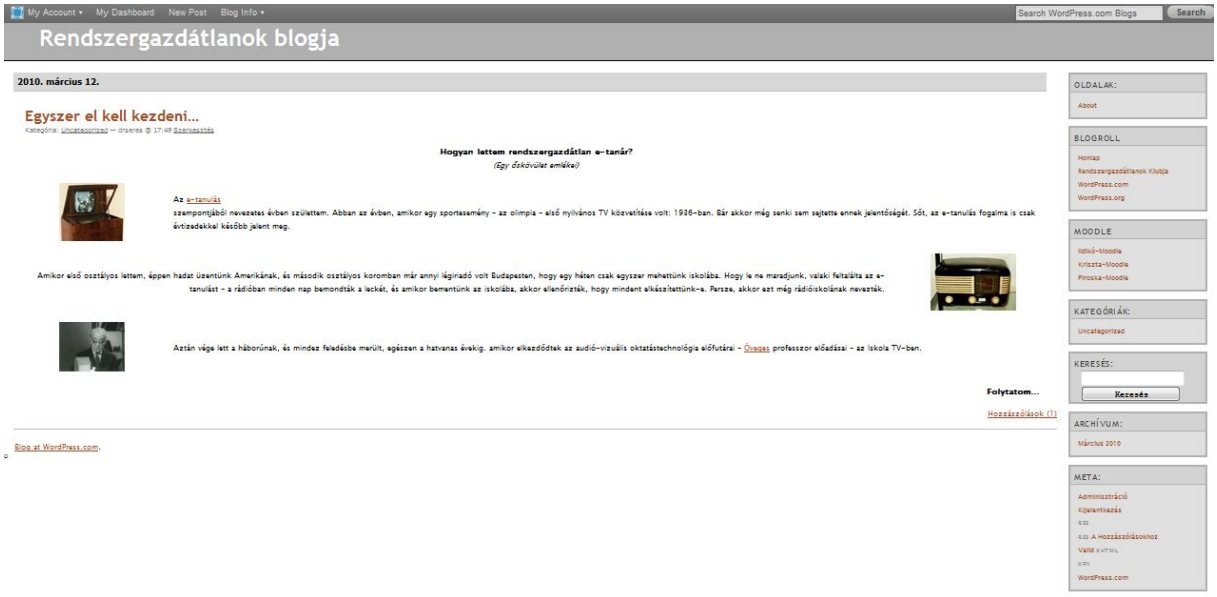
Egy oktatási csoport nyilvános hirdetőtáblájának alkalmas, az egyszerűen szerkeszthető, Wallwisher[20] portál szolgáltatása.

De a legtöbb oktatásvezérlő (LMS) rendszer – például, a Moodle[21], vagy az Ilias – portál is biztosít a résztvevőknek egyszerű blog-szolgáltatásokat.

[17] http://drseres.blogspot.com/
[18] http://drseres.wordpress.com/
[19] http://etanar.tumblr.com/
[20] http://www.wallwisher.com/wall/drseres
[21] http://www.miskolczi.net/moodle/blog/index.php?filtertype=site&



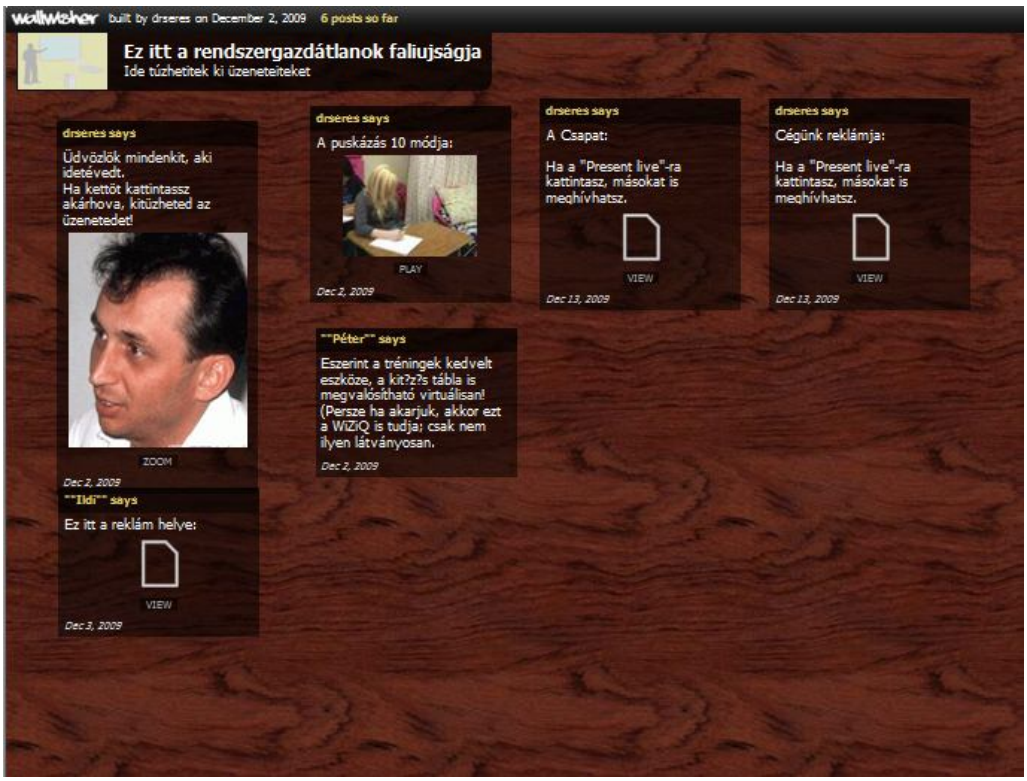
19. ábra. Blogbejegyzés a Blogger portálon



20. ábra. Ugyanaz a blogbejegyzés a Wordpress portálon



21. ábra. Szöveges és beágyazott prezentáció a tumblr portálon



22. ábra. A Wallwisher portál hirdetőtáblájára “ragasztott” szöveges, képes és videó üzenetek



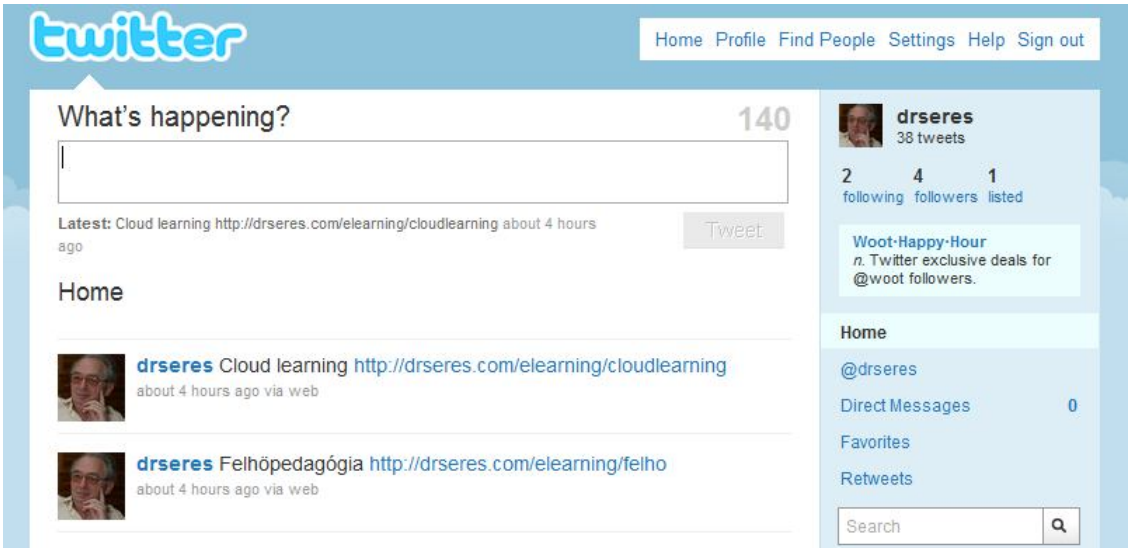
23. ábra. Blogbejegyzés a Moodle portálon

KÖZÖSSÉGI PORTÁLOK

A számítógépfelhőkben kialakítható közösségi szolgáltatások is hasznosíthatók az oktatás és a tanulás folyamatában – különösen hasznosak az így létrejövő közösségi kapcsolatok a hálózatalapú tanulásban.

A legelterjedtebb közösségi portálok közé tartozik a rövid, szöveges üzeneteket közhírré tevő (csiripelő) twitter[22] (24. ábra), illetve az ismerősök keresésére, és a velük való kapcsolattartásra szakosodott facebook[23] (25. ábra), és a magyar iWiW[24] (26. ábra) portál.

A különböző szakmák művelői közötti együttműködésre specializálódott LinkedIN[25] (27. ábra) közösségi portál is hasznos szakmai és üzleti kapcsolatok létrehozását és fenntartását teszi lehetővé.



24. ábra. „Csiripelés” a twitter portálon

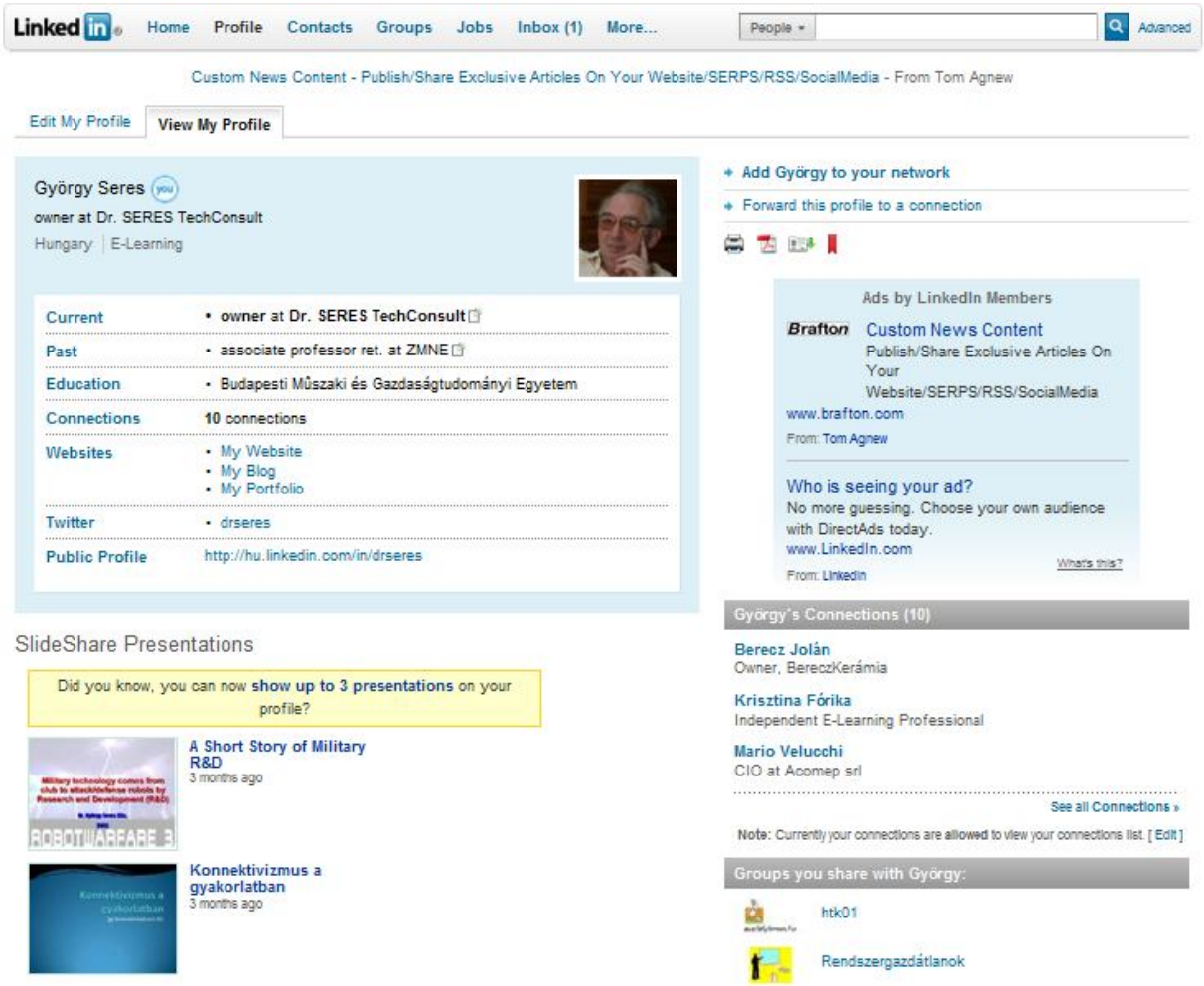
[22] http://twitter.com/drseres
[23] http://facebook.com/drseres
[24] http://iwiw.hu/pages/user/userdata.jsp?userID=14773705
[25] http://www.linkedin.com/in/drseres



25. ábra. Aktuális üzenetek a facebook portálon



26. ábra. Az iWiW portálon is létrehozhatunk saját klub-portálokat

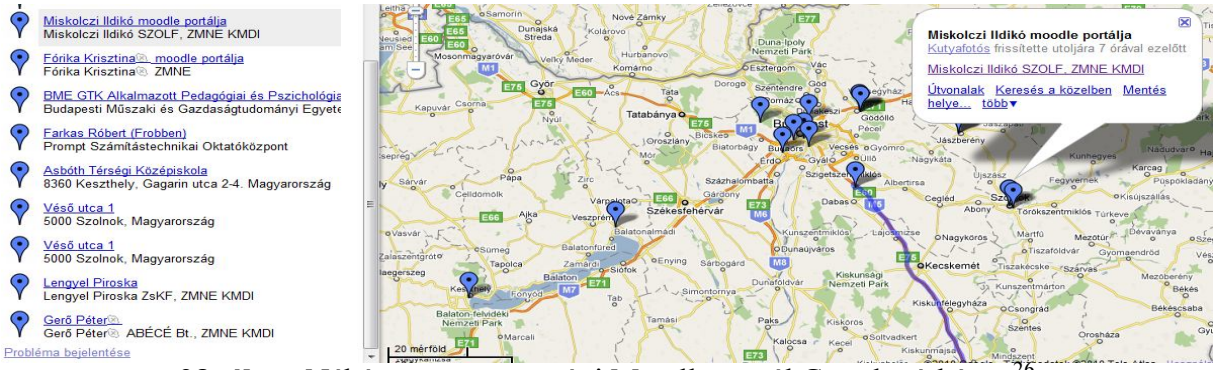


27. ábra. Szakmai profil a LinkedIN portálon

OKTATÁSSZERVEZŐ RENDSZEREK

A nagyobb cégek – Oracle, Microsoft, Adobe, stb. - bérelhető, vagy megvásárolható oktatásszervező (LMS – Learning Management System) rendszerei mellett, a számítógép-felhőkben sok, ilyen célú, szabad-felhasználású rendszer is található.

Ezek közül a legelterjedtebbek a Moodle és az Ilias, amelyeket már sok magyar felsőoktatási intézmény és távoktatással foglalkozó vállalkozás, sőt oktató is alkalmaz (28. ábra).



28. ábra. Néhány magyarországi Moodle portál Google térképen[26]

ELLENŐRZŐ ÉS ÖNELLENŐRZŐ TESZTEK

A számítógép-felhőkben működő, oktatás-informatikai szolgáltatások közül több is lehetőséget biztosít az online önellenőrzésre és tanári ellenőrzésre is.

Készíthetünk online kérdőíveket a Google Docs[27] (29. ábra) alkalmazásával, amelyeket kitöltés és beküldés után külön táblázatban értékelhetünk.

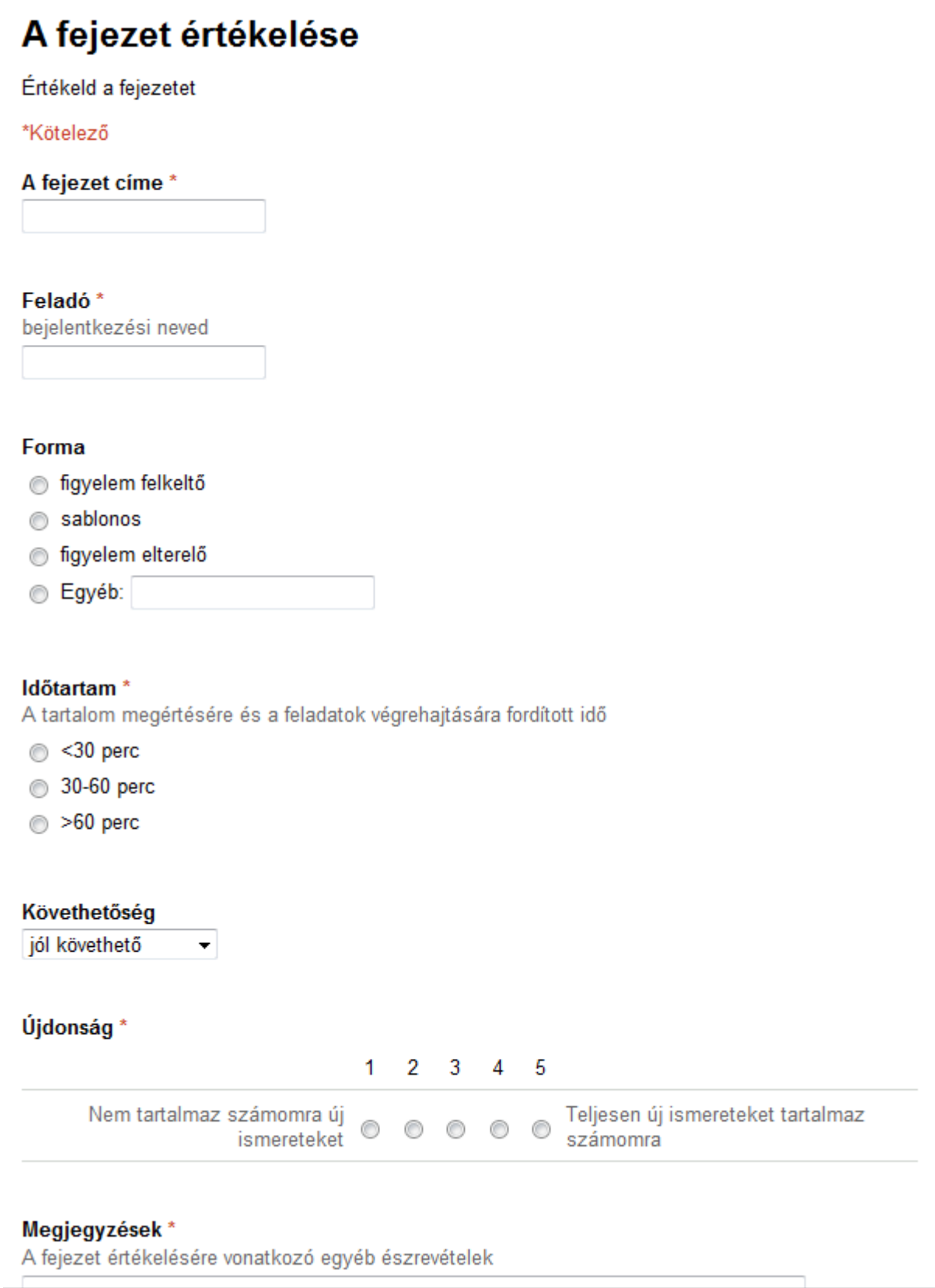
Egyes virtuális-tanterem szolgáltatások, és a tanulásszervező rendszerek is biztosítanak tesztkészítési eszközöket[28].

Hatékony, érdekes és látványos teszteket készíthetünk olyan, speciális, szabad-felhasználású tesztkészítő programokkal, mint a Hot Potatoes[29] (30. ábra) és a Quandary[30] (31. ábra).

26 http://maps.google.com/maps/ms?ie=UTF8&hl=hu&source=embed&msa=0&msid=101603881709700285892.000456741957ac82e86b4&ll=47.724545,18.775635&spn=4.404937,11.634521&z=7

27 http://spreadsheets.google.com/a/drseres.com/viewform?key=0Akgnf94P4BXVcEVpbDRSN1hRWEV5Y1ZPcXBvVVRpTUE&hl=hu

28 http://www.geropeter.hu/moodle/mod/quiz/view.php?id=228
29 http://drseres.com/elearning/tesztek/hotpot/index.htm
30 http://drseres.com/elearning/tesztek/quandary/index.htm



A fejezet értékelése

Értékeld a fejezetet

*Kötelező

A fejezet címe *

Feladó *
bejelentkezési neved

Forma

- figyelem felkeltő
- sablonos
- figyelem elterelő
- Egyéb:

Időtartam *
A tartalom megértésére és a feladatok végrehajtására fordított idő

- <30 perc
- 30-60 perc
- >60 perc

Követhetőség
jól követhető

Újdonság *

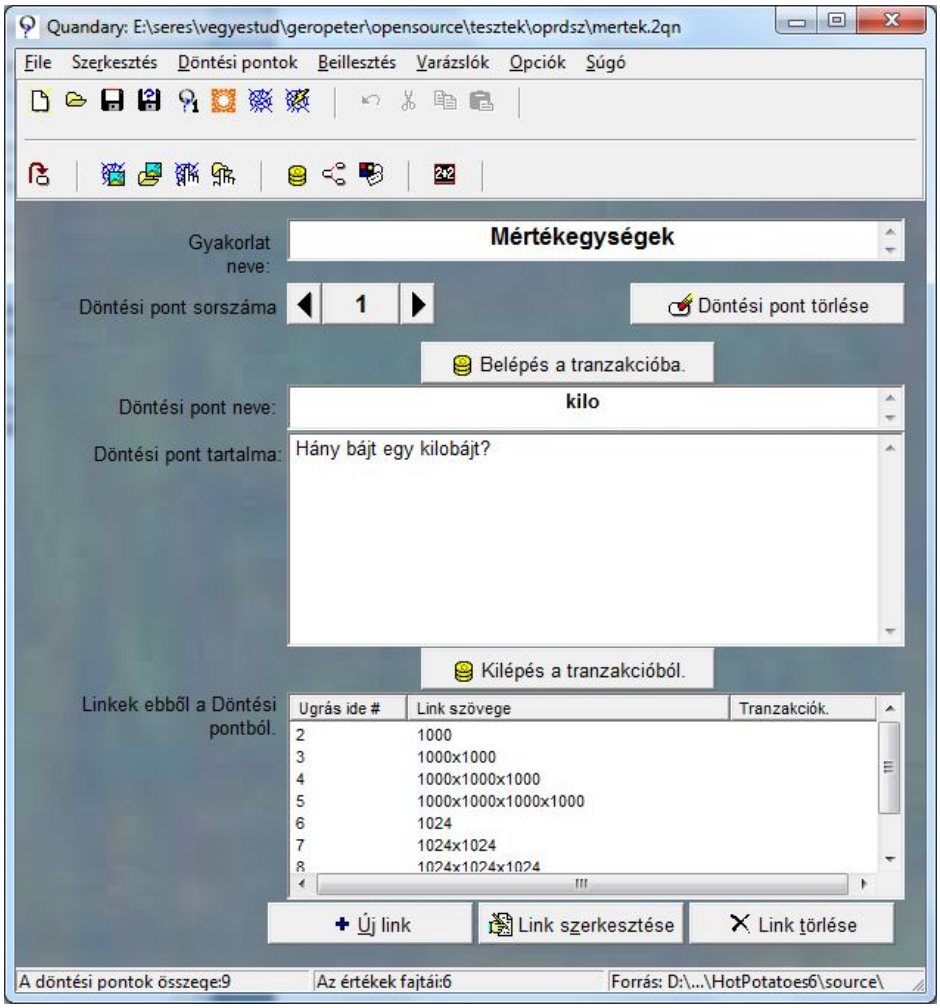
	1	2	3	4	5	
Nem tartalmaz számomra új ismereteket						Teljesen új ismereteket tartalmaz számomra

Megjegyzések *
A fejezet értékelésére vonatkozó egyéb észrevételek

29. ábra. Fejezet-értékelő kérdőív a Google Docs szolgáltatásában



30. ábra. A Hot Potatoes tesztkészítő szoftver indulóképe



31. ábra. Egy döntési pont szerkesztése a Quandary tesztlabirintus-szerkesztő szoftverrel

RENDSZERGAZDÁTLANOK KLUBJA

A ZMNE Katonai Műszaki Doktori Iskolájában, 2007-ben meghirdetésre került egy kutatási téma[31], *„Az e-tanulás (e-learning) és a távoktatás alkalmazása a katonai felsőoktatásban”*, valamint egy tantárgy[32], *„Az interaktív tudásátadás informatikai alapjai”* címmel.

Mivel egy tíz éve működő honlap már nem volt alkalmas az interaktív távoktatásra, ezért a „felhők” között útnak indult egy Drupál motorral működő, Web-2 portál, E-TANÁR néven[33] (32. ábra).

A nagy keresőmotorok gyorsan felfedezték a portált, és - minden reklám nélkül -, viszonylag sok látogatót vonzottak a világ minden tájáról (33. ábra).

A portálon elindult egy távoktatási kurzus. A távoktatási kurzust sokan elkezdték - többen be is fejezték.

Végül összeállt egy kis, hatfős csapat – a Rendszergazdátlanok Klubja, mely nevet a portál is felvette (34. ábra).

A mai napig hetenként összejövünk a „felhők között”.

Az eredmény: több önálló és közös publikáció, konferencia-előadás, díjnyertes pályázat [1.-11.], három doktoranduszhallgató és négy önálló Moodle portál (35.-38. ábrák).

És nagyon sokat tanulunk egymástól.

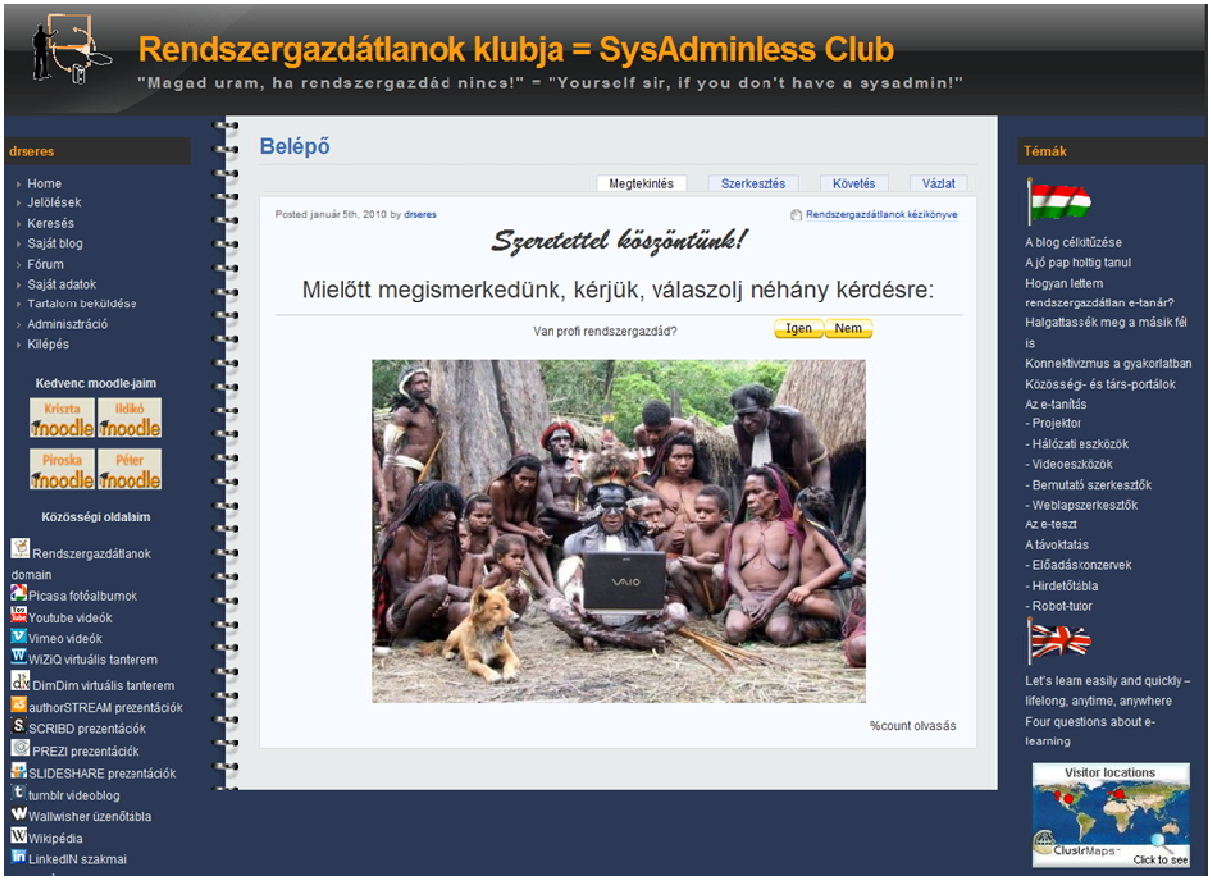


32. ábra. Az E-TANÁR portál

[31] http://www.zmne.hu/kmdi/kuttema_2007.html#3
[32] http://www.zmne.hu/kmdi/tantargy/eh4.html
[33] http://drseres.com/elearning



33. ábra. Az E-TANÁR portál látogatottsága



34. ábra. A portál új nyitóoldala



35. ábra. Miskolczi Ildikó Moodle portálja[34]



36. ábra. Fórika Krisztina Moodle portálja[35]

[34] http://miskolczi.net/moodle
[35] http://forika.hu/moodle



37. ábra. Lengyel Piroska Moodle portálja[36]



38. ábra. Gerő Péter Moodle portálja[37]

[36] http://www.lengyelpiroska.hu/moodle
[37] http://www.geropeter.hu/moodle

ÖSSZEFOGLALÁS

Egy ilyen áttekintésnek többféle összefoglalása is lehet. Megkérdezhetjük, hogy vajon melyek a fejlődés fő irányai. Elemezhetjük, hogy mi lehet a titka egyik vagy másik megosztó vagy közösségi oldal, portál sikerének. Összevethetjük őket technikai adataik szempontjából. A jelen tanulmány szerzői azonban a gyakorlatban kívánják használni a céljaiknak, szempontjaiknak megfelelő szoftver-segédeszközöket és -felhőket. Ez pedig az alábbi záró gondolatokat inspirálja: A felsorolt (és ezeken kívül még létező) lehetőségek sokasága már messze túl van az áttekinthetőség határán. A felhasználás nehézségét éppen a bőség zavara okozza. Akik ezeket a rendszereket használják, véletlenszerűen, divat szerint vagy esetleges szempontok alapján teszik. Léteznek ugyan összehasonlítások, de ezek jelentős hányadát a fejlesztők készítik, ezért az elfogulatlanságukban nem lehetünk biztosak - és egyébként is: "technikai adatok" alapján hasonlítják össze az egyes rendszereket. A pedagógiai szempontokhoz, a tanulói sikerességhez, a képzési hatékonysághoz kapcsolódó (ezeket akár csak szempontként felvető) összevetéseket nem ismerünk; egy ilyen (gyakorlaton, méréseken alapuló) összevetés meg is haladja jelen tanulmány kereteit. A legfontosabb következtetést azonban már most levonhatjuk. Az eszközök készen állnak a rugalmasabb és ugyanakkor hatékonyabb megoldásokhoz; itt az idő, hogy a módszertanok és eljárások, a tanuló és a tananyagszerző felkészítése, azaz az emberi faktorok is utolérjék őket.

IRODALOM

[1.]Kende György, Seres György: Egy interaktív e-learning portál első tapasztalatai, (Workshop 2008 of Knowledge Management Sub-board of Hungarian Academy of Science, Budapest)
http://vati.szie.hu/files/vati/mta-2008.pdf (2010.04.13.)

[2.]Kende György, Seres György, Miskolczi Ildikó, Hangya Gábor: Virtuális Campus, (Award of Zrínyi Miklós Fundation on Military Sciences, Budapest, 2008)
http://drseres.com/publik/pdf/virtuális_campus.pdf (2010.04.13.)
http://drseres.com/publik/pdf/virtual_campus.pdf (2010.04.13.)

[3.]György Kende, György Seres, Ildikó Miskolczi: Let's learn easily and quickly – lifelong, anytime, anywhere (Jampeper.eu, online quarterly 3./III./2008)
http://www.jampaper.eu/Jampaper_E-ARC/No.3_III._2008_files/JAM080302e.pdf (2010.04.13.)

[4.]Miskolczi Ildikó, Seres György: "Egy interaktív e-learning portál első tapasztalatai egy e-diák és egy e-tanár szemszögéből" (Workshop 2008 of Knowledge Management Sub-board of Hungarian Academy of Science, Budapest)
http://vati.szie.hu/files/vati/Miskolczi.ppt (2010.04.13.)

[5.]Seres György, Miskolczi Ildikó, Szabó László: Hatékony felsőoktatás – az Internet lehetőségei a távoktatásban (Scientific Conference on the Day of Earth, Szolnok, 2008)
http://portal.zmne.hu/download/bjkmk/bsz/bszemle2008/4/05_Seres%20Gyorgy.pdf (2010.04.13.)

[6.]Seres György, Kende György, Miskolczi Ildikó, Fórika Krisztina: Az e-tanulás lehetőségei a külszolgálatot teljesítő katonák képzésében (Scientific Conference ZMNDU, Szolnok, 2009)
http://www.szrfk.hu/rtk/kulonszamok/2009_cikkek/Kende_Gyorgy-Miskolczi_Ildiko_stb.pdf (2010.04.13.)

[7.]Miskolczi Ildikó: A tudásprezentálás elmélete és gyakorlata az e-learningben (Hadmérnök, 2009/2.)
http://hadmernok.hu/2009_2_miskolczi.php (last download: April 13. 2010)

[8.]György Kende, György Seres, Ildikó Miskolczi, Gábor Hangya: Virtual Campus (New Challenges in the Field of Military Sciences 6th International Scientific Conference Budapest, Hungary, 2009, Proceedings CD-ROM ISBN 978-963-87706-4-6)
http://drseres.com/publik/pdf/virtual_campus.pdf (2010.04.13.)

[9.]Seres György, Miskolczi Ildikó, Fórika Krisztina, Hangya Gábor: Terepi kivitelű moodle munkaállomás alkalmazhatósága a katonai továbbképzésben (Hadmérnök, 2010/1.)
http://www.hadmernok.hu/2010_1_seres_etal.php (2010.04.13.)

[10.] Fórika Krisztina, dr. Miskolci Ildikó: Agorák a XXI. században, avagy a virtuális terek közösségépítő szerepe, (Multimédia az oktatásban , tudományos konferencia, Debrecen, 2009.)
http://mmo2009.kfrtkf.hu/file.php/1/MMO2009_Programfuzet_v5.pdf (2010.04.13.)

[11.] Seres György, Fórika Krisztina, Miskolczi Ildikó: Az E-Tanár=E-Portál Közösség Oktatási Oldalai - Fórika-Moodle és Miskolczi-Moodle, távoktatásban (Scientific Conference on the Day of World Sciences, Szolnok, 2009)
http://www.szolnok.mtesz.hu/sztk/kulonszamok/2009/cikkek/Seres_Gyorgy-Forika_Krisztina-Miskolczi_Ildiko.pdf (2010.04.13.)

HADMÉRNÖK
V. Évfolyam 2. szám - 2010. június

Szegediné Lengyel Piroska
l.piroska@t-online.hu

SZÁMÍTÓGÉPES BŰNÖZÉS AVAGY FIATALOK A CYBER-TÉRBEN

Absztrakt

A cikk az életünkre komoly kihatással bíró informatika és számítástechnika fejlődésének árnyoldalát, a számítógépes bűnözést, a számítógépes hálózatok, az internet segítségével elkövetett támadások potenciális elkövetőit, az indítékokat próbálja bemutatni. Egy-két évtizeddel ezelőtt a számítógépes bűnözés még közel sem jelentett akkora veszélyt, mint manapság, de mára kimondhatjuk, társadalmi problémává nőtte ki magát. Modern korunkban a számítástechnika egyre nagyobb területeket hálóz be, így a kvalifikált, de az átlag ember is, sőt sajnálatos módon a kiskorú vagy kamasz fiatal is – esetleg tájékozatlansága, járatlansága, vagy egyszerűen figyelemkeltés céljából - sokszor tudatosan, sokszor akár akaratán kívül is elkövethet bűncselekményeket. Fontos társadalmi elvárás, tudatosítani a közvéleményben, hogy a technika gyors fejlődésével, a számítógépek, s főleg a hálózatok elterjedésével, a számítógépes bűnözés világméretűvé duzzadt, így mind több és több ember életére van kihatással, ezért komoly veszélyt jelent, amit nem lehet egyetlen kézlegyintéssel elintézni.

The article is to assist the reader to have a look at the shadow side of the development in the informatics and computer techniques, which have a great impact on our daily life; to present the computer based criminalities, the potential transgressors of attacks committed via computer networks, through the world wide web and to show the reasons laying behind the criminalities. One or two decades ago, the computer based criminalities represented far less risks than they do nowadays, as they became a major social problem to the present time. In our modern age, as computer techniques is conquering greater and greater fields, crimes might be committed by people with high qualification and even by average ones or more over, unfortunately, by small children or teenagers – several times in a willful way, but many times without any will – due perhaps to misunderstandings, misproceedings or to actions when someone would simply draw other's attention. It is an important social requirement to make people understand that due to the rapid technical development, to spreading out of computers and computer networks, the computer based criminalities have been pullulated throughout the entire world, thus the criminalities have a major

threatening impact on more and more people's life and this fact can not be neglected by a wave of hand.

***Kulcsszavak**: kritikus infrastruktúrák, cyber–tér, internet, hacker, terrorista, hardver, szoftver, vírus, információbiztonság ~ substantial infrastructures, cyber space, world wide web, hacker, terrorist, hardware, software, virus, security of information*

BEVEZETŐ

Az internet és más információs rendszerek utóbbi években tapasztalt erőteljes fejlődése lehetővé tette az információk, a termékek és a szolgáltatások gyors áramlását a világ országai határain átívelően. Ez nyilvánvalóan számos pozitív hatással jár, ugyanakkor számos új lehetőséget nyit a bűnözők részére. Egyértelműen megfigyelhető olyan újfajta bűncselekmények felbukkanása, amelyeket az internettel vagy információs rendszerek, mint eszközök felhasználásával követnek el. E bűncselekmények folyamatosan fejlődnek, és a jogalkotás, valamint az operatív bűnüldözés nehezen tud lépést tartani velük.

Az elmúlt években a biztonságpolitikával foglalkozó szakemberek által is megerősítést nyert, hogy a társadalom, a vállalkozások és a polgárok számára egyre nagyobb veszélyt jelent a **számítógépes bűnözés. Az aggodalmat** azonban valójában nem **a** számítógépes bűncselekmények erőteljes szaporodása okozza, hanem inkább ezen bűncselekmények kifinomultabbá válása, a számítógépes bűnözés elleni küzdelemmel kapcsolatos koherens politika és jogalkotás hiánya.

A közeli jövőben a társadalom, illetve az oktatási intézmények fontos feladata lesz a számítógépes bűnözés által jelentett veszélyekre való tudatos felkészülés, felkészítés, a számítógépes bűnözés szakismeretének megszerzésére és a védelmi technikai eszközök kifejlesztésére vonatkozó igény erősítése a leginkább érintettek körében.

De kik a leginkább érintettek? A számítógépes bűnözés a társadalom valamennyi területét érinti, így gyakorlatilag mindenhol fellelhető a vele szemben fellépő védekezés igénye. Érintett a közszféra, hiszen a mindennapi életünket kiszolgáló infrastruktúrákat számítógépes hálózatok működtetik és irányítják. De tekintettel arra, hogy ma, a XXI. században már nagyon sok ember használ magánszámítógépet, így a magánszférát is érinti a számítógépes bűnözés elleni küzdelmet célzó kezdeményezés, hiszen a magánszemélyek is potenciális áldozatok lehetnek

És kik a potenciális elkövetők és mik az indítékaik? A potenciálisan szóba jöhető elkövetőket a cyber tér szereplői között kell keresni – hackerek, hacktivisták számítógépes bűnözők, ipari kémek, vállalatok belső szakértői és külső szerződők, terroristák. [1] -, ugyanakkor potenciális elkövető lehet bárki – gyerek, fiatal kamasz, unatkozó felnőtt… -, aki az elkövetéshez szükséges, elegendő számítástechnikai ismeretekekkel és eszközökkel rendelkezik.

A számítógépes bűnözéssel kapcsolatos biztonsági kérdések átfogó jellegűek, így nem kezelhetők pusztán nemzeti szinten. A veszély nemzetközi jellegű, ezért – legalábbis részben – a válasznak is ilyennek kell lennie. A számítógépes bűnözés elleni küzdelem kétségtelenül továbbra is nemzeti szinten lesz a legfontosabb, egyértelműen szükséges azonban a nemzeti erőfeszítések összekapcsolása és esetleges kiegészítése európai szinten.

I. A SZÁMÍTÓGÉPES BŰNÖZÉS JELLEGZETES VONÁSAI

Bár a számítógépek elterjedésével (ami a 70-es évekre tehető) gyakorlatilag „egyidős" a számítógépes bűnözés, kb. a 80-as évekre tehető az a megállapítás, hogy a számítógépes bűnözés általános jelenséggé nőtte ki magát. Közrejátszott ebben a számítástechnika gyors fejlődése, a személyi számítógépek széleskörű elterjedése, az adatátviteli rendszerek robbanásszerű fejlődése, a szoftverkínálat rohamos bővülése, a bankkártyák elterjedése, és végül az, hogy a védelmi rendszerek fejlesztése elmaradt, ráadásul a meglévők is gyorsan „amortizálódtak" a számítástechnika gyors fejlődésének következtében.

A fejlődés okán a számítógépes bűncselekmények száma és típusai is megváltoztak. Megjelentek az adatmanipulálás útján elkövetett számítógépes csalások, számítógépes hamisítások, védett adatbázisok elleni támadások, illegális szoftver-másolás, terjesztés, visszaélés bankkártyával, telefonkártyával stb.

A helyzetet tovább rontotta a számítógépes hálózatok, s főleg az Internet elterjedése, aminek segítségével a bűncselekmények elkövetése gyorsabbá, leleplezésük még nehezebbé vált. Az 1990-es évektől a számítógépes bűncselekményeket egyre inkább az Interneten – mint legjelentősebb hálózaton – követik el, és az utóbbi években ez a tendencia egyre erősödik. Az Internet sajátos jellemzői – **a nyitottság, az interaktivitás, a decentralizáltság, a globalitás** [2] – teszik lehetővé, hogy a bűnözés számára ideális elkövetési területté váljék.

De mit jelent pontosan a számítógépes bűnözés fogalom? Annak ellenére, hogy a napjainkra a számítógépes bűnözés egyre elterjedtebbé, egyre jelentősebbé vált, még nincsen pontos - szakirodalom által egységesen elfogadott - meghatározása. Ennek oka feltehetően a jelenség változékonysága és sokszínűsége: amennyiben megszületik egy pontos definíció, könnyen lehet, hogy már nem sokat mond a jelenségről, annak változásai miatt.

A pontos fogalom-meghatározást talán az is gátolja, hogy nincs egységes álláspontom a szakirodalom a jelenség elnevezése tekintetében sem: **számítógépes bűnözés** vagy **informatikai, adat bűnözés** vagy **hitech bűnözés** vagy **cyber terrorizmus**?

Elnevezéstől függetlenül, egy olyan jelenséggel állunk szemben, amely minden társadalomra nézve veszélyes, mert egyrészt olyan tevékenység, amely számítógépes rendszerekbe történő közvetett, vagy közvetlen behatolással anyagi, illetve szellemi javakban kárt okoz, másrészt az információ-technológiai eszközök, rendszerek, illetve rendszerelemek ellen irányul, illetve ezeket az eszközöket, rendszereket használja a bűncselekmények elkövetésének eszközeként.

A számítógépes bűnözés egyik **fő jellegzetessége** a **gyorsaság**, amely az eredmény realizálódására vonatkozik. A gyorsaság, tehát nem azt jelenti, hogy a bűncselekmények a pillanat szülöttei, bár ez is gyakori eset, de az „akciók" többségére nem ez jellemző, hiszen tudjuk, hogy a legtöbb ilyen bűncselekmény komoly előkészületeket igényel. Az elkövetéseket megelőzi a megfelelő szoftverek beszerzése, azok kezelésének megismerése, biztonsági rendszerek kiismerése, információk beszerzése, gyűjtése és mindezek mellett hosszú tanulás (pl.: főiskolákon, egyetemeken, vagy autodidakta módon), és nem utolsó sorban gyakorlatszerzés.

Modern korunk technológiai, technikai színvonala, az egyre gyorsabb számítógépek, az elkövetők szakmai tudása és rutinja lehetővé teszik, hogy egyre gyorsabban lehet elkövetni a bűncselekményeket. Mindehhez hozzájárul az Internet elterjedése, így már világszerte, nehezen ellenőrizhető módon lehet, nagy gyorsasággal elkövetni számítógépes bűncselekményeket. [3]

A számítógépes bűnözés területét jellemző **magas látenciának** több oka van: Egyik, hogy a bűncselekmények egy része sokszor még a sértett előtt is rejtett marad pl.: betörnek a számítógépére, s másolatot készítenek egyes filekről, de nem észleli azt. A magas látencia másik fő okát egy elég sajátos jelenségben kell keresnünk, abban, hogy az esetek egy részét a sértettek nem jelentik. Ez általában a gazdálkodó szervezetekre és főleg a hitelintézetekre, biztosítókra jellemző, akiknek komoly érdeke fűződik ahhoz, hogy titokban maradjanak az esetek. „…… naponta tapasztaljuk, hogy a médiában bemutatni egy-egy informatikai támadást igen nehéz feladat, ennek következtében számos alkalommal még a sikeres támadásokat és azok következményeit is elhallgatják a megtámadott rendszerek üzemeltetői. Ebben élen járnak a bankok, bár az ő esetükben (is) komoly anyagi veszteséget okozhat – akár közvetett módon, pl. bizalomvesztés miatt – egy-egy ilyen támadás. Így többé-kevésbé érthető, ha nem, vagy nem szívesen ismertetik az ilyen eseteiket. Ugyanakkor azt is el kell mondani, hogy a kritikus ágazatok közül pont a pénzügyi szektor, ezen belül is a bankok azok, amelyek a lehető legtöbb figyelmet fordítják a fizikai védelem mellett az információs rendszereik védelmére". [4] A látenciát tovább fokozza, hogy a tettesek felfedezésének alacsony az esélye, mivel általában nem tartózkodnak az elkövetés helyszínén, az akciókhoz nincs szükségük külső segítőkre, így a kommunikációs csatornákon könnyedén és nyomtalanul eltűnhetnek.

Hangsúlyozni szükséges a számítógépes bűnözés erős **nemzetközi jellegét** is, többek közt azért, mert az elkövetők az Internetet, vagy egyéb más számítógépes hálózatot használnak a bűncselekmények során. Az Internet egy olyan virtuális világ, melyben nincsenek államhatárok, a névtelenség álarca mögé bújhat bárki. Kedvez az elkövetőknek, hogy az Internet hatalmas adatállományát, adatforgalmát nem lehet ellenőrizni, így a visszaéléseket nagyon nehéz nyomon követni.

Mindezek függvényében leszögezhetjük, hogy a számítógépes bűnözés rendkívüli mértékben függ a **technológia, technika fejlettségi szintjétől**, hogy a számítástechnikai eszközök, és azok rohamos fejlődése nélkül elképzelhetetlen lenne a létezése. Megfigyelhető az a tendencia, hogy amint kifejlesztenek egy újabb számítástechnikai vívmányt – hardvert, szoftvert…. – a bűnözők idővel felhasználják azokat az elkövetés során. Ha tehát valaki véget akarna vetni a számítógépes bűnözés fejlődésének, annak az alapot képező technikai fejlődést is meg kellene állítania.

A számítógépes bűnözés **intellektuális bűnözésnek** nevezhető, mert kialakulásához, a technológiai háttér mellett, jól képzett szakemberek *tömeges* megjelenésére és *tömeges* képzésére volt/van szükség. Amennyiben áttekintjük a számítógépes bűnözés fejlődését, észrevehetjük, hogy amíg a technika és a szakképzés nem vált tömegessé, addig nem is ölthetett olyan méreteket, mint napjainkban.

Az elkövetők **általában fiatal, magasan képzett, magas intelligenciájú, számítógépes szakemberek,** akik nem ritkán 2-3 fős csoportokba szerveződve követik el a bűncselekményeket a globalizáció és a technika, elsősorban az Internet felhasználásával. Az esetek többségében sokoldalúan szocializált elkövetőkről beszélhetünk, akik tisztában vannak

a jogaikkal, akik szakképzettségük miatt jó egzisztenciális körülmények között élnek. Természetesen olyan számítógépes bűncselekményekkel is találkozunk, amelyek elkövetése nem igényel magas szakképzettséget, az okozott kár azonban meglehetősen jelentős: vírusok, trójai programok… [5]

Összegezve elmondhatjuk, hogy az internet térnyerésével az emberi közösségek számára kitárult a világ, bárki számára hozzáférhetővé váltak eddig ismeretlen, vagy nehezen hozzáférhető információk, felgyorsult a kommunikáció, on-line üzenetváltások. Az internet hihetetlen lehetőségek tárát nyitotta meg, amely újfajta gondolkodást igényel az emberektől. Mára elmondhatjuk, a bűnözés új ága fejlődött ki, sokkal védtelenebbé téve az embereket, gazdálkodó szervezeteket. Gyermekek, személyes adatok, üzleti, szolgálati és államtitkok kerülnek veszélybe, gyanútlan embereket használnak ki, hatalmas méretű csalásokat hajtanak végre, amivel akár nemzetek gazdaságát dönthetik romba a láthatatlan bűnözők.

II. A SZÁMÍTÓGÉPES BŰNÖZÉS ÉRINTETTJEI

Az információs bázisokon a potenciális elkövetők különböző számítógépes hálózatok működési mechanizmusa után kutatnak. Kiemelt fontosságot képeznek számukra az olyan struktúrák, amelyek:

- közlekedési rendszerek ellenőrzésére szolgálnak, elsősorban a légi és vasúti közlekedés irányítására szolgáló infrastruktúrák
- állami intézmények - kiemelten a katasztrófa-elhárítással és a személyes adatok tárolásával megbízott intézmények, a távközlési hálózatok - igényeit szolgálják ki
- nem állami, de létfontosságú feladatot ellátó szervezetek működését támogatják, mint például a bankok, pénzintézetek vagy az áramszolgáltatók. [6]

Bár a hálózatok általában technikailag igen jól védettek, biztonsági protokollokkal nehezítve az adatokhoz való hozzáférést, mégis a tervezőknek több olyan körülménnyel is számolniuk kell, amelyek áthatolhatóvá teszik az egészen biztonságosnak hitt rendszereket is.

Különös figyelmet érdemelnek a napjainkban egyre jobban elterjedőben lévő számítógépes banki rendszerek, amelyeken pénzügyi tranzakciók sokaságát hajtják végre, így viszonylagos rendszerességgel esnek áldozatul támadási kísérleteknek is. Az elkövetők a rendszereket nemcsak illegális átutalásokra, hanem zsarolásra, üzleti tranzakciók megbénítására is használhatják

Az utóbbi években bizonyosságot nyert, hogy a számítógépes bűnözések tulajdonképpen bárki ellen irányulhatnak, mégis leszögezhető, hogy az elkövetők fő célpontjai. - a bűncselekmények többségében - a vállalatok.

A vállalatok, hivatalok sérelmére elkövetett bűncselekmények közül súlyuknál és számuknál fogva kiemelkednek az adatok megszerzésére, vagy manipulálására irányuló bűncselekmények, valamint az anyagi haszonszerzést célzó bűnelkövetések is. Ezeknél a bűncselekményeknél gyakran a sértettek könnyelműsége vezet oda, hogy áldozattá válnak. Nem vigyáznak kellőképpen jelszavaikra, amit ha, megszereznek az elkövetők, könnyen bejuthatnak a kérdéses rendszerekbe.

Összegezve megállapítható, hogy az Interneten végrehajtott támadások napjainkig egyelőre helyi jellegűek voltak határozott és pontos célokkal, ám a jövőben - szélesebb körű elterjedésükkel - nem zárható ki, hogy több támadás ér majd olyan nyílt rendszereket, amelyek létfontosságú infrastruktúrák, katasztrófavédelmi és pénzügyi létesítmények működését támogatják. Mindez megköveteli, hogy a jövőben kellő hangsúlyt fektessünk a számítógépes bűnözés elleni védekezés oktatására, mivel az emberek csak kellő informáltság mellett képesek felkészülni az ellenük irányuló támadásokra.

III. AZ ELKÖVETŐK

Amikor számítógépes bűnözésről beszélünk, megállapíthatjuk, hogy tulajdonképpen önmagában a technika nem veszélyes, az elkövetők azok, akik nem megengedett, illegális célokra használják.

Legelőször azt érdemes tisztázni ki válhat elkövetővé, milyen feltételeknek kell megfelelni? Véleményem szerint megfelelő szinten kell értenie a technikai eszközökhöz, azok kezeléséhez, olyan helyzetben kell lennie, amely lehetővé teszi számára a számítógép, vagy egyéb számítástechnikai eszköz használatát, aminek segítségével elkövetheti a bűncselekményt.

A tapasztalatok szerint társadalmi helyzetüket, munkakörüket tekintve **az elkövetők többsége magasan képzett, törekvő ember**. Többségük alkalmi haszonszerzés céljából követi el a bűncselekményt. Az elkövetők másik köre nem rendelkezik jelentősebb szakismerettel, olyan emberek, akik talán véletlenül döbbentek rá, hogy mi mindent tehetnek egy számítógéppel, s egyszerűen csak kihasználják az adandó alkalmat.

„Egy adott vállalat életében óriási szerepet játszanak a **szakértők,** akik sok esetben számos helyen - akár több telephelyen - is végzik munkájukat. A szakértők munkájuk elvégzése érdekében általában magas szintű hálózati hozzáféréssel rendelkeznek. Ebből következően adott esetben - pl.: munkahelyi konfliktusok, zsarolás, stb. - igen értékes adatokat tud eltulajdonítani, illetve akár különböző rosszindulatú programok bevitelére is lehetősége van, hiszen a hálózathoz belülről fér hozzá. A **külső szerződők** szintén kaphatnak hozzáférési jogokat a hálózathoz, és természetesen szintén számos igen értékes adathoz férhetnek hozzá, amelyekkel később visszaéléseket követhetnek el.” [1]

Megfigyelhető az is, hogy a számítógépes bűncselekményeket elkövetők gyakran bizalmi pozíciót töltenek be egy adott cégnél, ami nagyban megkönnyíti az elkövetést, hiszen az emberek bizalmával visszaélve könnyen hozzájuthatnak jelszavakhoz, s kijátszhatják a védelmi megoldásokat. A vállalatokat ért támadások közül komoly figyelmet érdemelnek a kívülről jövő támadások, amelyek esetében a támadók a **hackere**k.

„A hacker olyan személy, aki internet segítségével hozzá tud férni védett adatokhoz a számítógépeken. Kezdetben külön fogalmat alkottak a hackerek, akik azért törtek fel rendszereket, weboldalakat, illetve programokat, hogy bizonyítsák azok gyenge pontjait, azonban ezeket a hiányosságokat a rendszergazdák tudomására hozták, azaz általában jóindulatúan jártak el. Ők voltak az úgynevezett fehérkalaposok, azaz a "white hat" csoport tagjai. Az ellentábort azok a fekete kalaposok, "black hat" alkották, akik sokszor

rosszindulatból, vagy valamilyen haszonszerzés reményében hatoltak be egy-egy rendszerbe" [1]

A hackerek motivációik, céljaik elég eltérőek lehetnek: károkozás; védett adatok megszerzése, kíváncsiság, erőfitogtatás, tapasztalatszerzés, de utalva az előbbi meghatározásra, a „jó hackerek" segítő szándékkal törnek be egy rendszerbe. Felhívják a rendszergazda figyelmét a védelmi hiányosságokra, ezáltal segítik a hatékony védelmi rendszer kiépítését, Természetesen a jó szándék ellenére is komoly károkat okoznak, hiszen a rendszer feltörhető, irreleváns, hogy jobbító szándékkal törték-e fel vagy sem.

Napjainkra kialakult egy elkövetői réteg, az ún. **komputerunderground,** amely kategóriába az alábbi elkövetők sorolhatóak: [7]

- **Hackerek, crackerek** (A crackerek annyiban különböznek a hackerektől, hogy jellemzően haszonszerzési céllal törnek be védett rendszerekbe)
- **Phreakek** (Telefonvonalakba, illetve rendszerekbe próbálnak technológiai eszközökkel bejutni.)
- **Vírusírók** (Olyan személyek, akik olyan kódokat írnak, amelyek megpróbálnak behatolni más rendszerekbe, s gyakran mellékhatásokat is produkálnak)
- **Kalózok** (A crackerek közül váltak ki, szoftverek védelmi rendszereit feltörő személyek, akik e tőrt-szoftvereket terjesztik is.)
- **Cypherpunkok** (Olyan programokat terjesztenek, melyekkel bárki adatait erős kódolással láthatja el – nagy teljesítményű számítógépekkel is komoly feladat feltörni az ilyen erősen kódolt adatokat)
- **Anarchisták** (Törvénysértő, vagy legalábbis morálisan kétes megítélésű információkat terjesztő személyek. Olyan személyek, akik minden olyan kísérletet, rendelkezést elutasítanak, amely akadályozná az információ szabad áramlását)

Az elkövetők között meg kell említenünk a **terrorista** szervezeteket is, akik egyrészt propaganda, toborzás, adatszerzés céljából használják a számítógépes rendszereket, másrészt ezeken keresztül rombolnak, erőszakos bűncselekményeket hajtanak végre.

„A tapasztalatok szerint a független csoportok, hacktivisták által elkövetett incidensek előfordulási lehetősége nagy. Különösen igaz ez Magyarország esetében, hiszen a konfliktusokkal teli szomszédságpolitika bármikor elérheti azt a hatást, hogy a kormányoktól független szélsőséges csoportosulások néhány tízezer dollárnyi befektetéssel, mely akár nacionalista vállalkozói rétegtől vagy az alvilágtól is származhat, sikeresen zavarják meg hazánk mindennapos működését. Az országok közötti hasonló konfliktusok bekövetkezési valószínűsége kicsi, ám az informatikai kémkedés valószínűleg mindennapos, így a kritikus információs infrastruktúrák védelme mindenképpen kiemelt fontosságú." [4]

A támadásokat potenciálisan elkövetők típusa, száma igen nagy, és sajnálatos módon erőteljesen növekszik a deviáns, frusztrált, érzelmileg labilis fiatal kamaszok megjelenése a cyber–térben. Véleményem szerint egy átlagos számítástechnikai ismeretekkel rendelkező fiatal képes egy olyan egyszerű programot készíteni, vagy azt - interneten való jártassága miatt - különféle hacker oldalakról „beszerezni", amely, ha eljut egy célszámítógépre, azon automatikusan – a készítő beavatkozása nélkül – kicsomagolja és futtatja magát, majd a futtatás során elkövet valamilyen bűncselekményt, pl.: töröl bizonyos dokumentumokat, avagy lemásolja azokat, s továbbítja a készítőhöz. Az ilyenfajta bűncselekmények rendkívül gyorsan történnek, s a sértett akkor sem észleli, ha éppen a számítógépe előtt ül, s mivel a program minden nyomot megsemmisít, az elkövető biztonságban érezheti magát, hiszen ő

részt sem vett a bűncselekmény tényleges kivitelezésében. További veszélye az ilyen programoknak, hogy hálózatokon, Interneten keresztül, egyszerre juthatnak el rengeteg sértetthez.

Tovább vezetve ezt a gondolatot, egyre jellemzőbb, hogy **fiatal kiskorúak** követnek el számítógépes bűncselekményeket. Például egy előre elkészített programmal „életre hívnak" egy vírust, s azt útnak indítják az Interneten, ami akár jelentős károkat is okozhat. Meg kell azonban jegyeznünk, hogy a kiskorú fiatal elkövetők között inkább a file-cserélés és az illegális szoftvermásolás, terjesztés a jellemzőbb, ami bár enyhébb bűncselekmény, mint a vírusírás, de megfelelő odafigyelést kíván meg. A jelenség azért is aggasztó, mert koruknál fogva ezek a fiatalok nem látják, nem érzik át tettüknek súlyos következményeit.

IV. AZ ELKÖVETŐK INDÍTÉKAI

Az elkövetők motivációi rendkívül sokfélék lehetnek. Gyakori motiváció az **anyagi haszonszerzés,** amely a szoftverek jogosulatlan másolásának, forgalmazásának, a félvezetők tiltott másolásának, kereskedésének hátterében is áll, vagy **a védett személyes adatok, állami, szolgálati, banktitok jogellenes megismerésére irányuló szándék.**

Következő motivációként a **károkozás** emelhető ki. Az elkövetők betörnek rendszerekbe, és védett adatállományokat törölnek, módosítanak, vagy lemásolnak, s így azon túl, hogy komoly károkat okoznak, megsértik az egyes emberek magánszféráját.

Elsősorban munkahelyeken, fiatalok esetében az iskolában gyakori motiváció a **frusztráltság, elismerés hiánya**, vagy ami sokkal veszélyesebb **a bosszú**, de kiskorúak körében gyakran előfordul, hogy az **unatkozá**s, az **unalom váltja ki a** bűncselekmény elkövetését.

Bárkinél, de jellemzően a fiataloknál, további motiváló erőként jelentkezhet az **„Internet-mítosz"** nyújtotta hamis kép is, tehát amennyiben rendelkezik Internet hozzáféréssel, beléphet egy virtuális világba, egy olyan világba, ahol bármit megtehet (akár bűncselekményeket is elkövethet), amely világ teljesen más életformát kínál, mint a valódi, gyorsan a ranglétra legtetejére lehet emelkedni, s ott már szinte korlátlanok a lehetőségek.

"Az új világban mindenki a PC-je segítségével az Interneten keresztül fogja bonyolítani az ügyleteit, így aki nem akar lemaradni, aki modern, up-to-date ember kíván lenni, annak muszáj internetezni. Az igazán modern ember mindent az Interneten csinál ….Ha mindenki részesévé válik az Internet kínálta lehetőségeknek, és aktív felhasználója lesz a rendszernek, akkor bekövetkezik az "információs forradalom", és eljön a világbéke." [8]

A fiatalok számára komoly csábítást jelenthet egy ilyen lehetőség, s minél jobban megtanulják kezelni az Internetet, annál nagyobb lesz a csábítás. Véleményem szerint az Internet-mítosz erős hajtóerőként jelenhet meg azon fiataloknál, akik gyengébb iskolai teljesítményük miatt bizonyítási kényszert éreznek, vagy akik zárkózott, visszahúzódó magatartásuk miatt nehezebben kötnek barátságokat.

A bűnözés intellektuális jellegéből adódóan, a számítástechnika egyre népszerűbbé válásából eredően, sok, számítástechnikában jártas fiatal **szakmai kihívásként is** felfoghatja a bűnelkövetést, míg másokat a **hírnév-szerzés, mások elismerésének a megszerzése, az erőfitogtatás motiválhat**.[9]

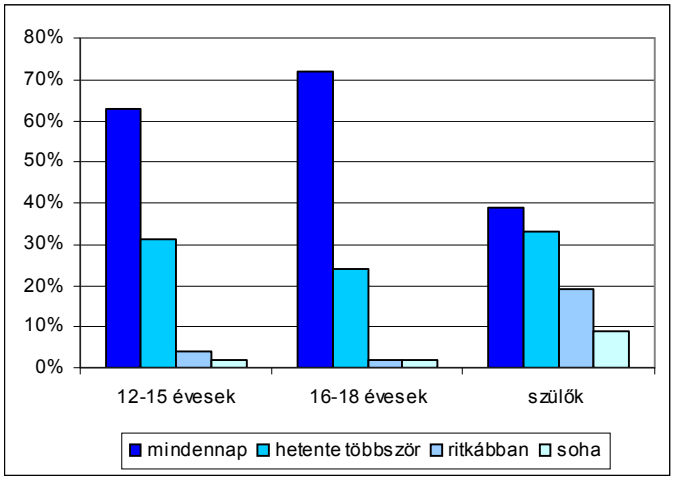
V. FIATALOK A CYBER-TÉRBEN

Az Internet nélkülözhetetlen eszköze a tudás megszerzésének, de a hálózat egyúttal rengeteg veszélyt is rejt. Az internet használata közben véletlenül is váratlan, szokatlan dolgokkal találkozhatunk.

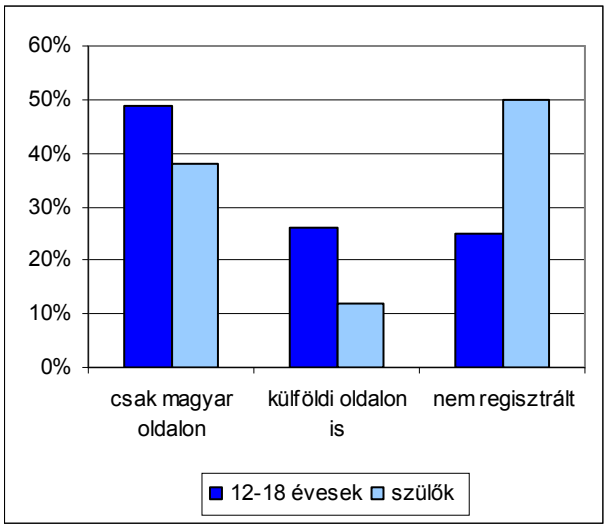
Kellemetlen tény, hogy bárkiből lehet elkövető és áldozat egyszerre. Az interneten barangoló személy gépe bármikor beleütközhet egy olyan szoftverbe, mely önmagát letölti a gépre és telepíti, vagy a rosszindulatú támadás áldozata lesz. Az ilyen gépeket a tulajdonos tudta nélkül képesek felhasználni bármire: fontos információt tölthetnek le a fertőzött gépről, képesek nem kívánt üzenetek (spam) ezreit szétküldeni onnan, de fel tudják használni akár más számítógép megfertőzésére is.

A tapasztalatok szerint a legsérülékenyebb és legveszélyeztetebb korcsoport a fiatal kamaszok, hiszen az internethasználat mára már életük részévé vált. Õk általában zenét töltenek le, azonnali üzenetküldõ (IM) programokat használnak, leveleznek, és on-line játékokat játszanak. Gyakran használnak keresõmotorokat is, hogy ráleljenek az általuk keresett információra. Többségük felkeresett már csevegõszobákat, és elképzelhetõ, hogy részt vettek felnõtt témájú csevegésben is. A tizenéves fiúk fegyelmezetlenebbek, róluk képzelhetõ el inkább, hogy véres vagy szexuális tartalmú honlapokra látogatnak, vagy szerencsejátékokba kezdenek. A lányok esetében inkább az a veszély fenyeget, hogy szexuális zaklatások érik õket.

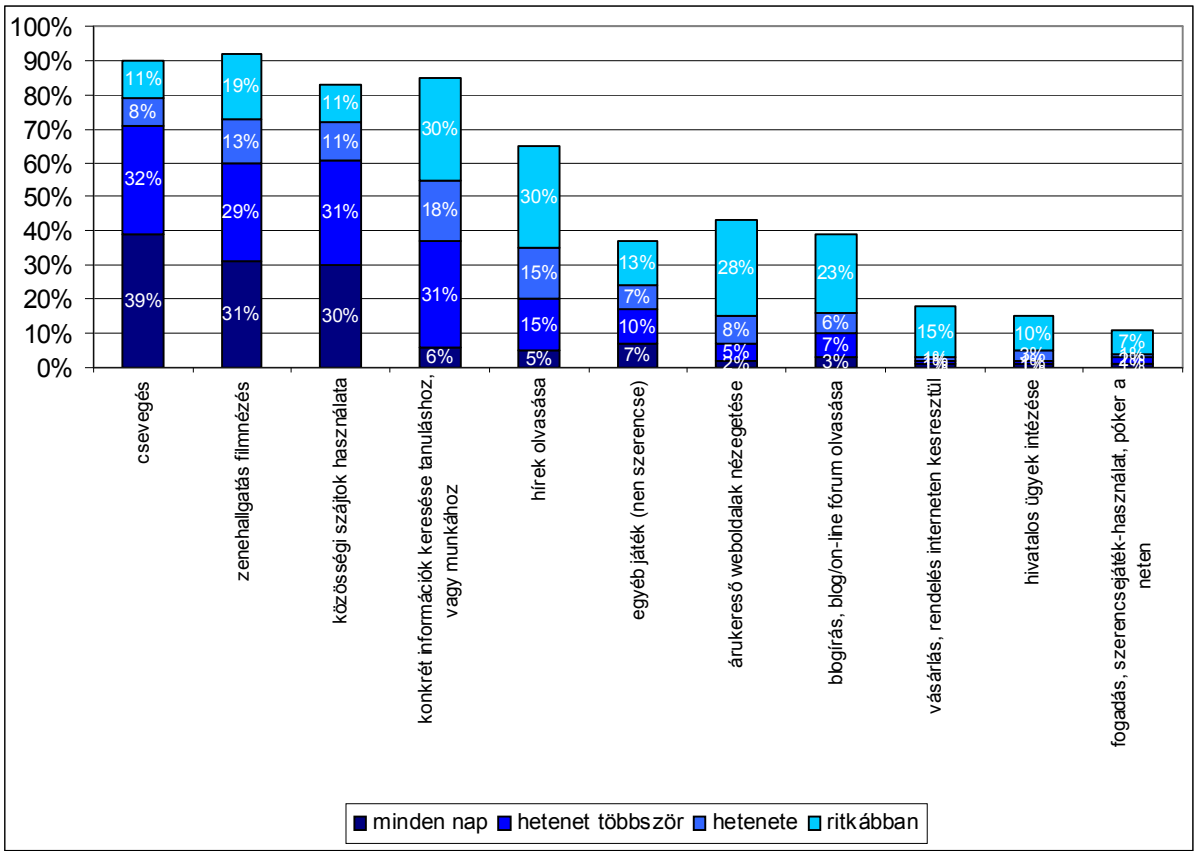
Egy 2009. évi felmérés szerint a 12-18 évesek 93 százalékának van Internet-hozzáférése, 86 százaléknak otthon is. A számítógép előtt hétköznaponként átlagosan 2 órát, hétvégeken közel 3 órát töltenek el



1. ábra. Otthoni Internet-használat, akiknek van otthoni internet hozzáférésük [Forrás: MEDIÁN, 2009]



2. ábra. Regisztrálás névvel, jelszóval [Forrás: Medián, 2009]



3. ábra. Mire használják a fiatalok az Internetet [Forrás: Medián, 2009]

A kamasz fiatalok - életkorukra való tekintettel -, az adaptív kockázatkeresés korszakában vannak, amit az evolúciós pszichológia „fiatal férfi szindrómának” nevez. Az „együttes élmény” hiánya a szülővel, vagy barátokkal, fokozza a magány, a depresszió, az unalom érzését, ami növeli az internet függőség kockázatát. Lehetnek olyan időszakok ebben a korban, amikor valamilyen érzelmi, hangulati vagy impulzus-kontroll probléma miatt erős függőséget mutat egy fiatal, vágyik felfedezni önmagát, elkívánkozik a szülői felügyelet alól, és a családon kívül keres új kapcsolatokat. A névtelenség látszata alatt szívesen vállal

kockázatot anélkül, hogy teljesen tisztában lenne a lehetséges következményekkel. Aggodalomra ad okot, hogy az interneten elérhető tengernyi információ - számtalan eset mutatja - csak súlyosbítja a fiatalok aggodalmait személyes problémáikkal kapcsolatban

Hosszasan lehetne sorolni az internet negatív hatásait, de emellett hangsúlyoznunk kell az áldásos oldalát is, azokat a lehetőségeket, amelyeket a fiatalok számára, a tudományos ismeretszerzéséhez nyújt. Elég arra gondolnunk, hogy az érdeklődő fiatal majdnem minden hírportálon találkozhat tudományos hírekkel, amelyekkel szélesítheti látókörét, bővítheti általános műveltségét. A használható nyelvtudással rendelkezők válogathatnak a világ vezető tudományos oldalainak kínálatából, de akár egészen speciális témákról is találhatnak hasznosítható anyagot.

Egyes fiatalok szakmai ambícióból, míg mások csak hobbiból, szeretnek elmélyedni egyes tudományágakban, így - a mai információ és kommunikáció alapú világunkban meghatározó szerepet betöltő - informatikában is. A világháló ehhez minden lehetőséget felkínál: az informatikának szinte minden ismerete megtalálható az interneten. Bármilyen szinten áll az érdeklődő, óriási támogatás és tudásanyag áll rendelkezésére a további fejlődéshez. Motivációval és kitartással komolyabb szintű szaktudás is szerezhető autodidakta módon.

Azon fiatalok, akik kutatói ambíciókkal rendelkeznek, vagy csak mélyebben szeretnének megismerni egy-egy speciális területet, szintén kihasználhatják a világháló nyújtotta lehetőségeket. A speciális szakmai oldalakon megismerhetik szakterületük új eredményeit, felfedezéseit.

Annak igazolására, hogy a mai fiatal nemzedék jó néhány csoportja kellő szakmai ismerettel rendelkezik, hogy - az internetről szerzett vagy saját ötletek alapján - anyagi haszonszerzés, de inkább, csak „egy jó hecc, egy jó balhé” kedvéért törvényellenes cselekményt kövessen el, nézzünk meg néhány esetet:

1. eset
2000. március 9-én jelent meg az a sajtó-hír, amely nyilvánosságra hozta, hogy a Rendőrség felderítette, elfogta és büntetőeljárás alá vonta azt a magyar hacker-társaságot, amely januárban kétszer is feltörte az Elender szervereit. A rendőrség kiemelt ügyként kezelte a bűncselekményt, mert a nyomozás során gyorsan felismerte, hogy nem egyszerű "piaci lopásról" van szó, hanem az internetre kapcsolódó számítógépes hálózatok ellen elkövetett olyan bűntényről, amely nemcsak a szolgáltatóknak okozhat károkat, hanem adott esetben a közszolgálati, a kormányzati, sőt a titkos adatbázisokat is veszélyeztetheti. A nyomozás során kiderült, hogy a fiataloknak nem volt az Elender Rt. alkalmazásában álló segítőjük. A számítógépes csalás bűntettével vádolt 15 és 19 éves fiatal hackerek vallomásukban azt állították, hogy **unaloműzésként** törték fel az Elender szerverét, és az ehhez szükséges speciális ismereteket autodidakta módon sajátították el. Arra nem gondoltak, hogy noha nem nyereségvágyból törtek be a szolgáltató szervereire, mégis több tízmilliós kárt okoztak a cégnek.[http://www.jogiforum.hu/publikaciok/75]

2. eset
Egy ismeretlen személy 2003. október 28-án az Országgyűlés Hivatala, a BRFK, valamint több kereskedelmi tévécsatorna e-mail címére fenyegető tartalmú levelet küldött, amelyben a Parlament és a Nemzeti Bank felrobbantásával fenyegetőzött. A Nemzetbiztonsági Hivatal

megállapította, hogy az e-maileket egy dunaújvárosi szakközépiskola számítógépéről küldték. Az iskola számítógépes nyilvántartási rendszerében végzett kutatás során beigazolódott, hogy az e-mailt egy ötödéves - stúdiókezelő feladatokat is ellátó - hallgató küldte, más felhasználói névvel belépve a rendszerbe. A Hivatal tájékoztatta az ORFK illetékes szervét, amely soron kívül végrehajtotta a diák meghallgatását. A fiatal a cselekmény elkövetését beismerte, tényleges végrehajtását nem tervezte, azt **"diákcsínynek"** szánta. [http://www.nbh.hu/oldpage/evk2003/terror.html]

3. eset

„Kétszáz óra közhasznú munkára ítélte egy brit bíróság azt a fiatalembert, aki még a tavalyi év során tört be egy amerikai részecskekutató intézetbe, és bénította meg annak működését napokra. Az ifjú hacker személyes zene- és filmgyűjteményének tárolására használta fel az intézet közel másfél tucat számítógépét, miután saját gépének merevlemezén már nem fértek el a nagyméretű médiaállományok.

A 18 éves James McElroy még 2002. májusában nyert illetéktelen hozzáférést az amerikai kormányzat által üzemeltetett Fermi Nemzeti Gyorsítóhoz, ahol a részecskekutatással és nukleáris kutatásokkal foglalkozó intézet 17 számítógépét kerített hatalmába. A több száz gigabájtnyi adatot illegálisan feltöltő fiatal többek között barátaival történő fájlcserélgetésre használta az áldozatul esett gépeket. McElroy a bíróság előtt azzal védekezett, hogy **fogalma sem volt** arról, hogy a megtámadott gépek kormányzati kutatólaboratóriumhoz tartoznak. A betörés által okozott zavarok következtében a részecskegyorsító működése három napig szünetelt, közel 21 ezer fontnyi kárt okozva az intézetnek." – olvashattuk a hírt az interneten is. [http://pcforum.hu/hírek/?qnid=2101&nfr=1&auth= f149 b6a885fa]

4. eset

Richter Csabát 3 év börtönre ítélték 2005-ben azért, mert feltörte az Ericsson informatikai rendszerét, és az onnan ellopott információkat **pénzért akarta eladni** a cégnek. A svéd titkosszolgálat tartóztatta le, mert fontos, bizalmas adatokhoz fért hozzá. Saját bevallása szerint hozzáfért telefon-szoftverek forráskódjához, radar förmverekhez, a Gripenek radarrendszerének rajzához, valamint adminisztrátori jogosultságot szerzett több rendszerben. [http://www.origo.hu/techbazis/internet/200504043ev.html]

5. eset

2004. áprilisában söpört végig Magyarországon, azután Európában is a Zafi névre keresztelt vírus, amely nevét erősen politikai töltetű tartalma miatt a hazafi szóból kapta, és amely hosszú hónapokig a legfertőzőbb kártevők közé tartozott. A vírus törzse szerint a pécsi SNAF Team készítette a kódot.[http://itcafe.hu/hir/zafi_a_virus_egy_igazi_hungarikum.html]

Összegezve elmondhatjuk, hogy a világ, így Magyarország informatikai rendszereit is folyamatosan támadások érik, érhetik, ezért a képzett fiatalok, a jó hackerek jó szolgálatot tennének az ország informatikai piacának és biztonságának is. Meg kell becsülnünk azokat a fiatalokat, akik rengeteg energiát fektetnek a rendszerek megismerésébe, és szaktudásukat a jó cél érdekében használják fel. Oktatási intézményeinkkel szemben fontos elvárás a jövőben, hogy a fiataloknak egyrészt magas szintű, az üzleti életben is hasznosítható informatikai ismereteket oktassanak, másrészt, hogy kiemelt hangsúlyt fordítsanak az **információbiztonsági ismeretek** oktatására.

Fontos elvárás továbbá a szülőkkel szemben, hogy ismerjék gyermekeik internetezési szokásait, hogy ismerjék azokat a játékokat, amivel a gyerekük játszik, hogy próbálják meg ésszerűen korlátozni gyermekük internet-használatát, hogy figyeljenek oda arra, gyermekük

mivel foglalkozik az interneten, és próbálják meg irányítani a „barangolásukat”. Véleményem szerint a fiatalok számára a legkézenfekvőbb és leghatékonyabb védelmet a jól funkcionáló családok biztosíthatják a cyber-térben.

ÖSSZEGZÉS

Az Internet elterjedése következtében a számítógépes bűnözés az egész világon elterjedt jelenséggé vált. Manapság kellő szakértelemmel és egy Internet hozzáféréssel rendelkező számítógép segítségével rendkívül gyorsan hatalmas károkat lehet okozni másoknak.

A jelenség jellemzőinek számbavételekor láthattuk, hogy a jelen kor, egyik veszélyes bűnözési formájával állunk szemben, veszélyességének egyik legfőbb forrása, hogy igazából bárki lehet elkövető, csak a szükséges technikai felszereltség (ami manapság már viszonylag olcsón beszerezhető) és némi szaktudás szükségeltetik, szemben mondjuk egyes hagyományos bűncselekményekhez, amelyekhez akár erős fizikum, drága felszerelések kellenek.

Ami a jövőt illeti, hangsúlyozni szükséges, hogy az információs társadalom térhódításával együtt a számítógépes bűnözés jelentősége s egyben veszélye is csak nőni fog. Az információs társadalom jövőképe a tudástársadalom: egy új minőségű, tudásközpontú, hálózati jellegű társadalom, ahol rendkívül fontos szerepe lesz az információnak, és a számítástechnikának. Egy információs társadalomban, ahol mindenki a mainál sokkal jobban függ a számítógépektől, számítógépes rendszerektől, s azok működőképességétől, illetve, ahol az információ s annak biztonságos megőrzése társadalmilag fontos tényező, igen komoly veszélyt jelent a számítógépes bűnözés.

A fiatalok közül a 12-18 éves korcsoport intenzíven használja a digitális technológia áldásait, és ezzel nagyobb kockázatot is vállalnak más korcsoportoknál. A biztonságos internetezés tudatosításának ezért elsősorban erre a korosztályra kell összpontosítania, különös tekintettel a közösségi oldalak használatában rejlő veszélyekre. Tudatosítani kell a fiatalokban az internet, az email, az üzenetváltó programok és a fizetős oldalak használatában rejlő veszélyeket.

Figyelemre méltó kezdeményezés a gyerekekre káros internetes tartalmak kiszűrését támogató **Biztonságos Böngészés Program (BBP),** amelyhez már több száz iskola csatlakozott, illetve több ezer munkaállomás tagja a programnak. Az iskolák számítógépeire olyan szoftvert telepítenek, amelyek képesek megvédeni a gyerekeket a káros vagy nem nekik való tartalmaktól és az internetes zaklatástól. A biztonságos böngészés program olyan szűrőszoftverek telepítését ajánlja, amelyek segítségével a pedagógus (otthon a szülő) maga állíthatja be és szabályozhatja, hogy a gyerekek milyen adattartalmat érhetnek el a világhálón, illetve, milyen, a számítógépre feltelepített programokat használhatnak.

Folyamatban van továbbá a **Magyarország Internetes Gyermekvédelmi Stratégia** kidolgozása, többek között az Országos Kriminológiai Intézet, a Symantec és a Biztonságos Böngészés Program az ORFK és a BRFK bűnmegelőzési szakembereinek együttműködésében, ami további bizakodásra adhat okot.

A védekezési lehetőségek közül fontos megemlíteni egyrészt a nemzeti és a nemzetközi együttműködést, a tapasztalatok átadását, a számítógépes és szoftveripar szoros kapcsolatát, illetve el az erőszakszervek és az igazságszolgáltatás bűnözőkkel szembeni határozott fellépését, másrészt a családok szerepét, a szülők felelősségét, hiszen a mikrokörnyezet, a család támogatása nélkül egyetlen program, egyetlen kezdeményezés sem lehet sikeres.

Felhasznált irodalom

[1] Kovács László: Az információs terrorizmus eszköztára http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html (letöltés: 2010. április 07.)

[2] Mezey Nándor: A számítógépes bűnözés http://www.jogiforum.hu/publikaciok/307 (letöltés: 2010. április12)

[3] Csepeli György: Veszélyesen élni? http://74.125.77.132/search?q=cache:LKlua6Imj8IJ:de.njszt.hu/files/kockazatkonf/01_Csepeli_Gyorgy_Veszelyesen_elni.ppt+sz%C3%A1m%C3%ADt%C3%B3g%C3%A9ps+szabot%C3%A1zs&cd=2&hl=hu&ct=clnk&gl=hu/www.zmne.hu/kulso/mhtt/hadtudomany/2008_e_2.pdf (letöltés: 2010. április 10.)

[4] Kovács László - Krasznay Csaba: Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság, III. évfolyam. 1. szám. 2010. február ISSN 1789-5286 p.: 44-56.

[5] Dr. Balogh Zsolt György: Jogi informatika, Dialog Campus Kiadó, Budapest-Pécs, 1998, 264-265. o.

[6] Dr. Sárkány Tamás: Támadási lehetőségek távközlési hálózatok ellen, Híradástechnika, LVIII. évfolyam, 2003/5. szám

[7] Steven Mizrach: Létezik-e „hackeretika" a 90 –es években, Replika 2000. 41-42; 303-305. oldal

[8] Tarr Dániel: Internet mítosz http://mek.niif.hu/01400/01437/html/kod03_2.htm#5 (letöltés: 2010. április 12.)

[9] Flammich Mariann: Hackerek http://krono.inaplo.hu/index.php/inter/recenzio/282-hackerek- (letöltés: 2010. április 05.)

HADMÉRNÖK
V. Évfolyam 2. szám - 2010. június

Szegediné Lengyel Piroska
l.piroska@t-online.hu

HATÉKONY VIRTUÁLIS OKTATÁS A PEDAGÓGIA ÉS A DIDAKTIKA SZEMSZÖGÉBŐL

Absztrakt

A cikk a minőségi virtuális oktatás feltételrendszerét, meghatározó elemeit – a hallgatók meglévő ismeretei, tapasztalatai, általános műveltsége; a tanulási-tanítási környezet; a tanítás-tanulás folyamata, módszertana; a pedagógus; a tananyag, az eredmények – vizsgálja, ismertetve, ütköztetve a téma jeles kutatóinak meglátásait, álláspontjait, illetve kiegészítve azt a szerző saját, személyes oktatói tapasztalataival, a témában elért kutatási eredményeivel, hipotéziseivel. A cikkben bemutatásra kerül a szerző elektronikus könyveinek néhány, a témához szorosan kapcsolódó részlete is.

The present article is focusing on the conditions and critical elements of high quality virtual teaching – the formerly acquired knowledge, experiences, the overall intelligence of the students; the teaching-learning circumstances; the teaching-learning methods and process; the teacher/lecturer; the learning material; the learning results – in a way of introducing and discussing the views and standpoints of some well known experts, when supplementing them with the writer's own teaching experiences, research hypotheses and results in the field. The writer also presents some details of those electronic learning materials which are closely connected to the discussed topic and have been developed by her.

Kulcsszavak: *e-tanulás, e-tanár, kognitív tudás, élménypedagógia, kompetenciamotiváció, módszertan ~ e-learning, e-teacher, cognitive knowledge, enjoying pedagogy, competence-motivation, methodology*

BEVEZETÉS

A virtuális oktatás megköveteli a hagyományos tanítási-tanulási környezet átalakítását, a korszerű információs és kommunikációs eszközök ismeretét, használatát. A fejlett világ jövője szempontjából elsőrangú feladattá lépett elő az „egész életen át tartó tanulás" társadalmasítása, ezáltal a norma, a kultúra részévé válása. Ebben a megvilágításban különös szerephez jut a korszerű e-learning és távoktatás, amelynek jellemzői a tanulásmenedzselés, a nyitott tanulás és a művelődés virtuális környezete.

Egy adott felsőoktatási intézménynek olyan kínálattal, **egyedi képzési profillal** kell rendelkeznie, amellyel versenyben maradhat a társintézményekkel szemben**. Piacképes tudást** kell

adnia a hallgatók megtartása érdekében, illetve ki kell alakítania olyan továbbképzési rendszert, amelynek keretében a legkorszerűbb ismereteket képes átadni a résztvevőknek (a jelen és a jövő vezető szakembereinek), fel kell készítenie a hallgatókat a versenyhelyzetekben való sikeres megfelelésre. **Az intézmények minőségét elsősorban ezek a mutatók jelzik**, amely mutatók a **kognitív tudás dominanciáját** erősítik.

A téma feldolgozása kapcsán induljunk ki abból az alapgondolatból, hogy a minőségi virtuális oktatásnak hat kulcsdimenziója van:

1. A hallgatók (tanulók) meglévő ismeretei, tapasztalatai, általános műveltsége
2. A tanulási-tanítási környezet
3. A tanítás-tanulás folyamata, módszertana
4. A pedagógus
5. A tananyag
6. Az eredmények

Az alapgondolat alátámasztására, megerősítésére, esetleg megcáfolására vegyük sorra az irodalomjegyzékben ismertetett tanulmányokat. Vessük össze a szerzők különböző nézeteit, álláspontjait. Az így kialakított képet a magam részéről annyiban kívánom árnyalni, hogy kiegészítésként – a személyes oktatói tapasztalataimat**,** a témában eddig elért kutatási eredményeimet is felhasználva – bemutatom a saját hipotéziseimet, illetve következtetéseimet is.

1. A HALLGATÓK MÁR KORÁBBAN MEGSZERZETT MEGLÉVŐ ISMERETEI, TAPASZTALATAI, ÁLTALÁNOS MŰVELTSÉGE

A hallgatók meglévő tapasztalatai, ismeretei, illetve **általános műveltségük,** amit magukkal hoznak a virtuális intézménybe, olyan szintű kell legyen, hogy képessé tegye őket arra, hogy aktív résztvevői legyenek az e-learning, illetve távoktatási kurzusoknak.

Polónyi István Válasz az e-learning, de mi volt a kérdés? című tanulmányában az e-learning, az internet alapú távoktatás, illetve távtanulás térhódítását vizsgálva, arra a megállapításra jut, hogy bár az internet gyorsan beépül az oktatásba, javítja a közlés minőségét, de lényegében nem változtatja meg az oktatás színvonalát, mivel általános elterjedésének gátat szab a képzéshez szükséges megfelelő tanulói előképzettség hiánya. „Persze, van egy-két oktatási szegmens, ahol az e-tanulás is szerephez jut, a felnőttképzés egyes területein, elsősorban a **magasan képzettek,** az önálló tanuláshoz kellő alappal és gyakorlattal rendelkezők továbbképzésében.”[1]

Az előképzettség alapvető fontosságát hangsúlyozza Vörös Miklós is, amikor a személyre szabott tananyag kifejlesztését preferálja: „1997-ben az USA Védelmi Minisztériuma és a Fehér Ház Tudományos és Technológiai Eljárások Hivatala elindították az Advanced Disrtributed Learning (ADL) kezdeményezést. Cél, a legkorszerűbb technológiai eszközök, és fejlesztési eljárások, szabványok felhasználásával, egy olyan web-alapú tanulási környezet kialakítása, melyben a tananyag egy világméretű elosztott tudásbázisból, a tanuló **személyére szabottan** kerül kialakításra”[2]. Ezt a gondolatot fejleszti tovább, amikor a sikeres e-tanulás előfeltételeként a tanulók előismereteinek feltérképezését jelöli meg: „…. Az élethelyzethez igazított tanulás ezért előírások meghatározott sorozata, mind a képzés tervezéséhez, szervezéséhez, mind annak végrehajtásához; rendszerezett módon áttekinti a tananyagkészítés és a tanulási folyamat egyes mozzanatait, a megszerzett tudás mérési kritériumait és módjait. Ismerni kell a tanulók

előismereteit, előzetes felkészültségét, sőt azt, hogy mi történjen, ha ezek nem tesznek eleget az előzetes feltételeknek" [3]

Gerő Péter Az élethelyzethez igazított tanulás című könyvében is hangsúlyozottan szerepel a tanulói kompetencia és a tanulási cél pontos meghatározása, mint az eredményes ismeretszerzés előfeltétele.

„Az alapgondolat: ha létezik a (mérhetően, tehát egzaktul megfogalmazható) tanulási cél, akkor nem kevésbé egzakt módon megállapítható, hogy az adott tanulónak (a jelenlegi előismeretei, meglévő kompetenciái kiegészítéséül) milyen kompetencia-bővülésre van szüksége a tanulási cél eléréséhez. Ennek alapján **létrehozható, illetve kiválasztható** (az adott tanuló személyes céljai, helyzete, lehetőségei függvényében) az ismert eszközök, források nagy tömegéből **az a variáció,** amely az adott tanuló esetében a legeredményesebb. A tanuló pedig – ennek megfelelő pedagógiai/andragógiai segítség mellett – végighaladhat a megtervezett tanulási folyamat valamelyik útvonalán."[10]

A képzettebb tanulók érettebbek az önálló tanulásra: rövidebb idő alatt átveszik a tanulás ritmusát, az új ismereteket befogadó képességük fejlettebb, lényeglátóbb.

Nincs abban semmi meglepő, hogy a szakmailag képzettebb, felkészültebb tanulók sokkal többet nyernek a virtuális oktatástól, mint kevésbé képzett társaik; a tananyagok összeállításakor, a módszertan kidolgozásakor azonban erre oda kell figyelni: „A tanulási folyamat sikerességének meghatározó tényezője a **tanulói különbségeket** figyelembe vevő oktatási módszerek alkalmazása…A hallgatókat hatékonyabban lehet felkészíteni az élethosszig tartó tanulásra, ha többet megtudnak saját tanulásukkal kapcsolatos **erősségeikről és gyengeségeikről**. Ha az oktatók figyelembe vennék az egyének erősségét és gyengeségeit, akkor valószínű, hogy javuló tendencia mutatkozna a formális tanulási programokban; és a tanulás tanulásának képessége megalapozná az élethosszig tartó tanulást." [4]

Az említett szerzők a tanulók előképzettségének és egyéni képességeinek meghatározó szerepét hangsúlyozzák. Az e-learning tanulás és tanuló központúságából adódóan az e-tanárnak törekednie kell olyan **tanítási-tanulási módszerek** kialakítására, amelyek iránymutatást adnak a tanulónak a **tanulás megtanulásához,** amelyek megoldást jelentenek a heterogén összetételű közösségekben az egyenlőtlen státuszból adódó problémák kezelésére.

A tapasztalatok azt mutatják, hogy a **tanulók interaktív közreműködésére** alapozott tanulási-tanítási módszerek szolgálják leghatékonyabban a virtuális oktatást.

Kiscsoporton belüli interakciók vizsgálata során azt tapasztaltam, hogy a csoporton belül a magas státuszt elfoglaló tanulók a tanítási órákon aktívabbak, többször nyilvánítanak véleményt, többet szólnak hozzá a tananyaghoz és ennek következtében szakmailag jobban fejlődnek, mint alacsony státuszú társaik.

Az új oktatási forma, tehát alapkövetelményként támasztja a pedagógusokkal szemben, hogy megoldást találjanak a heterogén összetételű csoportokban az egyenlőtlen státuszból adódó problémák kezelésére. A tananyagot az egyéni képességekre építve kell kifejleszteni: olyan **tanulási technikát**, módszert kell az ismeretek elsajátításához a tanulónak ajánlani, amely segíti a megtanulandó tananyag könnyű, gyors elsajátítását és reprodukcióját, segít a társakhoz való felzárkózásban.

Vizsgálataimhoz az általam kifejlesztett „számviteli ismeretek e-könyvek" [http://www.lengyelpiroska.hu/elkonyv.html] alkalmazása szolgált. Az e-könyvek összeállítása során kerestem azokat a módszereket, amelyek alkalmazása mellett az alacsonyabb státuszú tanulók felzárkózása megoldható, amelyek mellett részvételük aktívabb lesz a tanulási folyamatban és javul a tanulmányi teljesítményük.

A tananyagba, minden átfogó, nagyobb fejezet lezárásaként, egy projekt-feladatot építettem be. Felajánlom a hallgatóknak, hogy a gyakorlati természetű feladatot on-line foglalkozások keretében közösen oldják meg. A projekt munka a tanulók érdeklődésére, a diákok közös tevékenységére építő kooperatív munka.

A projekt-munkában minden egyes tanulótól a tanár is és a társak is azt várják el, hogy aktív résztvevő legyen. Elvárják, hogy érezzen felelősséget saját maga és a csoportja teljesítményéért. Ugyanakkor minden egyes tanuló kompetens, egyenrangú szereplője a tanulási folyamatnak. A munka során tudatosul a tanulókban, hogy mindenki rendelkezik fontos **intellektuális képességgel,** gyakran egyediekkel is, amellyel hozzájárulhat, hogy csoportja eredményesen oldja meg a feladatot.

A kiscsoportos munkában való részvétel nagyfokú tanulói önállóságot igényel, az ismereteket integrálja, a tanulók egymás munkájáért is felelősek, így közöttük kölcsönös függőségi viszonyok jönnek létre. A legfontosabb mozzanat az, hogy a feladat sikeres megoldásához a tanulók sokféle képességét kell mozgósítani, s ennek révén, azon túl, hogy minden tanuló hozzájárul a csoport feladatának sikeres megoldásához függetlenül attól, hogy milyen egyedi intellektuális képességekkel rendelkezik, a tanárnak is lehetősége nyílik – megfigyelő szerepkörből – az egyéni képességeket „tanulmányozni", feltérképezni. A tanár feladata, hogy a háttérből figyelje a tanulók tanulási stratégiáját, kövesse végig a teljes tanulási folyamatot, szükség esetén segítse az alacsonyabb státuszú tanulók aktív bekapcsolódását a csoportmunkába.

Célszerű tehát a csoportmunkán alapuló feladatot az első tananyagrész után beépíteni az elektronikus tananyagokba, hogy megfelelő időben visszajelzést kapjunk a kurzust felvevő hallgatók előképzettségéről, egyéni tanulási stílusokról, hogy annak függvényében a további tananyagrészek hatékony elsajátításához a megfelelő módszertani segítséget meg tudjuk adni. „Egy ideális oktatási környezetben az oktató azonosítja a **hallgatói egyéni különbségeket**, a különböző tanulási típusokat, valamint a hallgatók előismeretét, és ezek alapján állítja össze az oktatási tartalmat." [4]

2. A TANULÁSI KÖRNYEZET

A hagyományos oktatási környezethez hasonlóan, a virtuális tanulási-tanítási környezet is sokat foglalkoztatja a kutatókat: nap, mint nap felvetődik a kérdés, hogy milyen adottságokkal kell rendelkeznie az oktatás színterének, milyen környezetben végezhető minőségi tanítás és tanulás.

Vajon igaz-e az az álláspont, amely szerint, semmilyen képzést sem lehet a távolból adni? Vajon nem konzervatív azt állítani, hogy a hagyományos osztálytermet nem pótolhatja a virtuális osztályterem? „Minden pedagógusi tapasztalatunk azt mondatja velünk, hogy a campus közös emberi terében zajló tanítás és tanulás a kezdeti egyetemi évek tapasztalatának lényegéhez tartozik és nem áldozható fel nagyobb mértékben, hacsak az oktatást-nevelést nem akarjuk elfogadhatatlan színvonalra süllyeszteni." [1]

A kérdést egyértelműen nehéz megválaszolni, inkább úgy kell fogalmaznunk, hogy a tanulási – tanítási környezet kritikus területe a virtuális oktatásnak. Amíg a hagyományos oktatási formában az osztályterem az a hely, ahol a diákok szabadon tanulhatnak, ahol rendelkezésükre állnak a tanuláshoz szükséges források, ahol izgalmas tanulási kalandokat élhetnek át, ahol a lehető legtöbb időt tudják tanulással tölteni, ahol személyes kapcsolatok, barátságok születnek, addig az e-learningben a taneszközöknek, a tananyagoknak, a virtuális osztálytermeknek kell betölteniük ezeket a funkciókat.

A virtuális környezetnek kell olyan motiváló erővel rendelkeznie, amely felkelti a tanuló érdeklődését, tanulásra, gondolkodásra, alkotómunkára serkenti. Ezt az ún. **kompetenciamotivációt** találóan jellemzi Korom Erik, amikor a tanulási motiváció szintjeit vizsgálva, hangsúlyozza a belső motivációt: a tanuló nem kötelességtudásból tesz eleget iskolai kötelezettségeinek, hanem a tantárgy iránti kíváncsiságból, érdeklődésből, tudásvágyból. „A kompetenciamotiváció, amikor a környezettel való interakció sikeres, az egyén örömöt él át, pozitív érzése lesz magáról. Ez az elégedettségérzés adja a további motivációt a tanulásra, így a tanulás és a teljesítmény belső megelégedettséggel jár, és jutalmazó önmagában.” [5]

Következésképpen a virtuális környezetnek olyan életközegnek kell lennie, ahol a résztvevők megtanulnak tanulni, játszani, dolgozni, önmagukat ellátni, közösségben élni. A virtuális élettérben folyamatosan fejlődnie kell a résztvevők tanulási készségének, kreativitásának, problémamegoldó készségének, emberi kapcsolatainak: „az információs és kommunikációs technológia rendkívül gyors fejlődésének hatására kialakult és rohamosan fejlődik a virtuális tanulási környezet: fokozatosan általánossá válik a számítógépek által létrehozott interaktív audiovizuális tanulási közeg, amely nemcsak szövegeket, de képeket, hangokat és animációkat is közvetít – ez az ember természetes életvilágához hasonló. Az információ tárolásának és elérésének univerzális eszközévé a számítógépes világháló válik, mely ezért a képzés, és a továbbképzés természetes közege lehet” [2]

3. A TANULÁS FOLYAMATA, MÓDSZERTANA

A virtuális környezettel szemben támasztott követelményeket – minden bizonnyal – az **élménypedagógián** alapuló **tanítási módszerek** mentén érdemes megfogalmazni. Az élménypedagógia az egyéni élményt teszi a pedagógiai tevékenység középpontjába. H. Scharrelmann szerint az élmény a tanítás koronája. „Egy „kiemelkedő történés hatására keletkező erős érzelmektől kísért lelki jelenség… mély színezete miatt fokozott pedagógiai hatást fejt ki, s ezért megfelelő formában fokozhatja a nevelés hatékonyságát.” [8]

Hasonló a gondolatokat fogalmaz meg Gabnai Katalin drámapedagógus, amikor az élményszerű ismeretszerzés egyik fontos eszközének nevezi a drámapedagógiát, hangsúlyozva, hogy **„az a virtuális oktatás speciális tananyagának „színrevitelét” szolgálja”** [9]

Kétségtelen, hogy a tananyag „eljátszása”, a mondanivaló modellezése, a tanulók vizuális memóriáját fejleszti, a tananyag elsajátításának hatékonyságát sokszorosára növeli. Kémia tanárok gyakran alkalmazzák azt a módszert, hogy az egyes kémiai reakciótípusokat a tanulókkal játszatják el, aminek következtében még a leggyengébb képességű tanuló is pontosan el tudja mondani – akár sok évvel később is – a reakciók lényegét. A vizuális élmény hatására a tananyag bevésése, a gondolati emlékezetbe vésés olyan erős, hogy az előhívás, az ismereteknek a memóriából történő visszakeresése nem jelent gondot a tanulóknak.

A virtuális tananyagfejlesztés során kiváló terep kínálkozik mindehhez, függetlenül attól, hogy kémiai, vagy más tudományágakat tárgyalunk.

Számos elektronikus tananyagot fejlesztettem a közelmúltban (számviteli alapismeretek, könyvviteli alapismeretek, támogatások számvitele, adózási ismeretek), ahol a tartalmi és módszertani felépítés során az élményszerű ismeretszerzésre helyeztem a hangsúlyt: a mondanivaló modellezésével, képi megjelenítésével, a szerepjátékokkal, a játékos feladatokkal egy olyan **tanulási technika** elsajátítását ajánlom a tanulóknak, amelynek középpontjában az **összefüggések megértésen alapuló bevésése**, valamint az **emlékezet fejlesztése** áll. Az ötletek, elképzelések megvalósításához a korszerű IKT eszköztára korlátlan teret nyit, de az egészen egyszerű informatikai eszközökkel, programokkal is látványos megoldásokat lehet elérni.[http://www.lengyelpiroska.hu/szamvitele/konyv/Eloadas.html].

A tananyag elsajátításának **módszertana**, a **tanulási–tanítási folyamat** a virtuális oktatás sikerének kulcsterülete. Cél, hogy a tanulók gyorsan, tartósan és eredményesen sajátítsák el a tananyagot, hogy a tanulásra szánt idejük és erőfeszítésük megtérüljön. Annak érdekében, hogy naponta ne töltsenek a szükségest esetleg sokkal meghaladó időt „klasszikus" tanulással, hogy a tanulás eredménye ne maradjon el az elvárásaiktól, hogy éles helyzetekben (vizsga, csoportmunka) is hatékonyan tudják visszaadni az ismereteket, korszerű **tanulási ütemtervet/tantervet** (mikor? mit?) kell kialakítani, amelyhez hatékony tanulást irányító, tanulást segítő **módszereket** (hogyan?) kell kifejleszteni.

Átgondolt, szakmailag és didaktikailag jól felépített ütemterv nélkül nem lehet hatékony az oktatás. Ahogyan egy vállalkozás sikere elképzelhetetlen üzleti terv nélkül, ugyanúgy a sikeres oktatásnak is a célirányosan kidolgozott tanterv az alapja.

A tanterv egyrészt **tükör**, amely megmutatja mindazt, ami a virtuális közösségben történik, másrészt, pedig **ablak,** amelyen keresztül betekinthetünk a virtuális osztályteremben folyó munkába, hogy lássuk azt, aminek a tanterv szerint történnie kell. A tantervnek biztosítania kell, hogy a tanulók megtanuljanak tanulni.

Polónyi István szerint az iskolának nem az a fő feladata, hogy információkkal lássa el a tanulókat. Nem szabad abba a hibába esni, hogy azt gondoljuk az oktatás nem más, mint információközlés: „A tanulás leginkább az élő szervezet működéséhez hasonlít, mint, ahogy az élő szervezetnél is az inputok a szervezet működéséhez szolgáltatnak energiát, s az égéstermékek eltávoznak, a tanulásnál is az inputok nagy része elfelejtődik, s a szerkezetük, összefüggéseik azok, amik megmaradnak. Az oktatás során a pedagógus szerepe éppen ezeknek az összefüggéseknek a szemléltetése, megértetése, és persze a motiváció fenntartása. Nem az információk tömegére van tehát szükség, hanem olyan információkra, amelyek az információ feldolgozását támogatják, s amelyek az elsajátítani kívánt összefüggések megértését segítik elő. [1]

Vajon igaza van-e Buda Andrásnak, amikor azt állítja, hogy a tanulás és tanuló központú virtuális oktatásban „Az irányító szerep a diáké, ő határozza meg a tanulás idejét, ütemét, helyszínét, hogy csak a legfontosabbakat említsük"? [7] Vagy Polónyi Istvánnak, aki a teljes tanulói önállóságot az oktatás magasabb szintjéhez köti: „Az persze teljesen egyértelmű, ahogyan felfelé haladunk az oktatási rendszer szintjein, annál nagyobb szerepet kaphat az önálló információgyűjtés, -feldolgozás, -elemzés, tehát az önálló tanulás"? [1] Vagy Korom Eriknek, aki a tanulói önállóságnak már nem egyértelműen pozitív megítélését veti fel: „A tanulóközpontú oktatási formákban a tanulás testre szabott, a diák rugalmas, saját időbeosztásához igazítható képzést kap, meghatározza a tanulás ütemét és helyét, emiatt viszont a sikerhez nagyfokú motiváltságra, fegyelemre és önállóságra van szükség. Vannak, akik ezt kiváló lehetőségnek, tartják, mások viszont hátrányként élik meg"? [5]

Véleményem szerint a virtuális oktatás fejlődése akkor fog új lendületet kapni, ha belátjuk azt, hogy ebben az új oktatási formában is a **tanáré az irányító szerep**: ő határozza meg, (vagy legalábbis javasolja) a tanulás ütemét, ebből adódóan számos esetben az idejét is (projektmunka) és egyes esetekben (megbeszélések, viták on-line előadások keretében) a helyszínt is.

4. A PEDAGÓGUS

A virtuális oktatás a hagyományos oktatáshoz képest új módszerek kialakítását teszi szükségessé, ami új igényeket, új követelményeket támaszt a pedagógusokkal szemben, Az új feladatok, az új követelmények pedig **„újfajta pedagógust",** újfajta pedagógiai gondolkodást és gyakorlatot követelnek meg.

Tanórai keretek között a tanítás hagyományos funkciója az ismeretek átadása, a tudás bázisán alapuló szellemi képességek kifejlesztése. Ezzel szemben a tanulóközpontú szemléletű virtuális oktatás a **személyiségfejlesztés**t helyezi a középpontba, és annak rendeli alá az ismeretszerzést.

A hagyományos oktatásban a tanárt az foglalkoztatja, hogy az adott életkorban, az adott kompetenciaszinten milyen tananyag lenne legmegfelelőbb a tanulók számára, hogyan keltheti fel az érdeklődésüket úgy, hogy megtanulják az összes megtanulandó anyagot, milyen módszerrel vizsgáztasson, hogy pontosan le tudja mérni, hogy tanulói mennyit sajátítottak el a tananyagból.

Ezzel szemben az e-tanárt elsődlegesen az foglalkoztatja, hogy a tanulókat mi érdekli leginkább, milyen problémákat szeretnének megoldani, milyen a g**ondolkodásmódjuk.** Az e-tanár arra törekszik, hogy megteremtse azt a **lélektani klímát,** amelyben a tanulók szabadnak érzik magukat, felfedezhetnek, tanulhatnak a környezetüktől, a tanártól, a társaiktól, egyéni élményeket szerezhetnek. Az e-tanár arra törekszik, hogy olyan tanulási környezetet teremtsen, amelyben a tanuló átérzi a tanulás izgalmát, ami lángra lobbanthatja, és ha megvan a „láng", akkor keresi a módját, a módszert, hogy hogyan segíthet a tanulóknak megtalálni a forrásokat (az embereket, könyveket, az élményeket), ami segít megtanulni az anyagot úgy, hogy ezzel megtudja, amit meg szeretett volna tudni.

„…vannak-e egyáltalán olyan pedagógusok, akik megfelelnek az új kihívásoknak, hiszen a felsőoktatási intézményekben még csak elvétve találkozhatunk ilyen irányú felkészítéssel?" teszi fel a kérdést Buda András, amire logikus választ ad: „azt tapasztaljuk, hogy az egyre szaporodó e-learrninges kurzusok megtalálják vagy „kitermelik" a feladat ellátására alkalmas (vagy annak tartott) személyeket". [7] Mindez talán annyival egészítendő ki, hogy a hagyományos oktatásban a „sokat tapasztalt" pedagógusok a legalkalmasabbak erre a feladatra.

A virtuális oktatásban közreműködő pedagógusokat jellemzően három csoportba sorolja a szakirodalom: **tananyagfejlesztők**, az ismeretek elsajátítását, a tanulási folyamatot segítő tanárok (**tutorok/mentorok**), és az **értékelők**, a vizsgáztatók. Megoszlanak a vélemények a pedagógusi szerepkörök tartalmát illetően, abban, hogy kinek mi a feladata.

„Ahhoz, hogy egyáltalán képzésről beszélhessünk, rendelkezésünkre kell állnia a tananyagnak, melyet a tananyagfejlesztők állítanak össze, Munkájukat a technikai feltételek alapvetően befolyásolják, és annak ellenére, hogy nincs kapcsolatuk a tanulókkal, az általuk fejlesztett tananyag meghatározhatja az egész folyamat sikerességét, illetve a többi tanári csoport tennivalóit"[7]

Az ismeretek elsajátítását, azaz a tanulási folyamatot a tutorok, mentorok segítik, akiknek a szerepe eltér a hagyományos oktatás során megszokott tevékenységtől: „Csak annyi a dolguk, hogy a tanulók kérdéseit megválaszolják, segítsék problémáik megoldását, hogy a tanulási folyamat gördülékenységét, eredményességét biztosítsák…

…Nyilvánvaló, hogy a képzés végén szükséges az elsajátított ismeretek átfogó számonkérése, annak megítélése, hogy milyen szinten teljesítette a tanuló a vele szemben támasztott követelményeket. Ilyenkor – a direkt ellenőrzés hiánya miatt – legtöbbször csak időpont és/vagy helyszín megkötésekkel lehet számot adni a tudásról, általában a tanuló és az értékelő ekkor találkozik először személyesen." [7]

Pálinkás Jenő, az ILIAS LCMS programcsomagot bemutató tanulmányában külön ábrával érzékelteti a tanári szerepkörök éles elhatárolását. A tananyagfejlesztő átadja a tananyagot a kurzus számára, és ezzel a szerepe befejeződött. Az internetes tutor irányítja a fórumot, tartja a kapcsolatot a hallgatókkal, számukra dokumentumokat állít össze: „Az ILIAS támogatja az internetes tutorálást, belső e-mail és chat rendszerével, fórumaival segíti a hallgatói és tanári szinkron és aszinkron kommunikációt….A hallgató által megoldandó feladatot a tutor tíznaponként adja fel és a beküldendő megoldást a hallgatók a fájl-ba csatolják (küldik meg) a tutornak….A fórum, chat

rendszer a hallgatóval való kapcsolattartásra szolgál, itt történik a bejövő levelek, hozzászólások, kérdések tanszéki elvárások, határidők kezelése." [6]

De vajon el lehet-e, el szabad-e határolni ilyen formában a tanári szerepköröket? A válasz alábbi megfogalmazásában kétségtelenül benne rejlik bizonyos szubjektivitás, ugyanakkor logikai és tapasztalati úton is igazolható annak megfontolásra érdemes volta.

Ha egy fiatal tanár kollégám megkérdezne, hogy pedagógusként mi a véleményem az elektronikus oktatásról, és egyúttal tanácsot kérne tőlem, hogy vállaljon-e e-tanítást egy korszerű, igényes felsőoktatási intézményben, ahol éppen a távoktatási rendszer kiépítése, bővítése a cél, azt válaszolnám, hogy igen. Ha úgy konkretizálná a kérdését, hogy tananyagfejlesztésre, a tutor, vagy vizsgáztató tanári feladatkörre specializálódjon-e, valószínűleg azt ajánlanám neki, hogy választhatja bármelyiket, de előbb-utóbb szerezzen gyakorlatot mindhárom területen. Hosszú évek tapasztalata alapján ugyanis úgy látom, hogy a munkám lényegegétől, a tudás-átadástól, a neveléstől, a szervezéstől, a pedagógusi munka izgalmától fosztanám meg magam, ha egyik vagy másik tanári szerepkörbe „kényszerítene" az új oktatási forma.

Ha ennél valamelyest objektívebb megfogalmazásban közelítem a kérdést, abban az esetben is úgy gondolom, hogy a tanulási folyamat minden egyes szakaszában jelen kell lennie bizonyos szinten a pedagógusnak. Ha a tanár kifejleszt egy tananyagot, előnyös az, ha követi az útját a teljes tanulási folyamatban, hogy lássa az erősségeit, a gyengeségeit, a használhatóságát, a használhatatlanságát, hogy mérje az eredményességét, mert így derül ki egyértelműen, hogyan kell változtatni, javítani annak tartalmát, hozzárendelni a legmegfelelőbb tanulási módszereket, stb.

Egyetértek a szerzőkkel abban, hogy az ismeretszerzés során elengedhetetlen a **tanár-diák kommunikáció,** hogy ezt a sajátos kapcsolattartást a távoktatás céljára választott programcsomagnak maradéktalanul biztosítania kell, ugyanakkor kiegészíteném azzal, hogy a korszerű virtuális oktatás megköveteli a tanár-diák kapcsolat, a kommunikáció, a kapcsolattartás új dimenzióban való értelmezését. Egyrészt a hatékony ismeretszerzés érdekében az egyéni tutorálás és csevegés mellett, a **kooperatív tutorálásra** és csevegésre is lehetőséget adnék, szem előtt tartva azt, hogy a tanulók egymás kérdéseiből, észrevételeiből, az azokra kapott válaszokból is tanulnak, hogy megtapasztalva a társak problémáit, bátrabban beszélnek saját problémáikról.

5. A TANANYAG

Az e-learning legkritikusabb pontja a tananyagfejlesztés. Korszerű, az e-learning, illetve a távoktatás minden igényét kielégítő tananyagok csak tanárok, informatikusok, grafikusok, esetleg további segítők közös, összehangolt munkájának eredményeképpen születhetnek.

Azzal együtt, hogy a didaktikai szempontból újat hozó e-learning esetében a súlypont a tanításról a tanulásra helyeződik át, az ismeretek átadása, közvetítése és magyarázata éppen olyan fontos feladat, mint a hagyományos oktatásban. A tananyag feldolgozását önként vállaló tanulók állandó aktivitást igénylő tanulásához a tanár magas fokú szakismeretére, oktatásban szerzett nevelési, pedagógiai, andragógiai tapasztalataira épülő korszerű tananyagra van szükség, amelynek elsajátításához meg kell találni a legalkalmasabb módszertant is, ami legalább olyan fontossággal bír, mint maga a tananyag

Ezeket a gondolatokat hangsúlyozza Vörös Miklós is „eLearning a katonai felsőoktatásban" című tanulmányában: „A tananyag (tartalom) fejlesztés a távoktatás egyik legkritikusabb területe, döntően hat a hallgatók képzettségére, az adott tanfolyam színvonalára. A távoktatási tananyag teljesen más, mint a hagyományos, elkészítéséhez speciális ismeretekkel rendelkező oktatók és szakemberek kellenek, akik felkészítése folyamatosan történik. Az információhordozók (oktatócsomag) létrehozása hagyományos (tipográfia, grafikák elkészítése, nyomdai és egyéb

sokszorosítási munkák) és számítógépes hálózatokon folyó oktatás részére (elektronikus tankönyvek létrehozása, WEB lapokon megjelenő szövegek, képek, mozgóképek létrehozása, feladatlapok kialakítása) egyaránt történik." [1]

Azt gondolom, hogy a távoktató tananyagoknak, olyan tartalommal kell rendelkezniük, hogy a tanulók örömforrásként éljék meg a tanulást, és ez által motiváltabbak legyenek fejlődésüket, tanulmányi eredményeiket illetően. Amennyiben elfogadjuk, hogy a távoktató tananyagoknak ezeket a célokat kell szolgálniuk, teljesen világos, hogy hagyományos úton, hagyományos eszközökkel ez már nem lehetséges.

Tananyagfejlesztés kapcsán **örök kérdés,** hogy nyomtatható formában is rendelkezésére álljon-e a hallgatónak a virtuális oktatásra szánt tananyag?

Véleményem szerint egy korszerű e-tananyag olyan tanulást támogató módszertani megoldásokat tartalmaz, amely nyomtatott formában nem tudja betölteni szerepét.

Igaza van Korom Eriknek: „Ki kell alakulnia annak a „kultúrának", amely nem a feladatok azonnali kinyomtatását és „hagyományos" úton történő megoldását jelenti, elveszítve ezzel az interaktivitás adta előnyt. A másik ok a tanárok hozzáállása. Az interaktív tananyagok elkészítése nem kis munkát és kreativitást követel, mindemellett a végső megjelenése csak csapatmunkában valósítható meg."[5]

A tananyagírás megköveteli, hogy gondos előkészítő munka előzze meg a szakanyag/forrásanyag elkészítését, a tananyag elektronikus tanulásra való előkészítését, a megfelelő média-elemek (kép, hang, grafika, animáció) kiválasztását és nem utolsó sorban értékelési elemek beépítését Az oktatási-tanulási folyamatban ugyanis a tananyag és a tanuló között egyfajta személyes viszony kell, hogy kialakuljon, amely viszonynak elsősorban a tanulói motiváltságot kell kiváltania. A jó tananyag **innovatív gondolkodásra** késztet, lehetőséget ad a gyakorlati tapasztalat kialakítására, és ami a legfontosabb biztosítja a **„szórakozva tanulást"** Az e-tananyag ezzel lesz több a nyomtatott tananyagnál, és ezt a pluszt fogja elveszíteni nyomtatott formájában.

Elektronikus tankönyveim hagyományos, papíralapú formában - a beépített interaktív elemek elvesztése miatt - „oka-fogyottá" válnának: Az **e-tananyag** az önálló ismeret-feldolgozást, az önálló tanulást szolgálja. A téma feldolgozásához multimédiával támogatott passzív és aktív elemeket használ, a mondanivalót képekkel, ábrákkal, grafikákkal illusztrálva mutatja be. A témát információs egységekre bontva szerves egységgé formálja, amely támogatja az elsajátított ismeretek rendszerezését. A beépített irányító elemek és visszacsatolások aktív tanulásra serkentik a tanulót és egyben vezérlik, optimalizálják az ismeretszerzési folyamatot, alkalmazkodva ezzel a tanuló tanulási stílusához és mentális színvonalához. Az **előadások** alapvetően a szemléltető-magyarázó módszerre építenek. A módszer lényege, hogy vizuálisan bemutatok valamit (pl. egy ábra, kép), és ahhoz rövid szöveges információval magyarázatot fűzök. A módszer előnye, hogy egyszerre, összefüggésében mutatja be az adott témát, egy modell segítségével ráirányítja a figyelmet a mondanivalóra, így kizárja a tanuló felfedező vágyát. Az előadások igény szerint on-line, illetve konzerv előadások formájában is meghallgathatók.

6. EREDMÉNYEK

Eredmények csak a minőségen alapuló e-learning-től, illetve távoktatástól várhatók el, amely eredmények azáltal mérhetők, hogy a kurzusokat sikeresen teljesítő tanulók képesek-e alkalmazni tudományos ismereteiket, az elérhető technológiákat és más, az élethez szükséges készségeket.

A kérdés, hogyan fokozható a tanulás, illetve a tanulók eredményessége, hogyan lehet az oktatás sikeres?

Korom Erik szerint az **értékelés** javítja az oktatás minőségét és fejleszti a tanulók személyiségét: „Az értékelés milyensége kihatással van az oktatás minőségére, befolyásolja a tanulók teljesítményét, a hibák korrigálhatóságának mértékét, a tanulók közérzetét, érdeklődését, beállítódását, az iskolához fűződő attitűdjeit. Az értékelés komplex nevelői funkciójának érvényesülése tehát a tanulói személyiség fejlődését befolyásoló komponens." [5]

Véleményem szerint, az **értékelés milyensége** a kulcsfogalom a teljesítményértékelés tekintetében.

A kérdés, hogyan motiválhat egy vizsga, egy számonkérés?

A tanulási folyamatba épített tudásszint-ellenőrzések, vizsgák a hallgatók motiválását a „megajánlott százalék"elérésének lehetőségével, a „hagyományos" vizsgadolgozat kiváltásának lehetőségével motiválják. [5]

„A feladat határidőre történő megoldásnál az elért eredmény érdemjegy javító." [6]

Minden bizonnyal, a kiváló képességekkel rendelkező, aktív, szorgalmas tanulókat ezek a lehetőségek folyamatos tanulásra, mind több és több gyakorló, önellenőrző feladat megoldására serkentik, de hogyan fokozhatjuk a fejlődését az alacsonyabb státuszú hallgatóknak?

Azt gondolom, hogy úgy kell kialakítani az „**értékelés milyenségét",** hogy a számonkérés alkalmával az átlagos, vagy gyengébb képességű tanulóknak is legyen sikerélményük.

Elektronikus könyveimbe - egy-egy tananyagrész befejezéseként - **jutalomórákat** építettem be Az órákon való részvételnek az a feltétele, hogy a tanuló egy igen egyszerű feladatot – például egy alapfogalmakra épülő keresztrejtvényt – megoldjon. A megoldás a jelszó, amivel beléphet a jutalomórába, amely egy tanmese, egy anyagrésznek a játékos bemutatása [http://www.lengyelpiroska.hu/szamvitele/konyv/jutalom_eloadas.html]

Véleményem szerint a tanulói teljesítmények értékelésekor, az értékelési módszerek kidolgozásakor, abból kell kiindulni, hogy **a siker motivál**, és hogy **a sikerhez nagyfokú motiváltságra van szükség.**

ÖSSZEFOGLALÁS

A virtuális környezetben megvalósított oktatás csak akkor lehet eredményes, ha a kognitív stílusokat, az egyének tanulási különbségeit is figyelembe vevő minőségi tananyagokat fejleszt, olyan tanulási módszertannal, amely felkelti a tanulók érdeklődését, amely tanulásra serkent.

Természetesen nagy a felelőssége az oktatóknak, az intézményeknek, amikor bezárják az ajtaját a hagyományos osztályteremnek és kinyitják a kapuit az új, de még sok kérdőjelet hordozó virtuális iskolának. De, ha pedagógusként tisztában vagyunk azzal, hogy mi érdekli a tanulókat, hogy hogyan tanulnak, milyen a tanulási stílusuk, hogy miként lehet az érdeklődésüket felkelteni, és ha, mi magunk képesek vagyunk a tudást, az információt átadni, a rendelkezésre álló eszközök segítségével hatékonyan közvetíteni, akkor érdemes kinyitni a virtuális oktatás kapuit.

Zárásként Vörös Miklóst idézem:

„a Magyar Honvédség részére szükségszerű az új tanítási/tanulási módszerek, eszközök és médiumok bevezetése és elterjesztése. Az egyén versenyképessége közvetlenül kapcsolódik a teljes életpályára kiterjedő tanuláshoz, mely alapvető célja a kreativitás, a rugalmasság, az adaptációs, a

problémamegoldó és a tanulási készségek folyamatos fejlesztése. A tanulás és önképzés a pályán maradás és előrejutás feltételévé válik.” [2]

Felhasznált irodalom

[1] Polónyi István: Válasz az e-learning, de mi volt a kérdés? http://www.hier.iif.hu/hu/educatio_reszletes.php?id=14 (letöltés ideje: 2009. október 18.)

[2] Vörös Miklós: eLearning a katonai felsőoktatásban http://www.szamalk.hu/eLearning/Default.htm (letöltés ideje: 2009. augusztus 12.)

[3] Vörös Miklós Élethelyzethez igazított tanulás http://www.szrfk.hu/rtk/kulonszamok/2008_cikkek/Voros_Miklos.pdf (letöltés ideje: 2009. október 18.)

[4] Béres Ilona, Magyar Tímea, Turcsányi-Szabó Márta: e-tanulás hatékonyságának feltételei a felsőoktatásban http://www.agr.unideb.hu/if2008/kiadvany/papers/C21.pdf (letöltés ideje: 2009. szeptember 15.)

[5] Korom Erik A felsőoktatásban tanulók motiválhatósága elektronikus támogatással http://elib.kkf.hu/okt_publ/tek_2004_16.pdf, (letöltés ideje: 2009. augusztus 10.)

[6] Dr. Pálinkás Jenő: Piacfejlesztés tantárgy elektronikus tananyagfejlesztése http://agrinf.agr.unideb.hu/if2005/kiadvany/papers/B54.pdf (letöltés ideje: 2009. szeptember 15.)

[7] Buda András: Virtuális oktatás http://epa.oszk.hu/01500/01551/00025/pdf/276.pdf (letöltés ideje: 2009. október 21.)

[8] Nagy Sándor (1976, szerk.): Pedagógiai Lexikon. Akadémiai Kiadó, Budapest. 444. oldal.

[9] Gabnai Katalin: Drámajátékok - Bevezetés a drámapedagógiába, Helikon kiadó, 2008

[10] Gerő Péter: Az élethelyzethez igazított tanulás. Egyetemi tankönyv, ZMNE, 2008. 15. oldal

HADMÉRNÖK
V. Évfolyam 2. szám - 2010. június

Papp Csaba
pappcs@hajdu.police.hu

Solymosi Krisztina
solymosi@orfk.police.hu

Horváth László
horvath.laszlo@zmne.hu

Hullám István
hullam.istvan@zmne.hu

A BIZTONSÁG FOKOZÁSA A MAGYAR KÖZTÁRSASÁG SCHENGENI KÜLSŐ HATÁRSZAKASZÁN

Absztrakt

Magyarország, földrajzi elhelyezkedése miatt, kiemelten fontos biztonsági pillére az EU határbiztonsági rendszerének, Ukrajnán és Románián keresztül a volt Szovjetunió tagköztársaságaiból, Szerbián keresztül a Balkáni országokból kiinduló illegális migráció beáramlásának megakadályozásában. Schengeni tagságunkkal a veszélyek nem csökkentek, sőt a belső határon megszűnt ellenőrzés miatt — a keletkező biztonsági deficit csökkentésére — a határbiztonsági rendszert gyökeresen át kellett alakítani.
A jövő határbiztonsága az összetett kihívások (terrorizmus, áru- és embercsempészet, migráció-közbiztonság, korlátozott anyagi források) miatt integrált szemléletű határigazgatási rendszer kialakítása válik szükségessé. Mondanivalónk rávilágít arra, hogy elengedhetetlenül fontos a hagyományos határrendészeti tevékenységért felelős szervezet átalakítása, illetve megerősítése a legmodernebb katonai illetve civil szférában használatos technikai eszközökkel.

Having been at the crossroads of illegal eastern migration patterns, Hungary — situated right next to Ukraine, Romania, Serbia and through it the Balkan States — takes an important role concerning EU border security. Despite the country's membership of the Schengen area, threats are rather evolving than diminishing through the abolition of internal borders, which calls for an immediate action aiming to reconstruct the border security system.
Due to various challenges (including terrorism, smuggling, illegal migration, versus limited resources) an integrated approach (Integrated Border Management – IBM) is necessary to maintain border security in the future. In the following pages we would like to emphasize the importance of reorganizing the traditional border management and security systems, as well as supporting them with the newest military and civilian technologies.

***Kulcsszavak**: schengeni külső határ, határrendészet, pilóta nélküli repülő, migrációs halo, alkalmasságvizsgálat, stressz ~ Schengen external border, border management, no-pilot airplane, migration network, aptitude test, stress*

BEVEZETÉS

Magyarország életében a honfoglalástól egészen napjainkig mindig fontos feladat volt az államhatár védelme, ezzel biztosítva az ország függetlenségét és szuverenitását. A határ védelméért és őrizetéért Magyarországon a történelmünk során többször változó népcsoportok, katonai illetve rendészeti szervezetek voltak felelősek. A gyepűrendszertől a székely nemzeten keresztül a *Magyar Királyi Határrendőrség, Magyar Királyi Határőrség, Magyar Királyi Folyamőrség, Magyar Állami Határrendőrség, Államvédelmi Hatóság, BM Határőrség és napjainkban a Magyar Köztársaság Rendőrsége*, amelyet a mindenkori politikai helyzet folyamatosan befolyásolt [1].

Az 1989. évben történt rendszerváltást követő átalakítás az államhatár védelmével kapcsolatosan a rendészeti jellegű tevékenységek dominanciáját hozta, amely csak az első lépésnek tekinthető. Az ország integrálódása, a világban és régiónkban keletkező új körülmények újabb és újabb kihívásokat és feladatokat jelentenek, amelyre adott határőrizeti válaszok megkövetelték a határőrizeti, valamint a vám- és pénzügyőri szervezetrendszerek rugalmas átalakítását. 2004. május 01-i Európai Uniós csatlakozásunk nagy lépést jelentett az ország fejlődésében, és a közös vámunió tagjaként megkövetelte a Vám- és Pénzügyőrség diszlokációjának újraszervezését. A 2007. december 21-i szárazföldi és a 2008. március 31-i légi teljes jogú schengeni tagságunkból fakadó határnyitással pedig egy olyan folyamat zárult le, amely a schengeni belső határainkon az ellenőrzés megszüntetésével az önálló határőrizeti szervezetet is megszüntette.

Az integráció komoly feladat elé állította a rendőrséget, hiszen ezután felelnie kell a keletkező biztonsági deficit csökkentéséért, valamint a schengeni külső határszakaszok szigorított védelméért is.

Ezen publikációnkban a rendészeti szervek, különösen a Rendőrség magyarországi határigazgatásban[1] betöltött szerepének változásával foglalkozunk, valamint a klasszikus határrendészeti feladatok és rendszerek, továbbá az ezeket támogató informatikai és technikai eszközöket mutatunk be, illetve az állomány pszichológiai alkalmasságvizsgálatának hatékonyabbá tételére teszünk javaslatot.

AZ EURÓPAI UNIÓ HATÁRIGAZGATÁSI TÖREKVÉSEI

Az Európai Uniós gyakorlat szerint, a közös menekült-, migrációs és határigazgatási politika korábban főként jogszabályalkotással jött létre. Ezen jogszabályok alapozták meg az e területeken folytatott közösségi politikát. Az előírások végrehajtásában azonban az egyes tagállamokra különböző teher hárul, némelyikük aránytalanul nagy részt visel az egész közösség javát szolgáló kötelezettségekből, az egyenlőtlen alkalmazás pedig veszélyezteti az egyenlő feltételek kialakítását célzó törekvést. E politikaterületek meglehetősen sok személyt érintenek. A 27 tagú EU-ban a tagállamokra körülbelül 6000 km szárazföldi és mintegy 90 000 km tengerparti határ ellenőrzésének feladata hárul, a becslések szerint évente 100 millió utas érkezik az EU nemzetközi repülőtereire, köztük olyan személyek, akiktől meg kell tagadni a belépést.

---

[1] A tanulmányban az integrált határigazgatási és integrált határbiztonsági rendszer kifejezést egymás szinonimájaként használjuk, amely az angol integrated border management fordításának tekinthető.

Olyan közösségi pénzügyi szolidaritásra van szükség, amely képes támogatni a migrációs áramlások igazgatására megállapított átfogó, kiegyensúlyozott európai uniós megközelítés továbbfejlesztését és végrehajtását, és amely megfelelően járul hozzá a tagállamok által elkötelezett schengeni vívmányok alkalmazásához és a közös uniós integrált határigazgatási rendszer létrehozásához. Ennek megfelelően a tagállamok kötelesek a külső határokon hatékonyan kezelni a személyek áramlását, és így biztosítani egyrészt — a tagállamok belbiztonsága érdekében — a külső határok magas szintű védelmét, másrészt a jóhiszemű utasok zökkenőmentes határátlépését, például a tagállamok konzuli szolgálatai által kibocsátott vízumokkal. Ez azt jelenti, hogy az illegális belépések csökkentésére biztosítani kell különösen a földközitengeri partvonalat és keleti szárazföldi határokat, továbbá javítani kell a tagállamok harmadik országokban működő konzuli szolgálatainak tevékenységét.

A KÖZÖSSÉGI POLITIKA HATÁRŐRIZETI CÉLKITŰZÉSEINEK ELÉRÉSE

A közös politika célja, hogy a belső határokon történő átlépéskor a személyek állampolgárságuktól függetlenül mentesüljenek mindenfajta ellenőrzés alól; a külső határokon a személyek ellenőrzésének eredményes felügyelete valósuljon meg; az integrált határőrizeti rendszer fokozatosan kerüljön bevezetésre; továbbá az illegális bevándorlás és az emberkereskedelem megelőzésére és az ellene való küzdelemre fokozott figyelmet tudjanak fordítani.

Ezen célok eléréséhez az Unió forrásokat is rendelt, azaz megteremtette a feltételét célkitűzései elérésének. Az Európai Bizottság már a 2007–2013. közötti időszakra szóló, pénzügyi tervet meghatározó stratégiai irányról szóló közleményében kiemelt célként nevezte meg a szabadság, biztonság és a jog érvényesülésén alapuló térség fejlesztésének megfelelő pénzügyi forrásokból való támogatását, melyeket a „Polgárság, szabadság, biztonság és a jog érvényesülése" néven új fejezetben kellett szerepeltetni. A javasolt „Szolidaritás és a migrációs áramlások igazgatása" keretprogram [2] célja az Európai Tanács célkitűzéseivel összhangban — az Unió külső határai integrált igazgatásának bevezetéséből és a közös menekült- és bevándorlás politikák végrehajtásából adódó pénzügyi teher kapcsán — a tagállamok közötti igazságos feladatmegosztás kérdésének megoldása.

A keretprogram a Varsói székhelyű FRONTEX Ügynökséggel[2] kiegészítve a külső határok ellenőrzése és őrizete (*integrált határigazgatás*), valamint a vízumpolitika területén hozott létre pénzügyi szolidaritási alapot. A külső határ- és vízumpolitika, valamint a menekültpolitika végrehajtását támogató nagyméretű informatikai (IT) rendszerek (a Vízuminformációs Rendszer, a Schengeni Információs Rendszer és a EURODAC[3]) kialakítása a tagállamok közötti együttműködés és költséghatékony információcsere létrehozásával különösen hozzájárul a közösségi szolidaritáshoz.

A FRONTEX Ügynökség tevékenysége is hatékonyan javíthatja az együttműködést a technikai és működési támogatás, valamint az eszközök és források — minden résztvevő állam számára hozzáférhető — egyesítése révén.

MAGYARORSZÁG STRATÉGIAI CÉLKITŰZÉSE A HATÁRŐRIZET TERÜLETÉN

Magyarország az Unióhoz és egyéb nyugat-európai szervezetekhez való integrációs törekvése nyomán stratégiai jellegű dokumentumaiban [3] kinyilvánította határőrizeti feladatainak fontosságát és az Európai Uniós értékeknek való megfelelését. Ennek alapján kifejezésre juttatta, hogy Magyarország határai várhatóan hosszabb ideig az EU és a schengeni térség külső hatá-

---

[2] Az Európai Unió Tagállamai Külső Határain Való Operatív Együttműködési Igazgatásért Felelős Európai Ügynökség

[3] Az European Dactyloscopy rövidítéséből származik a név, ez egy ujjlenyomatokat tároló európai adatbázis

rai lesznek, ami együtt jár az uniós határszakasz igazgatásának felelősségével és terheivel.
A migráció Magyarországot korábban elsősorban tranzitországként érintette, viszont napjainkban hazánk azonban egyre inkább célországgá is vált (e megállapítást támasztják alá többek között Lajosmizsén, 2010. március 24-én megtartott, „A határrendészet helye, szerepe, jövője a schengeni övezetet érintő változások tükrében" című tudományos konferencián elhangzottak is). Magyarországnak az EU közös, vagy közösségi politikája által érintett keleti és délkeleti szomszédjai európai integrációs kilátásaik, migráció-, kibocsátó- és áteresztő szerepük továbbá a szervezett bűnözés elleni erőfeszítéseik szempontjából eltérnek egymástól. A migrációt természetes, de összetett jelenségként kell kezelni, mely gazdasági és demográfiai előnyöket, valamint biztonsági kockázatokat is egyaránt magában rejt.

A lehetőségeket és a kihívásokat is az európai integráció közép-, vagy hosszú távú perspektívájában használhatjuk ki, illetve kezelhetjük legmegfelelőbben. A biztonsági kockázatok kezelését az uniós tagságból fakadó kötelezettségek teljesítése mellett saját nemzeti biztonsági érdekeink is megkövetelik. Az illegális migráció elsősorban rendészeti kérdésként jelentkezik. A schengeni csatlakozást követően a külső — elsősorban szárazföldi — határok fokozott védelme a magyar határőrizeti szervek és a bevándorlási hivatal, valamint a Vám- és pénzügyőrségi szervezetrendszer hatékonyabb együttműködését követeli meg. A schengeni együttműködéshez történő csatlakozással párhuzamosan az uniós támogatások hatékony felhasználásával korszerű és biztonságos határigazgatási rendszert kell kiépíteni.

Az egyesült Európa országai a schengeni külső határokon a biztonság megerősítésével ellensúlyozzák a belső határellenőrzések megszüntetését. Ezért az Európai Unió a 2004-ben csatlakozott országok számára a csatlakozási szerződés [4] 35. cikke alapján létrehozta az ún. Schengen Alapot. Ez az ideiglenes pénzügyi alap 2004. és 2006. között pénzügyi segítséget nyújtott az érintett tagállamoknak annak érdekében, hogy az EU új külső határain a schengeni vívmányok érvényesülését és a külső határellenőrzés előírt feltételeit biztosíthassák.

A Schengen Alap tervezése során négy fő célkitűzést határoztak meg:
- a külső határok őrizetével kapcsolatos fejlesztések;
- a mélységi ellenőrzés hatékonyságának növelése;
- a rendészeti szervek adatszolgáltatási képességének növelése;
- a nemzetközi bűnügyi együttműködési képesség és kapacitás fokozása.

Az *Igazságügyi és Rendészeti Minisztérium* (korábban Belügyminisztérium) által megvalósított ilyen irányú fejlesztések rendkívül összetettek. A külső határon található határrendészeti kirendeltségek új épületbe történő költöztetése, illetve a kapcsolódó *építési beruházásoktól* kezdve a speciális eszközbeszerzéseken át a komplex informatikai fejlesztésekig igen sokféle fejlesztés fedezetét teremtették meg a Schengen Alap forrásai.

Az *eszközbeszerzések* nyomán továbbfejlődött a határellenőrzés speciális technikai háttere, a mobilitást biztosító gépjármű állomány és a rádió-kommunikáció technikai feltétele. Mindezek elősegítették az európai szintű határőrizetet, a határforgalom-ellenőrzést és megvalósult az integrált határrendészet. Az *informatikai* eszköz és alkalmazás fejlesztések nyomán megvalósult a nyilvántartások harmonizációja. Ezen kívül lehetővé vált a schengeni elvárásoknak megfelelő adatcsere, valamint az egyszerűbb és gyorsabb idegenrendészeti ügyintézés. Az informatikai fejlesztések további célja, hogy biztosítsa a második generációs Schengeni Információs Rendszerhez (SIS II) történő csatlakozás technikai feltételeit.

Az építési beruházások eredményeként számos határőrségi, rendőrségi és idegenrendészeti objektum felújítása történt meg. Az állomány Külső Határos Alapból finanszírozott speciális *szakmai, illetve nyelvi képzése* jelentősen elősegítette az európai uniós gyakorlat hazai adaptálását.

Szintén a beruházások keretében került sor a Vám- és Pénzügyőrség tulajdonában és kezelésében lévő közúti *határátkelőhelyek fejlesztésére*, a *biztonsági térfigyelő kamerarendszer*

kiépítésére, vasúti és kamionröntgenek beszerzésére. Jelentős összeg került felhasználásra a *mélységi ellenőrzés* hatékonyságának növelésére a bevetési erők és a Határvadász századok fejlesztésére.

Magyarország Nemzeti Biztonsági Stratégiájából [3] egyértelműen kitűnik, hogy az igazi veszélyt az államhatárán átnyúló szervezett bűnözés, a nemzetközi terrorizmus, az illegális migráció jelenti hazánk számára. Meggyőződésem, hogy Magyarország a teljesjogú schengeni tagságának elérése végett a felkészülésre biztosított forrásokat hatékonyan és eredményesen használta fel, melyet mind a szárazföldi mind a légi Seval ellenőrzés tapasztalatai alátámasztanak, azonban a határőrizetünk területén az elért színvonal fenntartására és a folyamatos jövőbeli fejlesztésekre a továbbiakban is figyelmet és erőforrásokat kell fordítani.

A NEMZETKÖZI SZŰRŐRENDSZEREK HÁLÓZATÁRA ÉPÜLŐ MAGYARORSZÁGI HATÁRBIZTONSÁGI RENDSZER

A nemzetközi „szűrőrendszer" [5] alapvető elemei: a vízumrendszer, a politikai, gazdasági tájékoztató eszközök, az összekötő tisztek, a külképviseletekre kihelyezett okmányszakértők, a szállító vállalatok, a tranzitállamok határőrizeti rendszere, a biztonságos harmadik országok, a külső határok szigorú őrizete, a belső határ ellenőrzése, valamint a kiegyenlítő intézkedések.

A schengeni tagságból adódóan Magyarország határbiztonsági rendszere új alapokon nyugszik, hiszen a schengeni tagállamok biztonsága — így a határbiztonság — nem csak a Rendőrség feladata, ezért a biztonságért való közös felelősség érdekében kiemelendő feladat korszerűsíteni a magyar rendvédelmi szervek együttműködését.

Kiemelt fontosságú a Katasztrófavédelmi Igazgatóságokkal a folyamatos és koordinált együttműködés. A magyar- és a szomszédos országok rendészeti szerveinek együttműködése elengedhetetlen feltétele az államhatáron átható természeti, ipari katasztrófák kezelése terén a hazai katasztrófavédelmmel kialakított és hatékonyan működtetett közös tevékenységnek.

A magyar rendvédelmi szerveken belül, valamint az eddigi együttműködésben szükségszerűen egy minőségében magasabb szintű kooperáció, racionális feladatmegosztás és integráció jött létre. Magyarország az EU-ban egyedüli példa arra, hogy a Rendőrség koordinálásával a Rendőrség, Vám- és Pénzügyőrség, Bevándorlási és Állampolgársági Hivatal, valamint az Országos Munkavédelmi és Munkaügyi Főfelügyelőség egységes elvekre és gyakorlatra épülő hálót alkalmaz az illegális migráció kiszűrése érdekében országos, területi és helyi szinten egyaránt (Integrált Vezetési Központ) [6] .

Az integrációs és együttműködési cselekvési kényszer alapvető okai között megemlítendő, hogy a 2001. szeptember 11-ei terrortámadás óta a biztonság iránti igény világszerte megnőtt. A fokozott biztonság megteremtésének nemzetközi szinten követett egyik legfőbb eszköze és módszere az együttműködés kiszélesítése, elmélyítése, valamint a szervezeti és tevékenységi integráció. Az integráció másik oka, hogy az állam drasztikusan csökkenteni kívánja saját működésének költségeit. Ezt legkönnyebben a közigazgatásban, és ezen belül a rendvédelmi szerveknél tudja elérni, különböző integrációs mechanizmusokkal. A biztonsági igény fokozódása, és a költségtakarékosság tehát párhuzamos folyamatként zajlik. A rendvédelmi szerveknek, ha a kihívásoknak meg kívánnak felelni, egy lehetőségük van, alternatívákat kínálni az átstrukturálódásra és a költségmegtakarításra. Az EU-hoz történő csatlakozásunkkal, amely a „szabadság, jog és biztonság" térsége a rendvédelmi szervekkel szembeni elvárások megnőttek, új nemzetközi dimenziót kaptak, a külső határokkal közösségi feladatok jelentkeztek, melyek végrehajtását a jelenleg a rendvédelmi szervekre jellemző alulfinanszírozottság ellenére is számon kérik. Az Országgyűlés négyéves politikai rotációi jelentősen megnehezítik a stratégiai elgondolások kivitelezését, mert újabb és újabb koncepciók jelentkeznek a váltások kapcsán és sajnos az újrakezdés gyakran több áldozattal jár, mint a régi korrekciója. A rendvédelmi szervek együttes tevékenységének jogi és szervezeti alapjai már most is adottak. Korábban a Rendőrség és a Határőrség stratégiai partnersége, illetve most az integrált egységes

szervezet, valamint a Vám- és Pénzügyőrséggel megvalósuló több évtizedes szoros együttműködés jó alapot ad egy új típusú, minőségében más feladat-összehangolásnak.

AZ INTEGRÁLT HATÁRIGAZGATÁSI RENDSZER MAGYARORSZÁGON

Az *integrált határigazgatási rendszer*[4] egy komplex, gyakorlatilag a határőrizet és -ellenőrzés során alkalmazott különböző technológiákat fedő fogalom (technológiai rend, szolgálatszervezés, informatikai rendszerek együttese), amelynek célja, hogy megfeleljen annak a közösségi kihívásnak, hogy egyrészt megkönnyítse a legális személy és áruforgalmat, másrészt fenntartsa a biztonságos határokat.

Ide tartozik a schengeni ellenőrzés rendszere, az egy megállásos ellenőrzés, az átfogó mélységi ellenőrzés, a térfigyelő kamerák, a sugárkapuk működtetése, illetve a határátkelőhelyeken működtetett szoftverek alkalmazása is.

HATÁRELLENŐRZÉSI ÉS REGISZTRÁCIÓS RENDSZER (HERR)

A Határregisztrációs rendszer definíciója szerint olyan sajátos multimédiás számítógépes rendszer, amely arra hivatott, hogy elősegítse a nemkívánatos és körözött személyek, járművek adatainak automatikus leolvasását, egyeztetését, rögzítését, bizonyos személyek, tárgyak járművek kiszűrését, beléptetésének megtagadását, az EU, illetve a schengeni övezet külső határán funkcionáló határátkelőhelyeken való mozgásának folyamatos nyomon követhetőségét, a törvényileg meghatározott adatok bizonyos időtartamig történő tárolását, ezáltal a bűnüldöző és a nemzetbiztonsági elvárások teljesülését.

Magyarországon a Határőrségnél 1998-ban már rendszerbe állt egy, a határforgalomellenőrzést nagymértékben elősegítő, hatékonyabbá, gyorsabbá és biztonságosabbá tevő számítógépes regisztrációs rendszer. Ezt több alkalommal módosították, majd 2005. február 09-én véglegesen leállították, és egy modernebb, más felépítésű, a célokat hatékonyabban szolgáló rendszer kezdte meg működését (HERR[5]). A schengeni tagságunkkal lehetővé vált ennek a SIS rendszerhez történő csatlakozása is.

Jelenleg a Határ Ellenőrző és Regisztrációs Rendszer, a Rendőrség (korábban a Határőrség) által üzemeltetett informatikai alkalmazás, amely a határforgalomban megjelenő személyek, járművek adatait (nevezetesen: név, útlevélszám, állampolgárság, rendszám, határátkelőhely, határátlépés iránya) veti össze a központi és az uniós nyilvántartásokkal.

A SCHENGENI INFORMÁCIÓS RENDSZER (SIS RENDSZER)

A Schengeni Információs Rendszer [7] egy olyan személy- és tárgynyilvántartási, körözési rendszer, amelynek azonos tartalmú adatbázisát a tagállamok mindegyike a központi adatbázisból kapott jelzések alapján vezeti, és nemzeti adatbázisából maga is jelzéseket küld a központi adatbázison keresztül a többi tagállam részére, így alkotva egy európai hálózatot. A rendszerből bármely tagállam lekérhet információkat, értelemszerűen azonban nem módosíthatja, nem változtathatja meg más tagállamok adatait, bejegyzéseit. A SIS-hez történő csatlakozás lehetővé tette, hogy a belső határokon folytatott ellenőrzés megszűnjön, illetve a schengeni külső határrezsimet vezessék be az érintett határszakaszokon, valamint a mélységi ellenőrzéseket ezzel egyidejűleg a schengeni adatbázis lekérdezésével tegyék hatékonnyá.

A Schengeni Információs Rendszer több elemből áll. A rendszer magja a Strasbourgban

---

[4] más fordításban integrált határbiztonsági vagy határirányítási rendszer (az IBM, Integrated Border Management kifejezés fordítása)

[5] Határ Ellenőrző és Regisztrációs Rendszer

működő C-SIS, amely összefogja az egész rendszert. A hálózatot az egyes tagországokban működő nemzeti N-SIS egységek alkotják. A SIS-rendszert kiegészíti a SIRENE[6] hálózat, amely lehetővé teszi, hogy a nemzeti és a helyi rendőrség, az igazságügyi szervek és a vámhatóságok kiegészítő információkat cseréljenek ki egymással. A SIRENE feladata az információk megszerzése, cseréje, a koordináció és a konzultáció segítése. A SIS I rendszert kialakítása óta többször módosították, ezzel hozzáigazították a megváltozott jogszabályi követelményekhez. A legnagyobb változást a 2004-ben az EU-hoz csatlakozott országok belépése okozta.

A SIS II-es rendszer bevezetésének csúszása miatt a SIS I-es rendszert kellett átalakítani oly módon, hogy alkalmas legyen az új tagállamok jelzéseinek kezelésére is. Ezt a bővítést a SISone4ALL projekt keretében hajtották végre a strasbourgi központ, a régi és az új tagállamok mindegyikének közreműködésével. Ugyanakkor az Unió bizottsága továbbra is szorgalmazza eredeti terveinek megfelelően a SIS II-es rendszer kialakítását és üzembe állítását.

A SIS II információs rendszer célja, hogy egy központi adatbázisban tartalmazza mindazon információkat, amelyek révén ellenőrizhető a schengeni térségbe belépő összes személy. A nyilvántartás tartalmazni fogja azon személyek adatait, akiket egy adott időtartamra bizonyos helyekről, városokból, rendezvényekről kitiltottak, nyilvántartásba kerülnek a tagállamok által elutasított vízumkérelmek is (a vízumok kezelésére hivatott Visa Information System, VIS). Egy terrorista-adatbázist is kialakítanak, illetve rögzítik azoknak a személyeknek az adatait is, akik valamilyen oknál fogva nem hagyhatják el a schengeni országok területét. Az adatbázis teljeskörűen tartalmazni fogja a körözött és eltűnt személyek, a lopott autók, az elveszett, ellopott személyi okmányok és bankjegyek adatait is.

A SIS II a szöveges adatok mellett biometrikus azonosítók adatait is fogja tudni kezelni, a további fejlesztések révén DNS adatok is tárolhatók lesznek. A jelenlegi SIS I-es rendszernél lényegesen alkalmasabb lesz a rendszer a jó minőségű fényképek tárolására.

A SIS II. rendszerrel szemben elvárt követelmények:

- nagyobb teljesítőképesség a több tagország kiszolgálására;
- a rendszernek rugalmasnak, egységesnek, megbízhatónak, biztonságosnak kell lennie;
- naprakészség, a megnövekedett adatbázis lehetőségeinek hasznosítása;
- költséghatékonyság, gazdaságosság;
- a közösségi és a nemzeti erőforrások megosztása;
- a biometrikus adatok és más új információs adatok kezelésének képessége;
- új EU-s igazságügyi eljárások támogatása (pl. EAW, European Arrest Warrant európai elfogató parancs, kiadatási egyezmény).

Az EU hivatalos leírása szerint a SIS II nemcsak a bűnözők, hanem a gyanúsítottak adatait is tartalmazza majd, valamint benne lesznek az eltűntnek vélt személyek is. A rendszer további célja, hogy meggyorsítsa a schengeni országokba belépő, vagy esetlegesen az egyik schengeni országból a másikba utazó illegális bevándorlók azonosítását.

A KOMPLEX MÉLYSÉGI ELLENŐRZŐ RENDSZER KERETÉBEN MŰKÖDTETETT MIGRÁCIÓS HÁLÓ (CHECKNET-RENDSZER)

A belső határokon a határellenőrzés ideiglenes visszaállítása átfogó EU jogszabályokba foglalt tagállami kötelesség. E követelmény teljesítésének a feltételei az eddig működtetett határőrizeti rendszerrel pár év alatt megszűnnek, ezért elengedhetetlen feladat olyan módszer és technológia kidolgozása, amely biztosítja a schengeni belső határokon az ellenőrzés ideiglenesen visszaállításának megfelelő végrehajtását.

---

[6] a név a "Supplementary Information REquested at the National Entries" rövidítése, a SIRENE egy, a nemzeti és helyi rendőri, vámügyi és igazságszolgáltatási szervek képviselőiből álló, 24 órás kölcsönös információs szolgálatot fenntartó hálózat

A *CheckNet*[7] *rendszer* [8] keretében végzett igazoltatási, jármű-, terület- és munkavégzés ellenőrzési tevékenység bizonyos tekintetben analóg a belső határokon végzendő határellenőrzéssel, hiszen ebben az esetben is a terepen kell a személyek kilétét, jogos ott tartózkodását megállapítani, a járművekkel kapcsolatos adatokat megszerezni.

Az EU követelményeknek megfelelő CheckNet kialakítása azt a célt szolgálja, hogy az adott ország mélységében meghatározzák azokat az ellenőrzési pontokat, ahol eredményesen lehet fellépni az utazó bűnözők, sorozat bűncselekményt elkövetők, az illegális migránsok, az embercsempészek, a terrorista gyanús személyek ellen. Ebben a feladatban a Rendőrség közrendvédelmi, közlekedésrendészeti és határrendészeti szolgálati ága mellett részt vesz a Vám- és Pénzügyőrség és az Országos Munkavédelmi és Munkaügyi Főfelügyelőség is.

A CheckNet-rendszer oly módon továbbfejleszthető mobil okmány- és ujjnyomolvasó készülékekkel, titkosított mobil kommunikációval (EDR[8]), egységes rendvédelmi térinformációs elemző- és vezetési rendszerrel, on-line adatkapcsolatokkal (központi adatbázisok, SIS, VIS), hogy képes legyen a terepről a megfelelő személy- és jármű ellenőrzésre, az igazoltatási adatok közvetlen eljuttatására a megfelelő adatbázisokba. Ezáltal megteremt egy olyan működő rendszert, amely bármikor áthelyezhető az ország mélységéből a belső határra és ott képes a határellenőrzés alapvető feladatainak az ellátására, egyéb esetben pedig magas színvonalon szolgálja az egységes rendészeti elvárásokat. Ez a működő CheckNet-rendszer az általános helyzetben nagy mértékben szolgája a nemzetközi szervezett bűnözés elleni harcot, a csempészek, illegális bevándorlók, az illegális munkavállalók felfedését, az operatív nemzetközi rendészeti és bűnügyi információcserét, ezáltal kettős cél teljesíthető. Egyrészt létrejön egy általánosságban működő, komoly rendészeti szűrőrendszer, másrészt pedig adott a belső határ ellenőrzési infrastruktúrája, szakértelme.

Magyarország a felsorolt informatikai rendszerek kiépítésében és használatában jelentős eredményeket ért el, azonban a világban bekövetkező XXI. századi információ-technológiai fejlődés nem szab határt a lehetőségek kiaknázásának. A technika fejlődését ugyan nyomon tudjuk követni, de lépést nem tudunk vele tartani, ezért továbbra is elmaradottak vagyunk a térinformatikai kamerákat használó bevetés-irányítás, a műholdas járműkövetés és azonosítás stb. területén, amely a következő időszak fejlesztési prioritása lehetne, főként a klasszikus zöldhatár őrizetében maradtak további fejlesztési lehetőségek.

Az átkelőhelyeken alkalmazott technikai és informatikai rendszerek hatására, a zöldhatárra egyre nehezedő nyomás csökkentésére számos lehetőség kínálkozik. Ilyen például, hogy a határátkelőhelyeken a már említett technikai és informatikai fejlesztések élveznek prioritást, a zöldhatár őrizetére beszerzett gépjárművek nagy segítséget jelentenek a mobil és kézi hőkamerák alkalmazása mellett.

A nehezen járható határszakaszok biztonságos ellenőrzésére eddig még nem született hatékony megoldás (ez alatt a hegyes, erdős, mocsaras illetve a mezőgazdasági növényi kultúra termesztése miatt fedett területeket értjük). A sorozott állomány kivonásával nemcsak a nap 24 órájában bevethető komoly erő szünt meg, hanem a nehezen járható terepekről eltűntek a lovak is, melyek kiváltása a mai napig nem megoldott.

TOVÁBBI TECHNIKAI ESZKÖZÖK ALKALMAZÁSÁNAK LEHETŐSÉGEI

A 90-es évek közepén már alkalmazott, de azóta leselejtezett Honda terepmotorok ismételt szolgálatba állítása változatossá tehetné a járőrözési rendszert, hiszen ezek az eszközök könnyűek, gyorsak, szinte bárhová képesek eljutni, és gazdaságos fogyasztásuknak köszönhetően jóval nagyobb határszakaszt lehet velük leellenőrizni, mint a személygép-

---

[7] Ellenőrzési Háló - Migrációs Háló ellenőrzési rendszer

[8] Egységes Digitális Rádiórendszer

járművel. Emellett beszerzési, és fenntartási költségük is jóval alacsonyabb, mint egy gépjárműnek.

Véleményünk szerint rendkívül hasznos, azonban különös szakértelmet senkitől nem igénylő eszközök a quadok. Európa nagyon sok határrendészeti szervénél évekkel ezelőtt megtörtént a rendszerbeállításuk, mely alkalmazhatóságáról csak pozitiv jelzések látnak napvilágot. Ezek a 4X4 típusú motoros járművek a zöldhatár ellenőrzésében jóval hatékonyabbak, megfelelő kialakítású, terepre gyártott fajtájuk sokkal kevésbé sérülékeny, viszont jelentősen mozgékonyabb, mint egy terepjárógépjármű. Alkalmazhatók olyan területeken is, ahol a szolgálati járművek nem képesek elmenni. Kisebb helyet foglalnak, ezáltal szükség esetén álcázásuk is jóval egyszerűbb. Emellett igen gyorsak, és nem utolsó sorban gazdaságosak. Napi karbantartásuk nem jelent nagyobb kihívást a személyi állomány részére, mint régebben a lovak, vagy ma a személygépkocsik.

A technikai eszközök célja a határőrizet és -védelem megerősítése, hatékonyabb határellenőrzés biztosítása, a Magyarország területén és a határok menti bűnüldözés elleni küzdelem hatékonyságának a fokozása. Ezek a szerkezetek elősegítenék az illegális határsértés felfedését azokon a területeken, melyek közkedveltek a migránsok körében a járőrök általi nehezen megközelíthetőség miatt, illetve ott, ahová a határrendész állomány a nagy távolságból adódóan ritkábban jut el szolgálata során.

Rendkívül nagy előnyt jelent az eszközök észrevétlensége, rejthetősége, ami ezáltal garantálja azt, hogy a határsértők nem érzékelik azt, hogy cselekményük az illetékes szerv által felfedésre került.

Ilyen eszközök például a MIDS I-IV. lépésérzékelők (szeizmikus, passzív infra érzékelő, mágneses érzékelő), a COP 99 lézeres lépésérzékelő vagy az EMIDS lépésérzékelő (szeizmikus, passzív infra érzékelő).

A MIDS és EMIDS rendszerek előnyei

Ezeknek a készülékeknek a hatótávolsága 1,5 km – 30 km, amely garantálja, hogy kirendeltségek illetékességi területén bárhol el lehessen őket helyezni. Működési hőtartományuk -25C - +50 C, melynek következtében az eszközök egész évben alkalmazhatók, nem szükséges őket felszedni. Élettartamuk hosszú, elemcsere nélkül elérheti akár a 3 hónapot is. Emellett különleges tulajdonságuk még, hogy képesek nemcsak a hiba, de a szabotázs jelzésére is.

Bizonyítottan kiemelkedő hatékonyságú többek közt a Biharkesztes Határrendészeti Kirendeltség által is évek óta használt stabil hőkamera [9]. Legnagyobb előnye, hogy nem von el nagy létszámú állományt a szolgálati feladatok végrehajtásától, mivel elegendő egyetlen személy, aki folyamatosan felügyeli az eszköz által sugárzott felvételt, és illegális határsértés észlelése esetén a legrövidebb időn belül képes mozgósítani a járőrállományt a technika által pontosan beazonosítható területre. Kezeléséhez nincs szükség különösebb szakmai felkészítésre, a vezérlőegység használata egyszerű, önállóan is képes a környező terület folyamatos pásztázására. A lépésérzékelőhöz hasonlóan magas hőtűrő képességgel rendelkezik, és igen nagy területeket is képes felügyelet alatt tartani.

Hasonlóan előnyösnek tekinthető a Barabás Határrendészeti Kirendeltség illetékességi területén felszerelt mozgásérzékelő rendszer. A rendszer pozitív tulajdonságai tekintetében (hőtűrőképesség, hatótávolsága) megegyezik a stabil hőkamerával, azzal az eltéréssel, hogy ehhez az eszközhöz külön kezelőszemélyzet sem szükséges, mivel a vevő berendezés az ügyeleti helyiségben kerül elhelyezésre, ezáltal képes az állomány rögtön reagálni a jelzésre.

Ártánd Közúti Határátkelőhelyen már évek óta eredményesen működött a Vám- és Pénzügyőrség által felállított röntgen kapu, amelynek alkalmazását azóta mellőznünk kell, amióta a szervezet levonult a határátkelőhelyről (2010. április hónap elején egyez-

tetések történtek az újbóli alkalmazásra). 2009. szeptemberben elfogott 37 fő vietnámi személy felfedését is ennek az eszköznek köszönhettük. Az eljárás egyszerű, gyors, és kétség kívül képes kiszűrni a kamionok bármely részében megbújt személyeket. Az eszköz kezeléséhez elegendő egy, megfelelő módon felkészített személy, aki feltalálás esetén értesíti a kutató járőröket.

Másrészről ezeknek a járműveknek az ellenőrzése más módon meg sem oldható, főleg nem ilyen eredményességgel, hiszen egy látszólag telepakolt kamiont nem lehet minden alkalommal kipakoltatni.

Másik, hasonlóan maximális eredményességgel alkalmazható eszköz lenne a román határrendőrség által a közeljövőben beszerezni, illetve telepíteni kívánt szívhang detektor. Elsődlegesen azokon a közúti határátkelőhelyeken jelentene lépéselőnyt az embercsempészekkel szemben, ahol van teherforgalom. A technika beszerzése ugyan költséges, de a röntgen kapuval megegyező hatékonyságú berendezés. Ez a leghatékonyabb eszköz, amellyel meg lehetne akadályozni, hogy a megbújt illegális határsértőket a rendszer bárhol megtalálja.

A fent felsorolt technikai eszközökön felül meg kell említeni még egy olyan szerkezetet, melynek alkalmazása az illegális migráció kezelése szempontjából gyökeres változást eredményezne. A Magyar Honvédség által már beszerzett izraeli gyártmányú pilóta nélküli robotrepülőgépek alkalmazása merőben más oldalról közelítené meg a zöldhatár őrizetét. Lehetségessé válna, hogy olyan területeket tartsunk felügyelet alatt akár nappal, akár éjszaka, melynek észrevétlen megközelítése a jelen helyzetben körülményes, vagy teljességgel kizárt. Átláthatóvá válna a kukoricatábla és a zárt erdő egyaránt.



Skylark I

Műszaki adatok	
Funkció	Pilóta nélküli repülőgép
Gyártó	Elbit
Méretek	
Hossz	2,20 m
Fesztáv	2,40 m
Tömegadatok	
Maximális felszállótömeg	5,5 kg
Repülési jellemzők	
Utazósebesség	20-40 csomó
Hatótávolság	5-10 km
Repülési időtartam	2 óra

A robotrepülő előnye, hogy viszonylag kicsi, bizonyos magasságban szinte teljesen zajtalan, alkalmazásához egy, a berendezés kezeléséhez, és karbantartásához értő személy szükséges. Az eszköz kamerával, hőkamerával felszerelt, ezért képes pontos képet közvetíteni az ellenőrzést felügyelő határrendész számára.

Véleményünk szerint ezek a technikai eszközök hasznosságuk, és hatékony alkalmazhatóságuk következtében képesek a Nyugat-Európára háruló illegális migráció elleni fellépést eredményesen segíteni.

ÚJ SZEMPONTOK AZ ÁLLOMÁNY KIVÁLASZTÁSA, ILLETVE PSZICHIKAI FELKÉSZÍTÉSE SORÁN

Az előző fejezetekben bemutatott technikai vívmányok eredményes alkalmazásához az is szükséges, hogy a technikát kézben tartó állomány megfelelő fizikai és pszichikai állapotban legyen a bevetések és akciók során, így képes legyen a működtetéshez szükséges ismeretek elsajátítására és a megszerzett tudást, illetve készségeket éles helyzetben vagy akár exrém körülmények között is képes legyen alkalmazni.

A folyamatos fejlődés alapvető feltétele, hogy a rendőrség határrendészeti feladatokat ellátó állományába csak az arra alkalmas kollegák kerüljenek felvételre, valamint hogy alkalmasságukat, aktuális mentálhigiénés állapotukat folyamatosan figyelemmel kísérjék, hiszen feladataik sok esetben megkövetelik a különleges körülmények (bizonytalanság, fokozott pszichikai és fizikai igénybevétel, szélsőséges időjárási viszonyok, fizikai veszélyeztetettség stb.) közötti hatékony munkavégzést. Ezt biztosítandó kerültek bevezetésre a hivatásos állományba kerülést megelőző ún. előzetes, valamint a szolgálat ideje alatt rendszeres időközönként megismétlődő ún. időszakos egészségügyi, pszichikai és fizikai alkalmassági vizsgálatok, melyeket a 21/2000. (VIII.23.) BM-IM-TNM együttes rendelet [10] szabályoz. A vizsgálatok orvos-egészségügyi vizsgálatokat, fizikai állapotfelmérést, valamint általános pszichikai funkciók vizsgálatát (többek között személyiségvizsgálat, szenzomotoros teljesítmény, percepciós teljesítmény) foglalják magukban, de nem terjednek ki kellő mértékben pl. a terhelhetőség, ezen belül is a coping funkciók specializált vizsgálatára, a burnout-veszélyeztetettség fizikai és pszichés előjeleinek mérésére, holott ezek a mutatók sok esetben megmutathatják, előrejelezhetik a teljesítményromlást. A munkakörrel járó stresszhatások – eredményes megküzdési technikák hiányában – hosszú távon mind a pszichés, mind a fizikai állapotra (és ezen keresztül a munkavégzés színvonalára is) hatással lehetnek. Hazai vizsgálatok is alátámasztják, hogy szubkrónikus fizikai és pszichés stressz hatására romlik az információtárolási és felidézési képesség, csökken az automatizmus szintjéig begyakorolt, komplex szenzomotoros működésekben nyújtott teljesítmény színvonala és megváltoznak olyan a feladatvégrehajtás és a teljesítmény szempontjából fontos mentális tényezők, mint a hangulati beállítódás, érzelmi stabilitás [11]. A stresszterhelés kumulálódása fokozódó mértékben rontja a stresszhelyzetekben adandó korrekt, szakmai alapú viselkedéses válaszokat és növeli az érzelmi, indulati és hangulati tényezők érvényesülésének lehetőségét, melynek következménye a hibás intézkedések, illetve feladat-végrehajtás lehet. Mindennek azonban vannak fizikai és pszichés előjelei, amelyek a megfelelő vizsgálatokkal (pl.: a stresszkezelést és az eredményes megküzdést működtető személyiségforrások detektálása, az elégtelen pszichikai működések időbeni felismerése) a rendszeres szűrések során tetten érhetőek. Ez kiemelt szempont lehet egy olyan rendszerben, ahol folyamatos létszámhiánnyal küzdünk és a – bármilyen ok miatt – kieső, szakképzett, tapasztalt kollégák pótlása nagyon nehézkes és időigényes.

Fenti okok miatt célszerűnek tartjuk a határrendészeti szolgálatot ellátó állomány éves, rendszeres fizikai és pszichikai állapotfelmérésébe illeszthető elemek segítségével a coping-mechanizmusokat maladaptiv módon alkalmazó, illetve a burnout-által veszélyeztetett kollégák kiszűrését, akiknek ezáltal lehetőségük lesz arra, hogy még a tünetek elmélyülése előtt becsatlakozzanak a megfelelő prevenciós és rekreációs programokba.

ÖSSZEGZÉS

Összességében megállapítható, és a legtöbb nemzetközi szervezet szakértője szinte egyhangúan úgy vélekedik, hogy jelenleg a biztonság fejlesztése még prioritást élvez a szabadság fenntartásához viszonyítva, továbbá megállapítható, hogy hazánk geopolitikai helyzetéből és a terrorellenes küzdelemben végzett tevékenységéből adódóan a bevezetett intézkedések fontosak, eredményesek voltak, ugyanakkor továbbfejlesztésük szükséges. Láthatjuk, hogy az új határbiztonsági rendszer dimenziói messze túlmutatnak a magyar határokon. Alakításához és működtetéséhez külpolitikai támogatásra is szükség van. A külpolitika szerepe elsősorban a feltételteremtésben előnyt kínáló és nyomást gyakorló eszközökkel valósul meg. Korábbi tradicionális külügyi területek, mint a vízumkiadás, a határbiztonsági rendszer fő elemét képezik.

Magyarország a keleti migrációs útvonalak kereszteződésében, Ukrajna és a Balkán kapujában elhelyezkedve fontos szerepet kapott az EU határbiztonsági rendszerében. Schengeni tagságunkkal a veszélyek nem csökkentek, sőt a belső határok lebontása miatt — a keletkező biztonsági deficit csökkentésére — a határbiztonsági rendszert gyökeresen át kellett alakítani. A jövő határbiztonsága az összetett kihívások (terrorizmus, áru- és ember- csempészet, migráció-közbiztonság, korlátozott anyagi források) miatt integrált szemléletű határigazgatási rendszer kialakítását teszi szükségessé. A feladat hazánk számára külső-belső biztonságot, politikai tekintélyt növelő tényező, az Unió számára a jövőbeni bővítési térség koordinált kezelésének lehetősége. Az állandósult kihívásokra, amikor a forráshiány is egy természetes jelenség, a válasz a jövőbemutató stratégiai fejlesztések, együttműködések a kormányzati és rendvédelmi szervek között országon belül és országhatárokon kívül.

A tanulmányban leírtak bizonyítják, hogy országunk az EU integrált határigazgatási rendszerében a határőrizet, a határforgalom-ellenőrzés, a vámigazgatás és az összehangolt migrációs hálót alkotó mélységi ellenőrzés feladataival jelentős részt képvisel. Mondanivalónk rávilágít arra is, hogy a hagyományos határrendészeti tevékenységért felelős szervezet (2008. január 1-je óta az integrált rendőri szervezet) mellett a különböző társszervek is fontos szerepet játszanak a jelen határigazgatási rendszerében.

FELHASZNÁLT IRODALOM

[1] Horváth László: Változások a védelmi igazgatás területén. Nemzetvédelmi egyetemi közlemények. 9. évfolyam 2. szám 2005. pp. 137-162., Zrínyi Miklós Nemzetvédelmi Egyetem. Forrás: http://193.224.76.4/download/konyvtar/digitgy/nek/2005_2/07_horvath.pdf (Letöltve: 2010. április 8.)

[2] Az Európai Parlament és a Tanács 2007/574/EK határozata (2007. május 23.) a „Szolidaritás és a migrációs áramlások igazgatása” általános program keretében a 2007–2013-as időszakra a Külső Határok Alap létrehozásáról. Brüsszel, 2005. 04. 06. Forrás: http://eur-lex.europa.eu (Letöltés dátuma: 2010. április 8.)

[3] A Magyar Köztársaság nemzeti biztonsági stratégiájáról szóló 2073/2004. (III. 31.) Korm. határozat. Forrás: http://www.mfa.gov.hu/NR/rdonlyres/0AA54AD7-0954-4770-A092-F4C5A05CB54A/0/bizt_pol_hu.pdf (Letöltés dátuma: 2010. április 8.)

[4] A Cseh Köztársaság, Észtország, Ciprus, Lettország, Litvánia, Magyarország, Málta, Lengyelország, Szlovénia és Szlovákia csatlakozási szerződése az Európai Unióhoz (2003) For-

rás: http://eur-lex.europa.eu/hu/treaties/dat/12003T/htm/12003T.html. (Letöltés dátuma: 2010. április 8.)

[5] Zámbó Péter: A Magyar Köztársaság Határőrségének megváltozott szerepe az Európai Unió bővítésének tükrében. „Globális biztonsági kihívások – közép-európai szerepvállalások". Nemzetközi társadalomtudományi konferencia (előadás), Pécs 2006. április 25-26.

[6] Ávár Imre, Balda Róbert, Boros Béla, Hegedűs Norbert, Stelmach László: Az integrált vezetési központ az illegális migráció kezelésének nemzeti koordináló szerve. Határrendészeti tanulmányok, 2006. 3. különszám. Forrás: http://www.rtf.hu/01_szervezeti/hor_oktat/hor_tanulm/haret_2006_3_kulonszam.pdf (Letöltés dátuma: 2010. április 8.)

[7] Johan Erzsébet Schutzbach Mártonné: A Schengeni Információs Rendszer. Határrendészeti tanulmányok, 2005. 1. szám, pp. 4-9. Forrás: http://www.rtf.hu/01_szervezeti/hor_oktat/hor_tanulm/haret_2005_1.pdf (Letöltés dátuma: 2010. április 8.)

[8] Zsigovits László, Wengrin István: Az EU tagállamok közös rendvédelmi tevékenységének összehangolási lehetőségei a „CheckNet" végrehajtásában korszerű információtechnológia alkalmazásával. Határrendészeti tanulmányok, 2007. 2. szám, pp. 46-73. Forrás: http://193.224.76.4/download/konyvtar/digitgy/tartalomjegyz/hatarrend_tanulm_2007_2.pdf (Letöltés dátuma: 2010. április 8.)

[9] PAPP Csaba (2009): Stabil hőkamera rendszer kialakítása a zöldhatáron, Hadmérnök, **4**(2), pp. 417-429. Forrás: http://hadmernok.hu/2009_2_papp.pdf. (Letöltés dátuma: 2010. április 8.)

[10] 21/2000. (VIII. 23.) BM-IM-TNM együttes rendelet a fegyveres szervek hivatásos, közalkalmazotti és köztisztviselői állományának munkaköri egészségi, pszichikai és fizikai alkalmasságáról, a szolgálat-, illetve keresőképtelenség megállapításáról, valamint a belügyi egészségügyi szolgálat igénybevételéről. Forrás: http://www.brdsz.hu/data/nyugdijas/15.pdf. (Letöltés dátuma: 2010. április 8.)

[11] Hullám István (2005): Az extrém megterhelések mentális következményeinek multifaktoriális vizsgálata és elemzése: az eredmények alkalmazhatósága az alkalmasságot és beválást vizsgáló szakértői rendszerek fejlesztésében. Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem. Bolyai János Katonai Műszaki Kar, Katonai Műszaki Doktori Iskola. Forrás: http://phd.okm.gov.hu/disszertaciok/tezisek/2005/tz_eredeti2438.pdf. (Letöltés dátuma: 2010. április 8.)

HADMÉRNÖK
V. Évfolyam 2. szám - 2010. június

Munk Sándor
munk.sandor@zmne.hu

A BIZTONSÁG KÉRDÉSEINEK DEKOMPOZÍCIÓJA

Absztrakt

Napjainkban szinte minden alkalmazási területen általánosan elfogadottá vált a biztonság komplex megközelítésének igénye, a fenyegetések és a védelmi megoldások, intézkedések jellegüktől független, teljes körű vizsgálata. A komplex megközelítés szempontjából elvileg felmerülhet a speciális biztonsági szakterületek feleslegessége, vagy jelentőségük csökkenése, amit azonban a gyakorlati tapasztalatok nem igazolnak. A komplex megközelítésre épülő módszertanok és a részterületi dokumentumok, módszerek általában nem kapcsolódnak egymáshoz. Jelen publikáció célul tűzte ki a biztonság komplex megközelítéséhez kapcsolódó kérdések szakterületekre történő lebontása alapjainak vizsgálatát. Ennek érdekében: összegzi az összetett objektumok biztonságának alapvető kérdéseit; elemzi a biztonság kérdései dekompozíciójának alapjait; végül részletesebben vizsgálja a fenyegetések, sebezhetőségek, illetve a védelmi intézkedések dekompozíciójának lehetőségeit, szükségességét.

In our days complex approach of security, comprehensive analysis of threats and security controls, independent of their nature, became generally accepted on almost every application areas. From the point of view of the complex approach it would be possible that specialized security areas may become unnecessary, and their importance may decrease, but this is not justified by practical experiences. Complex approach based methodologies, and component area documents, methods usually not related. Recent publication aims at studying the basics of breakdown of questions related to complex approach of security into specialized security areas. For this purpose: summarizes the basics questions of security of complex objects; analyses the basics of security questions' decomposition; finally in greater detail examines possibilities, and necessity of decomposition of threats, vulnerabilities, and security controls.

***Kulcsszavak**: biztonság, informatikai biztonság, kockázatmenedzsment, sebezhetőség, dekompozíció ~ security, information (IT) security, risk management, vulnerability, decomposition*

BEVEZETÉS

Napjainkra a biztonság értelmezése gyakorlatilag minden alkalmazási területen – legyen az a politika, a kritikus infrastruktúrák, a katonai/védelmi szféra, a környezetvédelem, a gazdaság, vagy az informatikai rendszerek világa – a komplex megközelítések irányába mozdult el. A komplex megközelítés lényege leegyszerűsítve: jellegüktől függetlenül a biztonság alanyára ható valamennyi fenyegetés feltárása és a védelem összes lehetséges megoldásának, intézkedésének számbavétele, felhasználása.

A komplex megközelítés igényéhez, megjelenéséhez kapcsolódóan felvetődhet a kérdés, hogy vajon következik-e ebből a speciális – pld. szakterületi – biztonsági megközelítések feleslegessé válása, megszűnése, vagy jelentőségük csökkenése. Ez a következtetés előzetesen úgy tűnik, hogy sem logikai úton, sem gyakorlati tapasztalatok alapján nem igazolható. Az átfogó biztonság elvének elfogadása nem vonja maga után a katonai biztonság, a gazdasági biztonság, vagy a környezetbiztonság megszűnését és a komplex informatikai biztonság uralkodóvá válása sem teszi szükségtelenné, idejétmúlttá az olyan szakterületeket, mint a hálózati biztonság, az adatbázis-biztonság, a fizikai biztonság, vagy a humán biztonság.

A biztonság részterületeinek változatlan létjogosultságát, szükségességét elfogadva szükségesnek látszik megvizsgálni összefüggésrendszerüket, helyüket és szerepüket a komplex megközelítésű biztonsági elképzelésekben, módszertanokban. Ezt indokolja az is, hogy napjaink nemzetközi szabványaiban és legjobb gyakorlatokat rögzítő dokumentumaiban leírt komplex módszertanok többnyire csak átfogó jellegű feladatokat fogalmaznak meg, míg a részterületi dokumentumok és módszertanok mindmáig nem, vagy csak érintőlegesen foglalkoznak az átfogó keretekkel.

Mindezek alapján jelen publikáció célja a biztonság komplex megközelítéséhez kapcsolódó kérdések biztonsági szakterületekre történő lebontása, dekompozíciója és kapcsolatrendszerük alapjainak vizsgálata. Ennek érdekében:

- összegzi a biztonság összetett jellegének, az összetett objektumok biztonságának alapvető kérdéseit;
- elemzi a biztonság alanya és védendő tulajdonságai dekompozíciójának alapjait;
- végül részletesebben vizsgálja a fenyegetések, sebezhetőségek, illetve a védelmi intézkedések dekompozíciójának lehetőségeit, szükségességét és rendjét.

A BIZTONSÁG ÉS ÖSSZETETTSÉGÉNEK ALAPJAI

A biztonság és egyes összetevői értelmezésének, számos más fogalomhoz hasonlóan – a közös jellemzők ellenére – nincs általánosan elfogadott változata. Ennek megfelelően a következőkben először összegezzük a publikációban felhasználásra kerülő alapvető értelmezéseket, megállapításokat, majd áttekintjük a biztonság összetett jellegének, az összetett objektumok biztonságának alapvető kérdéseit.

A továbbiakban a következő ***alapvető értelmezések*** kerülnek felhasználásra [részletesebben lásd 1]. A biztonság – általános értelemben – egy olyan állapot, amelyben valaki/valami a lehetséges fenyegető hatások ellen a kívánt mértékben védett, a védelem pedig a fenyegetések elleni, a biztonság megteremtésére és fenntartására irányuló tevékenységek, rendszabályok összessége.

A biztonság alapfogalma a biztonság alanya, a fenyegetések által veszélyeztetett objektum. A publikációban foglaltak törekszenek egy olyan általános megközelítésre, amelynek megállapításai, eredményei a biztonság kérdéseinek bármely alkalmazási területén, tetszőleges veszélyeztetett objektum esetében alkalmazhatóak, ezen belül azonban kiemelten figyelmet fordítanak az informatikai rendszerekre, mint a biztonság alanyára.

Ennek során informatikai rendszer alatt – a tágabb értelmezésnek megfelelően – eszközök, programok, adatok, valamint a működtető személyzet információs funkciók, tevékenységek megvalósítására létrehozott rendszerét értjük. [2, 21. o.] Ez a meghatározás magában foglalja a szűkebb értelemben vett számítógépes, kommunikációs (távközlési, híradó), navigációs, információszerző (felderítő, szenzor-), vezetéstámogató, folyamatirányító, stb. rendszereket, valamint az ezek integrációjára, összeolvadására épülő, a különböző szakmai közösségekben infokommunikációs, információtechnológiai, vagy IT jelzőkkel megnevezett technikai rendszereket.

A biztonság értelmezéséhez hozzátartoznak a biztonság összetevői (aspektusai), a biztonság alanyának azon tulajdonságai, amelyeknek a megengedett mértéktől eltérő megváltozása a biztonság sérülését, megsértését jelenti. A szakirodalomban ezek általában biztonsági célkitűzések[1] megnevezéssel szerepelnek [lásd pld. 3, 7. o.; 4, E-2. o.]. Az informatikai rendszerekhez és az általuk kezelt információkhoz kapcsolódóan ezek közé elsősorban a bizalmasságot, a sértetlenséget és a rendelkezésre állást, továbbá a hitelességet, letagadhatatlanságot, számonkérhetőséget, stb. sorolják.[2]

A biztonság alapvető fogalmai közé tartoznak még a fenyegetések, a biztonság alanyát veszélyeztető, a védendő tulajdonságokat károsan, a meg nem engedett/elfogadható mértéknél jobban befolyásoló potenciálisan káros [kölcsön]hatások. A sebezhetőségek a biztonság alanyának – illetve tágabb értelemben a biztonság fenntartására irányuló tevékenység- és eszközrendszernek – olyan tulajdonságai (biztonsági szempontból hiányosságai, gyengeségei), amelyek lehetőséget teremtenek a fenyegetést megvalósító kölcsönhatások érvényesülésére. Végül a veszélyforrások azok az objektumok, amelyek a biztonság alanyát veszélyeztető hatást közvetlenül, vagy közvetve (áttételesen) kiváltják, vagy a veszélyeztető kölcsönhatásokban érintettek.[3]

Egy adott objektum vonatkozásában joggal állítható, hogy ***a biztonság összetett fogalom***. Összetett egyrészt abból a szempontból, hogy az objektum biztonsága különböző megőrzendő tulajdonságokkal írható le, illetve a biztonságot különböző jellegű, sokszor egymástól teljesen független fenyegetések veszélyeztetik. Ezek egymással sok esetben szoros kapcsolatban állnak, meghatározott védendő tulajdonságokat meghatározott fenyegetések veszélyeztetnek.

Egy nemzet, egy állam biztonságát különböző fenyegetések, kockázatok és kihívások veszélyeztetik. A Magyar Köztársaság Nemzeti Katonai Stratégiája szerint "A Magyar Köztársaság kormánya a biztonságot átfogó módon értelmezi, amely a politikai és katonai tényezőkön túl magában foglalja annak gazdasági, pénzügyi, energiaellátási, rendvédelmi, emberi jogi és kisebbségi, információs és technológiai, környezeti, demográfiai és civilizációs, közegészségügyi, valamint nemzetközi jogi dimenzióit is.". [5, 6. o.] Hasonlóképpen különböző fenyegetések veszélyeztetnek kritikus infrastruktúrákat, kritikus információs infrastruktúrákat,

[1] Security objective, security goal.
[2] Confidentiality, integrity, availability, authenticity, non-repudiation, accountability.
[3] Threat, vulnerability, threat source.

illetve informatikai rendszereket is. A fenyegetések érkezhetnek a természeti, a technikai és az információs környezetből, hatásmechanizmusukat illetően lehetnek fizikai, információs, vagy pszichológiai jellegűek.

A fentiek alapján a komplex biztonság felbontható különböző részterületekre, amelyek egy meghatározott védendő tulajdonságra, vagy ezek összetartozó körére, illetve az ezeket veszélyeztető fenyegetésekre összpontosítanak, korlátozódnak. Ennek megfelelően beszélhetünk a bevezetőben már említett katonai biztonságról, gazdasági biztonságról, környezeti biztonságról, stb., vagy hálózati biztonságról, adatbiztonságról, fizikai biztonságról, humán biztonságról. A biztonság részterületekre bontásához kapcsolódóan azonban nyilvánvaló, hogy a komplex biztonság nem egyszerűen az egyes részterületek szummatív összegzése, egyre jelentősebb szerepet játszik a közöttük fennálló összefüggésrendszer: az egymásra épülés, a kölcsönös függőség (az interdependencia) kérdésköre, ami napjaink egyik jelentős vizsgálati területe.

A biztonság összetettnek tekinthető abból a szempontból is, hogy az objektumok általában maguk is összetettek, így a teljes objektum biztonsága többek között összetevői biztonságára épül. Az objektum adott követelményekkel meghatározott biztonságához szükség van arra, hogy az egyes összetevői is megfeleljenek meghatározott – az átfogó követelményekből levezethető – biztonsági követelményeknek. Emellett persze egy adott objektum biztonsága függhet olyan más – általa felhasznált, vagy vele együttműködő – objektumok biztonságától is, amelyek nem képezik részét, amelyek felett nincs rendelkezési joga. Összetett objektumok esetében a biztonsághoz kapcsolódó elemek (fenyegetések, sebezhetőségek, védelmi tevékenységek) nem kezelhetőek kizárólag az adott objektum szintjén, elemzésük, megvalósításuk végeredményben csak a konkrét összetevőkre lebontva, illetve ezekből összeállítva lehetséges.

A biztonság vizsgálatának, kialakításának és fenntartásának alapvető eszköze a ***kockázat-menedzsment***. A kockázat-menedzsment alapfogalma – a szintén különböző módokon értelmezett – kockázat. Ehhez kapcsolódóan a következőkben a jövőbeni esemény következményeihez rendelt érték-központú megközelítést használjuk, amelynek megfelelően a kockázat egy adott sebezhetőséget kihasználó fenyegetés bekövetkezésének valószínűségére, illetve az ennek következtében jelentkező biztonságsértés "értékére" (súlyosságára, kár-mértékére) épül. A kockázat-menedzsment alapvető összetevőinek a kockázat-értékelést és a kockázat-kezelést[4] tekintjük.

A biztonság kérdéseinek dekompozíciója alatt egy összetett objektum biztonsági kérdéseinek összetevői biztonsági kérdéseire történő lebontását, illetve az ezek között fennálló összefüggések meghatározását értjük. Ezen belül viszonylag önállóan vizsgálható a biztonság alanyának és a védendő tulajdonságoknak, a sebezhetőségeknek és a fenyegetéseknek, valamint a védelmi intézkedéseknek a dekompozíciója.

A BIZTONSÁG ALANYÁNAK ÉS VÉDENDŐ TULAJDONSÁGAINAK DEKOMPOZÍCIÓJA

A ***biztonság alanyának összetevőkre bontása*** általánosságban különböző kritériumoknak megfelelően is lehetséges. Ilyenek lehetnek többek között: a funkcionális kritériumok; a ren-

[4] Risk assessment, risk mitigation

delkezési jog, működtetési felelősség kritériumai; a térbeli (földrajzi) kritériumok; esetleg műszaki-technikai kritériumok. Bármelyik felbontás esetén meg lehet, meg kell határozni az adott objektum összetevőinek körét és ezek egymás közötti – a vizsgálat szempontjából érdeklődésre számot tartó – kapcsolatrendszerét. A felbontás során olyan összetevőket célszerű meghatározni, amelyek biztonsági szempontból viszonylagosan "homogének": hasonló fenyegetettségeknek vannak kitéve, hasonló sebezhetőségekkel rendelkez(het)nek, hasonló védelmi tevékenységeket, intézkedéseket igényelnek.

Informatikai rendszerek, hálózatok biztonsági szempontból történő részekre tagolása a gyakorlatban általában két szempont alapján történik. Magasabb szinten a részekre tagolás alapja az azonos helyszín és az azonos informatikai biztonsági politika, amely szerint egy összetett informatikai rendszer, biztonsági tartományokra, úgynevezett enklávékra bomlik. Az enklávé "(helyi informatikai környezet) a teljes fizikai és szervezeti környezet, beleértve a végberendezéseket és kommunikációs rendszereket (kapcsoló eszközöket), amelyek egyetlen felelős irányítása és egy közös, egységes biztonsági politika hatálya alatt állnak." [6, 4. o.]

Az egyes tartományok további összetevőkre bontása az informatikai rendszerek általános technikai architektúrális elveinek megfelelően történhet. Ennek megfelelően a felbontás első szinten hálózati infrastruktúrára és a végberendezésekre, ez utóbbiak esetében pedig kiszolgáló eszközökre és munkaállomásokra lehetséges. A végberendezések esetében további felbontás lehetséges hardver platformra, szoftver platformra (operációs rendszerre és környezetére), alkalmazói rendszerekre (szoftverekre), valamint adatbázisokra.

A ***biztonság összetevői, a védendő tulajdonságok dekompozíciója*** az összetett objektum, valamint összetevői megőrzendő, védendő tulajdonságainak és az ezek között fennálló kapcsolatrendszer meghatározását jelenti. Ennek során először azt kell meghatározni, hogy az összetevők mely tulajdonságainak megléte szükséges ahhoz, hogy az összetett objektum védendő tulajdonságai a kívánt mértékben fenntarthatóak legyenek. Ugyanez ellenkező oldalról megközelítve azt vizsgálja, hogy az összetevők mely tulajdonságainak, milyen mértékű megsértése eredményezi az összetett objektum megőrzendő tulajdonságának sérülését. Informatikai rendszerek esetében például feltehető az a kérdés, hogy a rendszer rendelkezésre állásának meglétéhez az egyes összetevők – hálózati infrastruktúra, hardver összetevők, alapszoftver platform, alkalmazói szoftverek, adatbázisok, működtető állomány, elhelyezési környezet, stb. – milyen tulajdonságainak fennállása szükséges.

A védendő tulajdonságok dekompozíciója elméletileg lehet homogén és heterogén. Homogén esetben az összetett objektum adott tulajdonsága kizárólag az összetevők azonos, vagy lényegében azonos tulajdonságai fennállásának függvénye. Ez a függőség kiterjedhet valamennyi összetevőre, vagy csak azok egy részére. Ez utóbbi esetben az összetevők között megkülönböztethetőek a tulajdonság szempontjából 'lényegesek' ('kritikusak') és 'lényegtelenek'. Heterogén összefüggés esetében az összetett objektum adott tulajdonsága az összetevők azonos tulajdonságai mellett más tulajdonságaiknak is függvénye. Informatikai rendszerek esetében példa lehet erre egy rendszer sértetlensége, amely egy összetevő bizalmasságának (csak jogosultak számára történő elérhetőségének) megsértése esetén veszélyeztetetté válik.

Mivel a védendő tulajdonságok szorosan kapcsolódnak az adott objektummal szemben támasztott biztonsági követelményekhez (amelyek lényegében bizonyos tulajdonságok fennállását, vagy ezen tulajdonságok meghatározott értéktartományba esését írják elő), a védendő tulajdonságok dekompozíciója a gyakorlatban az egyes összetevőkkel szemben támasztott biztonsági követelmények és az ezekben szereplő tulajdonságok meghatározását, 'levezetését'

jelentik. Az összetett objektum és az összetevők védendő tulajdonságai közötti kapcsolat nem mindig, sőt sok esetben nem közvetlen. Ebből következően az összetevők védendő tulajdonságainak meghatározása is egy iteratív, az összetevők közötti kapcsolatokat is figyelembe vevő folyamat kell legyen, amely már átvezet a sebezhetőségek, fenyegetések következő pontban tárgyalt kérdéséhez.

A védendő tulajdonságok dekompozíciója ezen tulajdonságok meglétének – a biztonsági követelmények érvényesülésének – megítélése, vagyis ***biztonsági ellenőrzések, értékelések*** során is lényeges lehet. Általánosságban megállapítható, hogy összetett objektumok esetében számos, biztonsági szempontból lényeges tulajdonság nem önmagában, hanem összetevői tulajdonságain keresztül mérhető, ítélhető meg. Egy objektum sértetlensége például nem értelmezhető, nem vizsgálható összetevői sértetlensége nélkül. De természetesen vannak olyan, elsősorban az adott objektum működéséhez, az általa nyújtott szolgáltatásokhoz kapcsolódó tulajdonságok is, amelyek megléte, értéke, vagy szintje az objektumot 'fekete doboznak' tekintve is megállapítható.

Az ellenőrzéshez, értékeléshez kapcsolódó kérdéskör annak meghatározása is, hogy egy összetett objektum valamely, biztonsági szempontból lényeges tulajdonságát (pld. sértetlenségét, rendelkezésre állását, stb.) mérhető, megítélhető módon milyen feltételek mellett tekintjük fennállónak, illetve milyen módon határozhatjuk meg fennállásának mértékét. Egy objektum sértetlensége például fennállhat úgy is, hogy – időlegesen – vannak sérülést szenvedett összetevői és szolgáltatásai rendelkezésre állhatnak úgy is, hogy egyes összetevői nem állnak rendelkezésre.

Az előzőekben elmondottak konkrétan is megjelennek az összetett termékek, illetve a rendszerek értékelési rendjét leíró magyar kormányzati dokumentumokban is. "Összetett termék … értékelése esetén is követelmény, hogy az egyedi komponenseket függetlenül értékeljék, mivel az összeállítás értékelése az egyedi komponens értékelések eredményeire alapoz." [7, 14 o.] "A rendszer szintű értékelés jelentős mértékben támaszkodik a rendszer komponenseire (termékekre és összetett termékekre) korábban már elvégzett értékelések eredményeire." [8, 9 o.] "A több funkciós rendszerek különböző alrendszereire eltérő biztonsági szabályzatok vonatkozhatnak. Egy ilyen rendszer ugyanazon biztonsági szabályzat alá eső részeit biztonsági tartománynak is nevezik. Minden biztonsági tartományra külön megadhatók a funkcionális és garanciális követelmények, így minden tartomány rendelkezni fog egy saját biztonsági szabályzattal, biztonsági probléma meghatározással, biztonsági célokkal, követelményekkel és specifikációkkal. Minden tartomány egyúttal a nagyobb rendszer általános szabályai, biztonsági problémái, céljai, követelményei és specifikációi körén belül működik." [8, 20 o.]

Összességében megállapítható, hogy a biztonság alanya, ezen belül például egy kritikus információs infrastruktúra, vagy egy informatikai rendszer különböző – sajátos alkalmazási, funkcionális, technikai és biztonsági jellemzőkkel rendelkező – összetevőkre, alrendszerekre tagolható. Összetett rendszerek biztonságának összetevői, megőrzendő tulajdonságai – mint követelmények – meghatározó szerepet játszanak összetevőik megőrzendő tulajdonságainak meghatározása során. Biztonsági ellenőrzések, értékelések során egy összetett rendszer biztonsága többnyire – bár nem kizárólagosan – összetevői biztonságának, megőrzendő tulajdonságai meglétének értékelésén keresztül mérhető, ítélhető meg. A biztonsági ellenőrzések, értékelések egy, jellemzően kisebb része megvalósítható globális módon, az összetett rendszert "fekete doboz"-nak tekintve, azonban nagyobb részt az egyes összetevőkhöz kapcsolódó biztonsági ellenőrzésekre, értékelésekre épülnek.

A SEBEZHETŐSÉGEK, FENYEGETÉSEK DEKOMPOZÍCIÓJA

A ***sebezhetőségek dekompozíciója*** az összetett objektum sebezhetőségeinek, illetve összetevői sebezhetőségeinek, valamint a közöttük fennálló kapcsolatrendszernek a meghatározását jelenti. Összetett objektumok, például informatikai rendszerek esetében a sebezhetőségek jelentős része lebontható egyes összetevők sebezhetőségeire, vagyis olyan tulajdonságokra (hiányosságokra, gyengeségekre), amelyek már kizárólag egyetlen összetevőhöz, alkotóelemhez kapcsolódnak. A sebezhetőségek egy másik – általában kisebb – része nem, vagy nem teljes egészében vezethető vissza összetevő szintű sebezhetőségekre, hanem az összetett objektum egészéhez, vagy annak felépítéséhez kapcsolódik.

Egy adott objektum sebezhetőségeinek feltárása, számbavétele háromféleképpen is lehetséges. Az első – amennyiben ilyen létezik – az adott objektumtípus nyilvánosságra került potenciális sebezhetőségeinek elemzése és annak meghatározása, hogy a közreadott sebezhetőség az adott objektumban fennáll-e, vagy sem. A második az adott objektum tervszerű, biztonsági szempontú vizsgálata a védendő tulajdonságok (biztonsági célok) potenciális megsértésére vezető hiányosságok, gyengeségek keresésére. Végül a harmadik – és legkevésbé kívánt – lehetőség a sebezhetőségek bekövetkező biztonságsértéshez kapcsolódó felfedezése. Ez utóbbiak általában ezt követően be is kerülnek a nyilvános sebezhetőség listákba.

A gyakorlatban közreadott, rendszerezett ***sebezhetőség katalógusok*** az informatikai eszközök és rendszerek, ezen belül is elsősorban a szoftverek területén léteznek. Ide tartozik mindenekelőtt a MITRE cég által kezelt Közös Sebezhetőségek Listája (CVE)[5], amely egy korai célkitűzés [9] szerint: "egy szabványosított lista, amely:

- számba veszi és megkülönbözteti az összes ismert sebezhetőséget;
- minden sebezhetőséghez hozzárendel egy szabványos, egyedi megnevezést;
- független a sebezhetőség különböző megközelítéseitől;
- és nyilvános, minden elosztási korlátozás nélkül hozzáférhető."

A lista 2010 elején több mint 40 ezer sebezhetőséget tartalmazott.

A Közös Sebezhetőségek Listájához szorosan kapcsolódik, a sebezhetőségek körében lényegében azzal megegyezik az Egyesült Államok Nemzeti Sebezhetőségi Adatbázisa[6], amely a sebezhetőség-kezelési adatok kormányzati szintű tárháza és amelyet a Belbiztonsági Minisztérium Cyber Biztonsági Osztályának támogatása mellett a Nemzeti Szabványügyi és Technológiai Intézet (NIST) Számítógép Biztonsági Osztálya[7] kezel.

A ***sebezhetőségek tervszerű elemzésre épülő feltárása*** célszerűen az összetett objektumok (pld. informatikai rendszerek, szoftver rendszerek) fejlesztéséhez kapcsolódó feladat, hiszen így a sebezhetőségek megfelelő védelmi megoldásokkal még a tervezés, illetve megvalósítás fázisában – tehát hatékonyabban és olcsóbban – kiküszöbölhetőek, csökkenthetőek, vagy megmaradásuk esetén számba vehetőek. A biztonságos rendszerek kialakítására az elméletben és gyakorlatban több módszer is megjelent, melyek közé tartoznak a biztonsági fenyegetések modellezésének sokban hasonló, de egyes jellemzőikben eltérő módszerei: a fenyegetés-fa

[5] Eredetileg Common Vulnerability Enumeration, ma Common Vulnerabilities and Exposures. Részletesebben lásd cve.mitre.org.
[6] National Vulnerability Database. Részletesebben lásd nvd.nist.gov.
[7] National Institute of Standards and Technology, Computer Security Division.

(támadás-fa) elemzések, valamint a hagyományos forgatókönyv módszerekre épülő negatív/támadási forgatókönyv módszerek[8]. [10, 11, 12, 13]

Az előzőekben említett módszerek közvetlenül nem a sebezhetőségek feltárására irányulnak, azonban eredményeik közé ez utóbbi is beletartozik. A feltárt fenyegetések és támadások esetében ugyanis meghatározható, hogy az adott fenyegetés/támadás ellen létezik-e védelmi intézkedés, megoldás, ekkor az objektum (rendszer) egészét tekintve az adott fenyegetéshez kapcsolódóan nincs sebezhetőség. Amennyiben azonban ilyen védelem nem létezik, lényegében az objektum általános, vagy konkrét sebezhetősége került feltárásra.

A ***fenyegetés-fa elemzés*** lényege a konkrét fenyegetések és részleteik fokozatos meghatározása. A módszer kiinduló pontja a fenyegetések lehető legáltalánosabb meghatározása, amely, vagy amelyek fenyegetés-fák gyökér-csomópontját alkotják. Ezek a – kezdetben absztrakt – fenyegetések kerülnek lebontásra az adott csúcshoz kapcsolódó további, konkrétabb fenyegetéseket reprezentáló csúcspontok formájában. A lebontás lehetséges változatai közé tartozhat: az adott objektum összetevői (egy rendszer alrendszerei), vagy a fenyegetések típusai[9] szerinti lebontás. A módszer hiányossága, hogy nehéz szabályokat, segítséget nyújtani a lebontás módjára és sok esetben nehéz biztosítani, ellenőrizni e lebontás teljességét, alaposságát. Ezen kívül a módszer nem nyújt segítséget új, vagy ismeretlen fenyegetések feltárására.

A ***támadás-fa elemzés*** lényege a biztonságot fenyegető támadási célokhoz vezető "utak" fokozatos meghatározása. A fa-szerkezetű modell gyökerében egy konkrét támadási cél áll, amely lépésenként kerül lebontásra támadási részcélokra, amíg konkrétan végrehajtható támadásokhoz nem jutunk. A részcélok egymással ÉS, vagy VAGY kapcsolatban állva vezetnek a lebontott cél eléréséhez. A támadási fa csúcspontjaihoz különböző értékek (pld. bekövetkezés/végrehajtás valószínűsége, a cél eléréséhez szükséges ráfordítás mértéke, stb.) is rendelhetőek és elemezhetőek. A módszer erőteljesen épít az előre elkészíthető, vagy korábbi elemzések során kidolgozott részfák, valamint az úgynevezett támadási sémák, minták[10] (újra)felhasználására.

A részcélok meghatározása, bár a fenyegetés-fa elemzéshez képest logikailag valamivel megalapozottabb, még mindig informális – intuíción, gyakorlati tapasztalatokon – nyugvó módszer. Összetett rendszerek esetében a támadási részcélokra történő lebontásnak szintén egyik alapvető lehetősége az összetevőket érő támadásokra, mint részfeladatokra bontás.

A ***negatív/támadási forgatókönyv módszerek*** a hagyományos forgatókönyv módszerek kiterjesztéseként, új célra történő felhasználási módjaként jelentek meg. A forgatókönyv módszerek lényege az adott objektum szolgáltatásai igénybevételének, működésének felhasználóközpontú folyamatszemléletű modellezése, a "hogyan kell a rendszernek működnie" leírása. A negatív/támadási forgatókönyv ezzel szemben, általában a hagyományos forgatókönyv lépéseihez kapcsolódóan, azt kiegészítve, a "hogyan lehet rosszindulatú tevékenységet megvalósítani" feladatok modellezése, leírása. A módszer eredménye az előzőekhez hasonlóan a sebezhetőségek és támadási lehetőségek feltárása, ennek alapján a védelmi megoldások, intézkedések megvalósítása.

[8] Threat tree modelling, attack tree modelling, use cases, misuse/abuse cases.
[9] Az eredeti megoldásban szereplő fenyegetés-típusok: a bizalmasságot, a sértetlenséget és a működőképességet érintő fenyegetések (disclosure, integrity, denial of service).
[10] Attack pattern.

A forgatókönyv-alapú módszerek során különböző megközelítésű és hatókörű, illetve részletezettségű megvalósítások lehetségesek. A megközelítés lehet alkalmazás-, vagy rendszer központú. Az előbbi tárgya a szervezet és a szervezeti folyamatokra összpontosít, az utóbbi tárgya pedig egy rendszer és a rendszer funkcióira összpontosít. A hatókör alapján készülhetnek forgatókönyvek egy szervezeti folyamat, vagy egy rendszer működésének egészére, illetve egyes részfolyamatokra, vagy alrendszerek működésére. Ez utóbbi gyakorlatilag részekre bontást és részletesebb kifejtést jelent, ami rendszerek esetében jellemzően alrendszerekre tagolást és azokhoz kapcsolódó részfunkciók leírását foglalja magában. [14, 9. o.]

Az ***informatikai rendszerek sebezhetőségeinek, támadásainak rendszerezése*** régóta vizsgált kutatási terület. A nyilvános sebezhetőség-adatbázisok, listák konkrét – elsősorban szoftver, de részben hardver – összetevők sebezhetőségeit tartalmazzák és nyilvánvaló, hogy ezek között hasonló jellegű, vagy meghatározott szempontok alapján egy kategóriába sorolható sebezhetőségek is vannak. Az egyes, több ezer elemet is tartalmazó sebezhetőség-listák könnyebb kezelhetőségének, a különböző listák közötti kapcsolat kialakításának igénye vezetett az úgynevezett sebezhetőség taxonómiák kialakítására, vizsgálatára. Ezek közül napjainkig számos javaslat látott napvilágot [lásd pld. 15, 16, 17, 18], de egységesen elfogadott taxonómia még nem alakult ki.

A javasolt taxonómiák között több olyan is van, amely egyik osztályozási szempontként az informatikai rendszerek összetevőit (mint a sebezhetőséget hordozó, a fenyegetés célpontját képező objektumokat) használja. Egy hálózati és számítógépes támadás taxonómia második szintű osztályozási szempontja például a támadás (elsődleges) célpontja, ami lehet:

- hardver összetevő, ezen belül számítógép, hálózati eszköz és periféria (majd ezek tovább bontva konkrétabb eszköztípusokra);
- szoftver összetevő, ezen belül operációs rendszer és alkalmazás (utóbbi tovább bontva kiszolgáló jellegű – pld. adatbázis-kezelő – és ügyfél-oldali szoftverekre);
- végül hálózati összetevő (ezen belül pld. protokollok). [17, 8-10. o.]

Egy másik taxonómia [18] egyik osztályozási szempontja szintén a támadás célpontja, ami lehet: az operációs rendszer, a hálózat, a helyi számítógép, a felhasználó maga, valamint az alkalmazás (ami lehet ügyfél-oldali, vagy kiszolgáló oldali alkalmazás).

Összességében megállapítható, hogy összetett objektumok, köztük az informatikai rendszerek sebezhetőségeinek jelentős része lebontható, visszavezethető egyes összetevőik sebezhetőségeire, vagyis olyan tulajdonságokra (hiányosságokra, gyengeségekre), amelyek már kizárólag egyetlen összetevőhöz, alkotóelemhez kapcsolódnak. Az összetett objektumok sebezhetőségeinek feltárására leggyakrabban használt módszerek (fenyegetés-fa elemzés, támadás-fa elemzés, negatív/támadási forgatókönyvek) alapvető jellemzője a fenyegetések, sebezhetőségek egyre elemibb részekre bontása, amelyek egy szint elérését követően a legtöbb esetben már meghatározott rendszer-összetevőkhöz kapcsolódnak. Az említett módszerek esetében eredményesen használhatóak fel az egyes rendszer-összetevő specifikus fenyegetés-fák, támadás-fák és részforgatókönyvek.

VÉDELMI RENDSZABÁLYOK, INTÉZKEDÉSEK DEKOMPOZÍCIÓJA

A biztonság megőrzésének egyik alapvető feladata a kockázatok kezeléséhez szükséges védelmi rendszabályok, intézkedések, eszközök meghatározása, megvalósítása és alkalmazása. Ezen intézkedések irányulhatnak a fenyegetéseket lehetővé tévő sebezhetőségek kiküszöbölé-

sére, vagy csökkentésére, valamint a fenyegetések elrettentésére, megelőzésére, észlelésére, az ellenük való védelemre, bekövetkezésük esetén káros hatásaik csökkentésére, majd következményeik felszámolására. A továbbiakban vizsgálatainkat leszűkítjük az informatikai biztonsághoz kapcsolódó kérdésekre.

A kívánt mértékű biztonság fenntartására irányuló, a kockázatokat elhárító, vagy elfogadható mértékre csökkentő ***védelmi megoldások, eszközök*** megnevezése az angol nyelvű szakirodalomban 'security control'. Az ISO 27000 fogalomjegyzék szerint a 'control' "a kockázatok kezelésének eszköze, beleértve politikákat, eljárásokat, irányelveket, gyakorlati megoldásokat, vagy szervezeti struktúrákat, amely lehet adminisztratív, technikai, igazgatási, vagy jogi jellegű. Megjegyzés: a 'control' használatos a védelmi intézkedés, vagy ellenintézkedés szinonimájaként is." [19, 2. o.]

Az Egyesült Államok Szabványügyi Hivatalának vonatkozó dokumentuma szerint a 'security control'-ok "az informatikai rendszerek számára előírt, a rendszerek és információk bizalmasságának, sértetlenségének és rendelkezésre állásának védelmére irányuló igazgatási, eljárási és technikai védelmi intézkedések és ellenintézkedések[11]". [20, 1. o.] A védelmi intézkedések magukban foglalnak "biztonsági jellemzőket, igazgatási korlátozásokat, a személyi biztonságot, valamint a fizikai struktúrák, területek és eszközök biztonságát." [21, 8. o.] Az ellenintézkedések pedig "tevékenységek, eszközök, eljárások, módszerek és más rendszabályok, amelyek egy informatikai rendszer sebezhetőségét csökkentik". [21, 6. o.]

Az Egyesült Államok hadereje vonatkozó dokumentuma szerint az 'IA [Information Assurance] control' "a sértetlenség, a rendelkezésre állás, vagy a bizalmasság objektív IA feltétele, amely meghatározott védelmi intézkedések alkalmazásával, vagy meghatározott tevékenységek szabályozásával érhető el és amely meghatározott formában van megfogalmazva ('control' szám, 'control' név, 'control' szöveg és egy 'control' osztály)." [22, 20. o.] A szabályozó szerint az 'IA control' olyan feltétel, vagy állapot, amely tesztelhető, teljesülése mérhető, illetve a megvalósulásához szükséges tevékenységek hozzárendelhetőek, így számonkérhetőek. [22, 48. o.]

A továbbiakban a 'security/information assurance control' fogalomra a védelmi rendszabály, intézkedés kifejezést használjuk, amely bár nem teljes egészében fejezi a fentiekben körülírt tartalmat, de megítélésünk szerint közelebb áll és közérthetőbbnek tűnik, mint az ellenőrzés, könyvvizsgálat szakterületéhez kapcsolódó – a COBIT módszertan magyar változata által is használt – kontroll. A COBIT a 'control' kifejezés további fordítási változatára többek között az irányítási és ellenőrzési eljárást tartalmazza. [23, 3. o.] A Magyar Informatikai Biztonsági Ajánlások párhuzamosan, lényegében érdemi megkülönböztetés nélkül használják a védelmi intézkedések, biztonsági intézkedések és kontroll kifejezéseket. [Lásd pld. 24]

A ***védelmi rendszabályok, intézkedések*** jellegük, megvalósításuk alapján különböző csoportokba sorolhatóak. Egyes osztályozások [pld. 19] adminisztratív, technikai (logikai) és fizikai védelmi intézkedéseket különböztetnek meg. Egy másik, széles körben használt osztályozás szerint vannak igazgatási (menedzsment), eljárási és technikai[12] védelmi rendszabályok, intézkedések. A három alapvető kategória a funkcionális hasonlóság alapján aztán tovább

[11] Safeguards, countermeasures.

[12] Az igazgatási rendszabályok, intézkedések a kockázatkezeléshez, illetve az informatikai rendszer biztonságának kezeléshez kapcsolódnak, az eljárási rendszabályok, intézkedések sajátossága, hogy azokat emberek, míg a technikai jellegűeket az informatikai rendszer hardver és szoftver összetevői valósítják meg, hajtják végre

osztható védelmi rendszabály, intézkedés családokra (négy igazgatási, kilenc eljárási és négy technikai). [20, 6 o.]

A védelmi rendszabályok, intézkedések kiválasztása, meghatározása az informatikai biztonság kialakítása és fenntartása folyamatának egyik alapvető feladata. Alapját a kockázatelemzés eredményei képezik és a feladatrendszer a kockázatkezelés része, lényegi összetevője. A biztonságpolitika és a biztonsági célkitűzések által meghatározott biztonság eléréséhez szükséges rendszabályok, intézkedések meghatározása alkotó folyamat, amelyet azonban jelentős mértékben segítenek különböző védelmi rendszabály, intézkedés katalógusok, listák. Ezek részben a háttértámogatás szándékával kerültek összeállításra, másrészt meghatározott területeken, például különösen a kritikus infrastruktúrák, vagy a katonai (védelmi) informatikai rendszerek esetében a minimális védelmi rendszabályok, intézkedések előírásához is alapul szolgálnak.

Átfogó védelmi rendszabály, intézkedés listák találhatóak többek között az ISO 27001 szabványban [25], amely tizenegy kategóriába, azon belül mintegy negyven alcsoportba sorolva száznál több rendszabályt, intézkedést tartalmaz; a NIST 800-53-ben [20], amelynek tizenhét családjába közel 200 rendszabály, intézkedés tartozik; vagy a DoD 8500.2 Utasításában [22], amely nyolc kategóriába sorolva közel száz rendszabályt, intézkedést rögzít. A NIST 800-53 a felsorolt intézkedéseket a szövetségi informatikai rendszerek számára javasolja, a DoD 8500.2 pedig a katonai informatikai rendszerek számára – működésbiztonsági kategóriájuktól és a kezelt információk bizalmassági szintjétől függő módon – minimálisan írja elő.

Az említett átfogó rendszabály, intézkedés listák mellett, azokat kiegészítve részterületenként ***részletes védelmi rendszabály, intézkedés listák*** is készültek. Ezek közé tartoznak például a biztonsági beállítási (konfigurációs) útmutatók és a biztonsági technikai megvalósítási útmutatók[13]. Ezek között megtalálhatóak szakterületekhez, objektumtípusokhoz – például hozzáférés ellenőrzés, adatbázis-kezelő rendszerek, stb. – tartozó és konkrét termékekhez (termékcsaládokhoz) – például Microsoft IE6, Oracle 8i, stb. – kapcsolódó útmutatók is.

Egy konkrét rendszerben érvényesítendő védelmi rendszabályok, intézkedések meghatározásának célszerű rendjét az alapvető módszertanok a lépésenkénti közelítés módszerével javasolják. Ennek első lépése a kiinduló[14] rendszabály, intézkedés lista kiválasztása, amelyet az egyes dokumentumok közös, vagy minimális rendszabályokként, intézkedésekként határoznak meg. Ezek egy része választható összetevőket és meghatározandó értékeket tartalmaz, amelyek segítségével második lépésként a rendszabályok, intézkedések "testre szabhatóak".[15] Végül az így kialakult lista bővíthető az adott rendszerre specifikus védelmi rendszabályokkal, intézkedésekkel.

Összetett objektumok, például informatikai rendszerek esetében a védelmi rendszabályok, intézkedések jelentős része, különösen alacsonyabb szinten – a sebezhetőségekhez és fenyegetésekhez hasonlóan – hozzárendelhető annak összetevőihez. A rendszabály, intézkedés listákban szereplő átfogó kategóriák nem elsősorban rendszer-összetevők szerint tagolódnak,

[13] Security Configuration Guide, Security Technical Implementation Guide (STIG).

[14] Baseline.

[15] Például: AC-7 Sikertelen bejelentkezési kísérletek: Az informatikai rendszer egy adott felhasználó számára [*meghatározott szám*] számú sikertelen bejelentkezést engedélyez [*meghatározott időtartam*] időtartamon belül. A megengedett számú sikertelen bejelentkezés túllépése esetén a rendszer [*[meghatározott idő] időre lezárja az azonosítót/eszközt; [meghatározott idő] időtartamig késlelteti a bejelentkezési kérdést*]. [20, F-6. o.]

azonban ezek többsége értelmezhető összetevőnként is. Például a hozzáférés ellenőrzés, a biztonsági mentések, az auditálás és megfelelőség-ellenőrzés konkrétan megvalósítandó feladatok a fizikai környezet, az operációs rendszerek, vagy az alkalmazások, köztük kiemelten az adatbáziskezelő rendszerek esetében.

Összességében megállapítható, hogy a védelmi rendszabályok, intézkedések jelentős része kapcsolódik közvetlenül összetett objektumok egyes összetevőihez. Ennek megfelelően találkozhatunk a szakirodalomban a hálózati védelmi intézkedések; az alkalmazás-szintű védelmi intézkedések, vagy az adatbázis védelmi intézkedések fogalmakkal, illetve listákkal.

Az említett – és más hasonló – informatikai rendszer-összetevő orientált védelmi rendszabályok, intézkedések jelentős szerepet játszanak az informatikai biztonság kezelésének rendszerében azonban megítélésem szerint hiányos az összhang az átfogó biztonság-, illetve kockázat-kezelési módszertanok és háttéranyagok, valamint a szakterületi megközelítések között. A gyakorlatban viszont egyaránt szükség van az átfogó megközelítésre és az ebből levezethető szakterületi szintű részletekre, illetve a bevált megoldásokra.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Összegzésképpen abból az általános megállapításból kell kiindulnunk, hogy a biztonság alanyai általában különböző – sajátos alkalmazási, funkcionális, technikai és biztonsági jellemzőkkel rendelkező – összetevőkre, alrendszerekre tagolhatóak. Ez mindenképpen igaz a vizsgálatunk szempontjából kiemelt kritikus információs infrastruktúrák, illetve informatikai rendszerek esetében. Ezek technikai összetevői közé tartoznak végső soron a hálózati infrastruktúra, valamint a végberendezések hardver, operációs rendszer, alkalmazói szoftver és adatbázis komponensei.

Az összetett objektumok, köztük az információs infrastruktúrák és informatikai rendszerek biztonsági vonatkozásai, kérdései – megőrzendő tulajdonságok, fenyegetések, sebezhetőségek, védelmi intézkedések – értelmezhetőek, vizsgálandóak és meghatározandóak az objektum egészére, illetve külön-külön egyes összetevőire. Az egyes biztonsági kérdések dekompozíciója alatt egy összetett objektum biztonsági kérdéseinek összetevői biztonsági kérdéseire történő lebontását, illetve az ezek között fennálló összefüggések meghatározását értjük.

A publikációban vizsgált kérdések mindegyikénél megállapítható volt, hogy szoros kapcsolat áll fent az összetett objektum szempontjából vett és az egyes összetevők szerinti megközelítések (vizsgálat, meghatározás, megvalósítás, ellenőrzés, értékelés, stb.) között. A két szint között elsődlegességet az összetett objektum egészére vonatkozó átfogó megközelítés élvez, azonban a gyakorlatban – sőt az elméletben – megkerülhetetlen az összetevő, ezzel egyben szakterületi szintű megközelítések (sajátosságaik, módszereik, eszközeik, megoldásaik) érvényesülése is. Következtetésként tehát megfogalmazható, hogy az átfogó biztonsági módszertanokhoz illeszkedő módon továbbra is szükséges és érdemes vizsgálni a biztonság különböző - összetevő-típusok szerint elkülönülő – részterületeit.

FELHASZNÁLT IRODALOM

[1] Munk Sándor: Informatikai biztonság vs. információbiztonság. – Robothadviselés 7 tudományos szakmai konferencia anyaga (2007.11.27.), Hadmérnök különszám.

[2] Munk Sándor: Katonai informatika II., Katonai informatikai rendszerek, alkalmazások. Egyetemi jegyzet. – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2006.

[3] ISO/IEC 15408-1, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. Third Edition. – 2009.

[4] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems. – National Institute of Standards and Technology, 2002

[5] A Magyar Köztársaság Nemzeti Katonai Stratégiája. Összefoglaló. – HM Zrínyi Kommunikációs Szolgáltató Kht. – Zrínyi Kiadó, Budapest, 2009.

[6] Information assurance through defense in depth. – Directorate for C4 Systems, US DoD Joint Chiefs of Staff, Washington, 2000.

[7] Összetett termékekre vonatkozó értékelési módszertan. – Miniszterelnöki Hivatal, Budapest, 2008.

[8] Rendszerekre vonatkozó értékelési módszertan. – Miniszterelnöki Hivatal, Budapest, 2008.

[9] Mann, David E.-Christey, Steven M.: Towards a Common Enumeration of Vulnerabilities. – MITRE Corporation, Bedford, 1999.

[10] Amoroso, Edward G.: Fundamentals of Computer Security Technology. – Prentice Hall, Englewood Cliffs, 1994

[11] Schneier, Bruce: Attack trees – modeling security threats. – Dr. Dobbs Journal, 1999/12., 21-29.o.

[12] McDermott, John-Fox, Chris: Using Abuse Case Models for Security Requirements Analysis. – Proceedings of the 15th Annual Computer Security Applications Conference, Phoenix, Arizona, 1999, 55-66. o.

[13] Sindre, Guttorm-Opdahl, Andreas L.: Capturing Security Requirements through Misuse Cases. – Proceedings of Norsk Informatikkonferanse NIK'2001, Trondheim, 2001. 11.26-28., 219-230. o.

[14] Kettenis, Jan: Getting Started with Use Case Modeling. An Oracle White Paper. – Oracle Corp., Redwood Shores, 2005.

[15] Landwehr, Carl-Bull, Alan R.-Mcdermott, John P.-Choi, William S.: A Taxonomy of Computer Program Security Flaws, with Examples. – ACM Computing Surveys, 1994/3, 211-254 o..

[16] Bishop, Matt-Dailey, David: A Critical Analysis of vulnerability taxonomies. TR CSE-96-11. – Dept. of Computer Science University of California, Davis, 1996.

[17] Hansmann, Simon-Hunt, Ray: A taxonomy of network and computer attacks. – Computers & Security, 2005/1, 31-43 o.

[18] Shiva, Sajjan-Simmons, Chris-Ellis, Charles-Dasgupta, Dipankar.-Roy, Sankardas-Wu, Qishi: AVOIDIT: A cyber attack taxonomy. Technical Report CS-09-003. – University of Memphis, 2009.

[19] ISO/IEC 27000:2009(E), Information technology – Security techniques – Information security management systems – Overview and vocabulary. – International Organization for Standardization/International Electrotechnical Commission, 2009.

[20] NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems. Revision 2. – National Institute of Standards and Technology, 2007.

[21] FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. – National Institute of Standards and Technology, 2006.

[22] DoD Instruction 8500.2, Information Assurance (IA) Implementation. – US Department of Defense, 2003.
[23] COBIT 4.1 Szószedet. Szakmai szótár. – ISACA Budapest Chapter, 2007.
[24] KIB 25. számú Ajánlása, Magyar Informatikai Biztonsági Ajánlások (MIBA). 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK). 25/1-1. kötet Informatikai Biztonság Irányítási Rendszer (IBIR). 1.0 verzió – Közigazgatási Informatikai Bizottság, 2008.
[25] ISO/IEC 27001:2005(E), Information technology – Security techniques – Information security management systems – Requirements. – International Organization for Standardization/International Electrotechnical Commission, 2009.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Németh Károly

Gerontology in Military Medicine

Absztrakt/Abstract

A gerontológia és a geriátria léte és alkalmazása napjaink fontos követelményévé vált. A téma több szempontból is aktuális! Társadalmunk rohamléptekkel öregszik. A gerontológia az öregedés kutatásával, a geritária a kóros öregedéssel és az idősek betegségeivel foglalkozó tudományág. Két szakmát határoz meg a beteg életkora: a korábban önállósult gyermekgyógyászatot, majd újabban az idősgyógyászatot a geritériát. A geriátria a szülészetet és gyermekgyógyászatot kivéve lefedi az egész klinikumot. Ennek ellenére a geriátria mégsem vált önálló klinikummá a gyakorlatban, szubklinikumai – pl. a mindennapokban is oly szükséges „gerontosebészet" – pedig még kevésbé léteznek. Ha megvizsgáljuk a katonák gerontológiai folyamatát, akkor nyugodt szívvel ki lehet jelenteni, hogy a katonai pálya nem nyugdíjas állás. A történelem háborúi a nemzetek fiainak színe-javát irtotta és írtja ki ma is az emberre jellemző, általa kimunkált kegyetlen eszközök, anyagok segítségével. Az állandó fegyverkezési verseny, a fejlesztések, kutatások kényszere rányomja súlyos bélyegét az ebben résztvevő katonára. Ilyen életritmusban, sajátos életkörülmények között csak a katona él. Az állandó stressz, készenlét, kiképzés, a megfelelési kényszer, a gyakorlatok, háborúk, végül, de nem utolsó sorban az idő előtti meghalás fenyegetettsége elsősorban a hivatásos katona életét befolyásolja negatív irányba! A nyugdíjkorhatárt elért tisztek, tiszthelyettesek 70%-a nem éri meg a 70. életévét, 25 %-a meghal 65 éves korára, míg 5%-a él „boldogan" hetven éven túl. 1986. november 10-én nyílt meg az akkori Magyar Néphadsereg Betegotthona, - 2007. július elsejétől a Honvédelmi Minisztérium Állami Egészségügyi Központ Intézeteként (továbbiakban HM ÁEK) – amely a mai napig 120 ágyon igyekszik segíteni ill. gyógyítani a Magyar Honvédség, a rendvédelmi szervek valamint a MÁV geriátriai ellátásra szoruló állományát.

Gerontology and geriatrics are exceedingly important nowadays for several reasons, one being that our society is ageing with enormous speed. Gerontology is a science of ageing processes, while geriatrics studies pathological ageing and diseases of elderly people. Patient's age determines two professions: pediatrics that became an independent profession earlier, and healthcare of elderly people, or geriatrics, recently. Geriatrics covers the whole spectrum of clinical medicine, except for obstetrics and pediatrics. Despite of this fact, geriatrics did not gain

its independence in clinical care, and its clinical sub-branches, like geronto-surgery, hardly exist at all. If we examine gerontology (ageing process) of military people, the conclusion that military profession does not favor soldiers in regards of reaching their retirement age, is easy to make. Different wars during the history of mankind have depopulated and still are depopulating nations taking away the best of their human resources, using cruel and sophisticated equipment, methods and material. The constant imperative for armament race, developments and research leave their heavy scars on soldiers. Only soldiers live such a life style, only they have such special conditions of life and work. Constant stress, readiness and training, necessity to meet the expectations, exercises, wars and – last but not least – the threat of early death, are all factors negatively influencing the life of active duty personnel. 70% of retirement age officers and non-commissioned officers will not make it to their 70th birthday, 25% of them will die before their 65th birthday, and only 5% of them will "live happily" after 70.

The former Hungarian Armed Forces opened its Home on November 10, 1986. This facility still has 120 hospital beds and as an institution of the MOD National Medical Centre is aiming to help the personnel of the Hungarian Defence Forces, the Police Force and the Hungarian State Railways requiring geriatric care also nowadays.

Kulcsszavak/keywords: *gerontológia, geriátria, szociális gondoskodás, idősgondozói hálózat ~ gerontology, geriatrics, social care, care network*

Introduction

Gerontology is a discipline dealing with the specialities and the implications of the process of ageing. It is a very young area of medicine; it is only a couple of decades that it has gained ground as an acknowledged field of study.

Geriatrics, which deals with the treatment and care of old patients, has become part of the field of study as a result of the achievements of gerontology.

In the last couple of decades parallel with the development of medicine geriatrics has become an independent specialty for several reasons. In most countries, in Hungary too, substantial part of the population is old, and this tendency is still growing. At the same time the general demand for improved quality of life is continuously increasing, multiplying and diversifying the tasks of doctors and other experts working in both primary care and in hospitals and clinics. The economic aspects of medical care in general and within this the accumulating special tasks of the medical treatment and social care of the aged, also account for the independence of geriatrics.

The pre-requisite for the relatively secure life of the aged population was the strengthening of the middle classes and the growing respect for human life. Industrialisation accounts for the appearance of the class of propertiless labourers, who lived in poverty, who could not save up, and when old, even lost their ground of existence. To solve this situation workers', private and civil

servants' pension funds were established in the 19th century. (The founder of these was Bismarc, German councilor in 1887) Both the employers and the state took part in financing the system. This started off a fast but far from accomplished change in the division of labour in medicine which was simply called medical reform. Medical disciplines started to develop or reorganize along different principles: some on the basis of methodology (radiology, surgery) others on basis of organs (ophthalmology), systems of organs (neurology). There are two areas which are determined by the age of the patient. One is pediatrics, which has become independent earlier; the other is geriatrics, the care of old people emerging in our days. While the fact that a child is not a small adult is generally accepted, the fact that and old man is not just a grey haired, adult with wrinkles, but a person of very different character is not widely known. What is common in childhood and old age is that they are both dependent on adults. Consequently the specialty of their medical care is that it should be done by involving the family or supporter. This is the main feature of the care of old people. The older and less healthy a person is the more vulnerable and the more dependent he is on his family or people around him, just like a child. With the exception of obstetrics and pediatrics geriatrics covers the whole spectrum of clinical medicine.
There are more and more old people with chronic illness, who are becoming more and more ill and developing more and more symptoms. Consequently geriatrics has to treat more and more seriously ill patients on every field of clinical specialties.

In the past decades in welfare states there has been an improvement both in the financial and the medical state of the pensioners, the former as a result of the growth of GDP the latter as a result of the development of medicine. Their average age and ratio in the population has increased. Earlier the life of an individual was divided into three stages: first the period preceding the working age, when he is dependent and studying; second the active period, when he is working and supporting others; the third when he is dependent again and supported by others. In welfare states a new stage has been identified between the above second and third period: active old age. People in this period are not part of production any more, nevertheless their financial state is still stable, their activities are not limited by their age or medical state is; they can devote themselves to their hobbies, they travel and study.

It is obvious that as opposed to the welfare states geriatrics in the transforming East-European societies has a very different task to accomplish with opportunities far from being equal. The knowledge and experience which has been the basis of the respect and might of old people all through history has unfortunately lost its value by our age. The reason for this is the immense speed of development which can only be followed by the elderly, if they have special abilities. Nowadays not just the old, but also the middle aged people are

disadvantaged on the labour market. Only the more dynamic, creative intellectuals may keep their advantaged position, but in case of the average employee this change means the ageing of the society.

Some numbers illustrating the demographic and "social-economic" features of the ageing population.

Chart 1.[1]

Year	Population	Over 60 (people)	(%)
1960	9.961.044.	1.372.661.	13.7
1990	10.374.823.	1.959.846.	18.8
2003	10.142.362.	2.111.585.	20.8
2004	10.116.742.	2.126.027.	21
2025	9.400.000.	3.008.000.	30.2

The rate of the old (over 60) age group in Hungary between 1960-2025

The growing rate of the aged is caused by the unfavourable changes in the demographic composition of the whole population; the decrease of live birth and the growth of middle age mortality. In Hungary the rate of population over 60 has increased to 22,1% from 13,7% between 1960 and 2010 while the average life expectation of the whole population has increased from 68 to 72,6 years. In 1890 people over 60 were only 5,1% of the whole population. There is also a regional difference in the distribution of the old age population, Heves being the oldest and Szabolcs-Szatmár the youngest county with 21,4% and 17,1% respectively.

Epidemiological features

In Hungary life expectancy of the 60 and 70 year old population has decreased in case of men, but has shown a slight increase in case of women in the last 50 years. There has been a slight decrease again in recent years. Life expectancy is 68,6 years for man and 76,9 for women at present. (In France it is 78 and 84 respectively.)

The leading cause of death in both sexes results from the illness of the circulatory system. This cause represents 50-52% of the mortality in the

population between 65-74 and more than 60% of the mortality in the population over 60 [1].
Among the leading causes of death the second is cancer, the third is chronic hepatopathy and hepatic cirrhosis, the forth is chronic respiratory disease. The fifth place is taken by violent deaths, the rate of which is over 10 %. The rate of the so called avoidable deaths is high. 30-36% of the 2000-3000 annual terminal suicide is committed in the over 60 age group. The Hungarian old age suicide rate is the worst in international comparison. The causes of this may be the loss of social prestige and status as a result of retirement, (depression, the feeling of becoming useless) the restriction of the most often concerned psychic areas which effect old age e.g. judgment, memory, intellectual performance, temper, orientation..

The aged are disposed to several negative environmental effects, retirement in itself, financial loss, lack of human relationships, decrease of physical and mental performance, insecurity in independence and self assessment, depreciation of others, isolation, illnesses, having to be hospitalized, or having to move into old peoples' home etc. It is even more difficult for the lonely old people: they lose their aim, their daily routine is derailed and they miss physical and spiritual support. In addition, the average pension is just a little higher than the minimum wage.

Military Gerontology

In light of the above there are tasks to be accomplished in the field of geriatrics concerning the Hungarian Armed Forces too. Examining the gerontologic process of soldiers, we can state that military career is in inverse proportion with longevity, due to the fact that mankind has been in constant warfare with itself for several centuries. Since ancient times, well organised armies with the leadership of talented commanders have been slaughtering each other for ethnical and religious reasons or with the aim of conquering territories, always making sure that soldiers should not die in bed with white hair of old age. Wars have exterminated and are still exterminating the best of our human resources with the most cruel devices and materials. This is proved by the military operations going on today. Military profession – because it is a real profession – cannot be compared to anything. It involves all forms of the technical revolution combined with all fields of science. Armies try and apply the latest scientific inventions. The constant arms race and the pressure of research and development exert their very negative effect on the most important factor involved in it, the soldier! Constant stress, readiness, training, pressure to meet the requirements, exercises, wars and last but not least the threat of premature death all negatively effect the lifespan of the professional soldier. 70% of retired officers don't live to be 70, 25 % die before the age of 65, and only 5% live longer than their 70^{th} birthday.

The importance of care was already recognised by the military leadership of the 80s. In 1982 the Military Committee of the Hungarian Peoples' Army made a decision that after the dislocation of the Verőce missile unit a social and medical institution should be established on the 17 hectare area.
This was a rational decision partly because of the infrastructure of public utilities of the area and partly because until then there had not been chronic and old age rehabilitation and care in the medical system of the Hungarian Armed Forces.
This is how the Medical Home was built. It was opened on 10th November 1986. Now the treatment and care of old people is carried out on 120 beds.

The Verőce Medical Home of MOD NMC receives the entitled and their relatives needing chronic and long term (90-180-day) treatment. The 98 strong staff treats and looks after the patients with great expertise and empathy. To this day they have treated 14350 patients the youngest being 16, the oldest 101.
58% of their patients need comprehensive treatment. There is no doubt that the Medical Home is necessary.

Chart 2.[2]

Year	Degree of bed utilization in %
2005	96,3
2006	95.5
2007	86,5*
2008	91,3
2009	96,7
30.04. 2010.	97,4

(* Utilization of beds decreased in the period of creating new beds.)
MOD NMC VMH indices of bed utilization between 2005 and 2010.

The ratio of entitled patients on average is 85%. If bed utilization makes it possible the Home receives patients from the region too. Mortality rate is 22%. Patients arriving at the Home are in a very serious condition requiring long treatment or often they are in the final stages of their life. The primary responsibility and task of the Institution is to take perfect care of the patients till the end of their life. This should be done in a way to enable the patient to die with dignity. So far this has been achieved, which earned the home countrywide acknowledgement.
In summary we must state, that the importance of gerontology and geriatrics has substantially increased over the last decades, and by today it has become indispensable. However it is important to emphasize the role of the family, and the cohesive power, active support and participation of the society in this issue.

References

[1] Magyar Statisztikai Évkönyv, 2009

[2] Verőcei Betegotthon statisztikai adatok 2005-2010.

HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Tóth András
toth.andras@regiment.hu

Farkas Tibor
farkas.tibor@zmne.hu

Pándi Erik
pandi.erik@zmne.hu

A VÁLSÁGREAGÁLÓ MŰVELETEK HÍRADÓ ÉS INFORMATIKAI TÁMOGATÁSÁNAK ELMÉLETI ALAPJA

Absztrakt

Az elmúlt több mint másfél évtizedben lezajlott világpolitikai folyamatok jelentős befolyást gyakoroltak a nemzetközi biztonságpolitikára. A hidegháborúval a globális méretű politikai, gazdasági és katonai szembenállás ugyan megszűnt és minimálisra csökkent egy világméretű fegyveres konfliktus veszélye, de új típusú konfliktusforrások, és új kihívások törtek felszínre. Jelen közlemény az MH-val, illetőleg a híradó és informatikai rendszerével kapcsolatosan fennálló feladatokra világít rá.

The international security policy had changed by the process of world-politics, in the last one and half decade. After the end of the cold war, global political, economic and military opposition was broke off, and the danger of word-wide armed conflict is very law. But the new type of conflicts and new challenges appeared, which's supplement the conventional contingency. This article deals with the Hungarian Defence Forces and the extant tasks of the CIS.

Kulcsszavak: *háborús és nem háborús műveletek, híradó és informatikai rendszer, válságreagáló műveletek, vezetés és irányítás ~ military operations other than war, communication and information system, command and control*

1. A NATO válságreagáló műveletének alapelvei, a szövetséges erők képességei

A nem háborús katonai műveletek[1] új típusú sajátos szemléletet, és az adott válság rendezéséhez legalkalmasabb, változó összetételű szervezeteket követelt meg. A politikai döntéseket követően, a megalakításra kerülő katonai szervezeteket különböző civil egységekkel kooperálva szervezik meg, amelyek együttműködése a sikeres műveleti feladat végrehajtásának alapvető követelménye[2]. A létrehozott ideiglenes katonai szervezetek speciális kiképzési, felkészítési formákat igényelnek az adott területnek megfelelően, és a végrehajtott műveletek megkövetelik az egyéni-, technikai biztosítást, felszerelést és a szilárd, rugalmas vezetést.[3]

A NATO válságreagáló műveleteknek (CRO)[4] nevezi azokat a tevékenységeket, amelyek a kialakult konfliktus kezelésére, esetlegesen megelőzésére, a válságkezelésre irányulnak. **Tehát a CRO minden esetben egy összetett, többfunkciós művelet, amely során katonai képességek kerülnek felhasználásra polgári-, humanitárius- és más rendészeti szervekkel együttműködve, amely a megelőzésre, ellentevékenységekre, és a kialakult helyzet stabilizálására, és esetlegesen egyéb kiegészítő tevékenységekre irányul.** Természetesen ezeknek a műveleteknek összhangban kell lenniük a vonatkozó nemzetközi jogokkal, felhatalmazásokkal és mandátumokkal. Az 1999-ben elfogadott stratégiai koncepció[5] alapján a Szövetség legfontosabb feladata a különböző konfliktusok, az instabil államok helyzetéből adódó biztonsági kockázatok megszüntetése és felszámolása, kiemelve a közel-keleti és észak-afrikai térség biztonsági kockázatát. Véleményem szerint ezt a dokumentumot kell kezelni az alapvető, a jelenleg is érvényben lévő elvek „alapkövének". A NATO Katonai Bizottsága[6] segíti a Szövetséget az átfogó stratégiai koncepciók kidolgozásában az általuk elkészített dokumentumokkal, amelyek ajánlások a katonai erők felkészítésre és a készenléti tervek végrehajtására. Ebben az időszakban kerültek felállításra a többnemzeti összhaderőnemi alkalmi harci kötelékek[7], amelyek rugalmas, mozgékony kötelékek a többfunkciós alkalmazások ellátására.

A NATO-t létrehozó Észak-atlanti Szerződés 14 cikkelyből áll, amely V. cikkelye rendelkezik a kollektív védelemről. Az V. cikkely értelmében bármely tagállamot ért támadás az egész Szövetség elleni támadást jelenti, amellyel szemben a szervezet fegyveres fellépést tesz a béke és biztonság helyreállítása érdekében. Az idő előrehaladtával, a technológiai fejlesztések rohamos ütemével párhuzamosan megváltoznak a veszélyek jellegei, ezért napjainkban a szakértőkben több kérdés is felmerül, amely alapjaiban változtatja meg az alapelveket, stratégiákat. Ilyen a kibernetikai támadások kérdésköre is. Rábai Zsolt előadásában felhívta a figyelmet, hogy egy NATO-tagország elleni hagyományos értelemben vett támadásra történő reagálást tartalmazza az V. cikkely, de ha az adott nemzet gazdaságát is fenyegető számítógépes támadás éri a tagállamot, akkor az értelmezhető vagy sem az V. cikkelyben megfogalmazottaknak. [2]

---

[1] Az amerikai hadsereg megfogalmazása szerint: Military Operations Other Than War (MOOTW) [1]

[2] Fontosnak tartom a polgári szervezetekkel történő együttműködés elsajátítását, amely a műveleti feladatra és annak minden oldalú biztosítására egyaránt kiterjed.

[3] A speciális felszerelés, technikai biztosítás természetesen a híradó- és informatikai rendszereket is magába foglalja, amelyek alkalmazása kiemelt fontosságú a vezetés és irányítás támogatásában.

[4] Crisis Response Operations

[5] Washington, 1999. április 23.

[6] Military Committee; Az általuk kidolgozott dokumentumokat „MC"-nek nevezik.

[7] CJTF (Combined Joint Task Forces)

Az előzőekben leírt válságreagáló műveletek a NATO válságkezelésének részét képezi, amelyet az V. cikkely alá nem tartozó műveletekként azonosítja a Szövetség. A NATO alapokmányai közül meg kell említenem az AJP-3.4 Non Article 5, Crisis Response Operations-t[8], amely a vonatkozó doktrína ezen típusú műveletek végrehajtása során, illetve a Katonai Tanács dokumentumát az MC 327/2-t[9] és az AJP-01B (C)[10] doktrínát. A dokumentumok, és a koncepció szerint fel kell készíteni a tagállamok fegyveres erőit a válságok kezelésére, fegyveres konfliktusokra, amely célja, hogy a Szövetség kellő időben és összehangoltan reagáljon a fenyegetésekre. A szabályzatok, okmányok minden esetben behatárolják a vezetés és irányítást, a részvételt a műveletek teljes spektrumában és a különböző típusú műveleteket. A tagországok az ilyen típusú műveletekben nem minden esetben vesznek részt, eltérően a kollektív védelemtől. A Szövetség esetleges felkérésére, a nemzetek politikai döntését követően vállalnak feladatokat lehetőségeikhez mérten. A megszervezésre kerülő többnemzeti műveletek az alábbi főbb kategóriákba sorolhatók:

- béketámogató műveletek (Peace Support Operations);
- egyéb műveletek.

A különböző nemzeteket, szervezeteket figyelembe véve ez az alapvető felosztás eltérő lehet, amelyet az alábbiakban fogalmaztak meg a szerzők „A Válságreagáló műveletek elmélete és gyakorlata a 21. században" című egyetemi jegyzetben: *„Mindenek előtt célszerű tisztázni, hogy mint minden felosztás ez is esetleges. A válságreagáló műveletek meghatározására az egyes országok, a NATO, és más nemzetközi szervezetek által elfogadott és használt felosztás nem egységes. A NATO-ban használt felosztás szerint ezek az alábbiak: Először béketámogató műveletek […] Másodszor, Humanitárius műveletek […] Harmadszor, Kutató-mentő műveletek. [3]*

A béketámogató műveletek valamilyen nemzetközi szervezet[11] felhatalmazását követően kerülnek végrehajtásra a Szövetség vezetésével, a feladatokat ellátó nemzetek részvételével. Fontos megjegyezni, hogy ezekben a műveletekben a nem NATO tagállamok is részt vehetnek, felajánlhatnak erőket. A béketámogató műveletek az alábbiak szerint lehet szétválasztani, a konfliktushelyzet kialakulásától kezdve, a békeállapot újbóli eléréséig, időrendben. (Természetesen ezek szintén változhatnak a válság intenzitásától, a közbelépéstől, és egyéb más tényezőtől.)

- *konfliktus megelőzés (conflict prevention)*; amely a diplomáciai lépésektől általában a kijelölt alegységek telepítéséig terjedő időszak tevékenységei, magukba foglalva a fegyveres összetűzések kialakulásának megakadályozását;
- *béketeremtés (peace-making)*, a konfliktus megelőzést követő tevékenység, amely a már kirobbant fegyveres összetűzések megfékezésére irányul, főként diplomáciai úton és megelőző katonai lépésekkel;
- *békekikényszerítés (peace enforcement)* olyan diplomáciai, katonai, gazdasági lépések (vagy együttes alkalmazása) adaptálása, amelyet a békés eszközök eredménytelenségét követően katonai kényszerítő eljárásmód követ;
- *békefenntartás (peace-keeping)* célja, hogy a már kialakult (kikényszerített) béke helyzetet, stabilitást a műveletekben résztvevő erők stabilizálják,

[8] 5. Cikkelyen Kívüli Válságreagáló Műveletek; NATO, 2005. március 1.
[9] NATO Military Policy for Crisis Response Operations, amely irányadó a CRO műveletek tervezéséhez szervezéséhez és meghatározza a vonatkozó alapelveket, szempontokat.
[10] AJP 01B: Allied Joint Doctrine (Szövetséges Összhaderőnemi Doktrína) és az AJP-01C, amely a doktrína 2006-os kiadása
[11] Például ENSZ: Koszovó, Afganisztán területén végrehajtott, a válság rendezésére irányuló műveletek.

fenntartsák, az esetleges ellentéteket enyhítsék valamennyi fél hozzájárulásával;

- *békeépítés (peace building)* azon eljárások összessége, amelyek megszűntetik a kialakult konfliktusok okait, és elősegíti a konfliktus előtti állapotok visszaállítását, de a feladatok végrehajtása során már a polgári szervezetek tevékenységén van a nagyobb hangsúly, akik tovább erősítik a lakosság életének visszaállítását, a gazdaság újbóli fellendülését;
- *humanitárius segítségnyújtás/műveletek (humanitarian relief)* azon tevékenységek összessége, amely az emberek életének elősegítését biztosítja, többnyire civil szervezetek végrehajtásával és esetleges katonai biztosítással.

A válságreagáló műveletek másik csoportjába tartoznak a különböző feladat végrehajtások támogatására irányuló tevékenységek, amelyek nemzeti vagy többnemzeti szinten egyeztetett feladatok. Ez lehet:

- humanitárius segítségnyújtás támogatása;
- kutató-mentő feladatok ellátása, biztosítása;
- a civil szervezetek és hatóságok katonai támogatása;
- esetleges evakuálási, kiürítési feladatok végrehajtása, biztosítása;
- katasztrófák megszüntetésében való részvétel.

Ezeket a feladatokat és azok sikeres végrehajtását nagymértékben befolyásolja a résztvevő *állomány összetétele* (katonai, civil, egyéb hatóságok, más fegyveres szervezetek, kormányzati-, és nem kormányzati szervek), *az adott terület mérete és földrajzi elhelyezkedése*, a *tevékenységet folytató erők nemzeti összetétele*, és természetesen a *politikai döntések és jogi szabályozások*. **A válságreagáló feladatok tehát olyan tevékenységek összessége, amelyek az adott ország, régió béke állapotát megszüntető konfliktushelyzetet (esetlegesen háborút), vagy a területen kialakult egyéb válságokat felszámolja, az újbóli béke megteremtése érdekében.** Az előzőekből jól látható, hogy a tevékenységek jelentős részében a katonai jelenlét elkerülhetetlen, így a nemzeti haderők képességei meg kell, hogy feleljenek a hagyományos értelemben vett háborús feladatok mellett, az ilyen típusú műveletek ellátására.

2. A többnemzeti műveletek végrehajtását biztosító képességek és követelmények a NATO-csúcsértekezletek tükrében

A közlemény elején hivatkozott washingtoni szerződésben leírtaknak megfelelően, az új stratégiai koncepcióban – amely főként a balkáni missziók tapasztalatain alapul – megfogalmazottak szerint került kialakításra a képességfejlesztési irányelv, amely a **mozgékonyság és telepíthetőség**, a **fenntarthatóság,** az **eredményes harci alkalmazás**, a **túlélőképesség** és **a hatékony kommunikáció** irányelveit vetítették előre, mint jövőbeli követelményként. A NATO ennek megfelelően folytatta a stratégiai koncepciójának bővítését, amelyet a későbbiekben megrendezett NATO-csúcsértekezleteken megtárgyaltak, írásba foglaltak. A csúcsokon minden alkalommal a kor akkori kihívásainak, követelményeinek megfelelően, és az adott időszak veszélyeinek figyelembevételével tárgyalták és vitatták meg azokat a legfontosabb kérdéseket, amelyek a Szövetség későbbi (mai) koncepcióját tükrözi. Ez szolgál alapul a NATO és a tagországok képesség fejlesztési stratégiájának.

A *prágai NATO-csúcson*[12] további megfontolások hangzottak el a képességfejlesztéssel kapcsolatban, amely a koszovói válságot és a 2001. szeptember 11-i terrortámadásokat vette alapul. Egy olyan „átfogó intézkedési csomag" került kialakításra, amely az addigi stratégiai koncepciót és a Szövetség képességeit erősíti. A dokumentum szerint különösen nagy figyelmet kell fordítani a NATO küldetéseinek ellátására, amely a tömegpusztító fegyverek és a terrorizmus hatására megjelenő fenyegetéseket hivatott lecsökkenteni. Mindezek érdekében olyan erők létrehozását kell megvalósítani, amelyek **rugalmasak, együttműködésre képesek, gyorsan telepíthetők** az adott helyszínre – ez magába hordozza a szállítás kérdéskörét is –, a **feladatok végrehajtását önállóan képesek ellátni** akár hosszabb időre is, és fel kell készíteni ezeket az erőket az esetleges **NBC**[13] **támadások kezelésére**. Az elvárásokat figyelembe véve kezdték meg az NRF[14] létrehozásának előkészítését, amelynek teljes készültségét 2006-ra határozták meg. Kihangsúlyozták az **együttműködő képességre** való törekvés, a **hírszerzés**, a korszerű **vezetés és irányítási** elvek, és a **támogató képességek** fontosságát, továbbá előtérbe helyezték a modern hadviselés követelményeinek, illetve a **számítógépes hálózatok védelmének** előmozdítását. Ezt követően vált az MH elsődleges feladatává a missziós tevékenységek ellátása, amelyet jól tükrözött a külszolgálatokat ellátó katonák létszámának növekedése (amelyet elősegített a professzionális haderő kialakítása), és 2004-től az NRF-ben való szerepvállalásunk.

A 2004-ben megrendezett *isztambuli-csúcson*[15] a XXI. századi **műveletekhez való alkalmazhatóságot** és a **felhasználhatóságot** helyezték előtérbe, amely értelmében **komplexebb hozzájárulást** (szárazföldi, haditengerészeti, légi) követelnek meg a tagországoktól. Az afganisztáni nemzetközi erők fokozottabb támogatását sürgették, amely a közelgő választásokat hivatott biztosítani. Ennek megfelelően kellett a helyi erőket felkészíteni mind képességben, mind technikai eszközökkel a megfelelő biztosítás érdekében. Az **együttműködési képességek** további megerősítése nélkülözhetetlen a sikeres műveleti feladatok ellátásában, amelyre nagy hangsúlyt kellett fektetni a misszió többnemzeti jellegéből adódóan. **Korszerű technikai eszközökkel felszerelt**, új **vezetés és irányítási elvekkel** rendelkező, „használhatóbb", **telepíthető alegységek** megszervezésére volt szükség, amelyek felállítása a nemzetek feladata, és lehetséges alkalmazásuk segíti elő a Szövetség elkötelezettségét a nemzetközi béke és stabilitás iránt. A **tömegpusztító fegyverek (WMD)**[16] és a terrorizmus további térnyerése fokozott fenyegetést jelen a Szövetség számára. Ezt támasztják alá az isztambuli[17] és a madridi[18] terrortámadások is. Ennek érdekében a **hírszerzési feladatokat** és a megszerzett **információk megosztásának képességét** a tagországok között meg kell erősíteni. A **gyorsreagáló képesség** további fejlesztése, az NRF erők biztosítása a későbbiekben is jelentős a követelményeknek való megfelelésben. A sikeres küzdelem és a tömegpusztító fegyverek ellen történő fellépés érdekében megalakításra került egy NATO CBRN[19] Védelmi Zászlóalj.

A 2006-os *rigai-csúcs*[20] fontos és sarkalatos pontja volt az afganisztáni helyzet elemzése. Nagy hangsúlyt fektettek a **tartományok újjáépítésére** a térségben, amelyek az eddigieknél **nagyobb civil jelenlétet** és **együttműködési képességet** követelt meg. Dr. Szenes Zoltán

[12] 2002. november 21–22
[13] Nuclear Biologichal Chemical
[14] NATO Response Forces
[15] 2004. június 28–29.
[16] Weapon of Mass Destruction
[17] 2003. november 15. és november 20.
[18] 2004. március 11.
[19] Chemical, biological, radiological and nuclear
[20] 2006. november 28–29.

publikációjának összefoglalásában leírja, hogy az előbbiekben felsoroltak alapján a Magyar Honvédség képességei, feladatrendszere teljes mértékben megváltozott. *„A NATO-transzformáció teljes mértékben megváltoztatta a Magyar Honvédség biztonsági környezetét, magát a haderőt és annak működési feltételrendszerét." [4]* Fontos kérdéskör volt a találkozón a terrorista akciókra történő fellépés új dimenziói. Előtérbe kell helyezni a **legmodernebb technológiai eszközök alkalmazását**, amelyek képesek megerősíteni az ellenséges erők új típusú támadásaira történő hatásos reagálást illetve a megelőzést. Mindezek érdekében minden nemzetnek **folyamatos fejlesztéseket** kell végrehajtania, amelyek tovább erősítik a Szövetség katonai képességeit. A rigai-csúcson ismételten kihangsúlyozták a **mobilitás** kérdéskörét, amely elengedhetetlenül fontos eleme a **hatékony**, **időbeli reagálásnak**, illetve azt, hogy a jövőben tökéletesíteni kell a **multinacionális**, a Szövetség területétől távol lévő – befogadó nemzeti támogatást nem nyújtó – területeken végrehajtott műveletekben való részvételt. Ezen a csúcsértekezleten került megfogalmazásra a **NEC**[21] egyre növekvő igénye, amely alapvetően a műveletekben résztvevő Szövetséges erők között az **információk megosztását, és azok megbízható, gyors és biztonságos továbbítását** jelenti, illetve azok **védelmét a számítógépes hálózatok elleni támadások során**. További képességfejlesztések főbb eleme a CBRN fenyegetések elleni védelem is, amely tovább növeli az erők védelmét a siker kivívása érdekében.

A 2008-ban megrendezett *bukaresti-csúcstalálkozón*[22] kiemelték a terrorizmus elleni fellépés fontos elemének, a **hírszerzésnek és az információcserének a megerősítését**, amely hatékony alkalmazása tovább erősíti a NATO műveletekben résztvevő erők jelenlétét, védelmét. Kihangsúlyozták, hogy a NATO továbbra is készen áll a mindennemű fenyegetésre történő gyors fellépésre, de szükséges a szorosabb együttműködés a nemzetközi biztonsági veszélyek mai és jövőbeli kezeléséhez. A tagországok kezdeményezései, felajánlásai – a **stratégiai légi szállítás** és a **hadszíntéren belüli légi szállítás** – az erőteljesebb jelenlétet segítette elő (mindenekelőtt a többnemzeti műveletekben), amely a találkozó különösen fontos kérdésköre volt. Egyetértés született a **hálózat nyújtotta képességek** megerősítésére az információs fölény kivívása érdekében, amely **integrált vezetés-irányítási rendszert** követel meg a nagyobb hatásfokú művelet-végrehajtás érdekében. A NATO továbbra is elkötelezett a **szabványosítás** és **magas fokú együttműködő képesség** fejlesztése, és az **informatikai hálózatok megóvása**, biztonságának növelése területén. A terrorista akciók és az azok ellen történő fellépés az aszimmetrikus hadviselés jegyeit hordozzák magukban, de a terrorista csoportok a hagyományos (kézi) fegyverek mellett alkalmazhatnak **tömegpusztító fegyvereket** is, amely igen megnehezíti a Szövetséges erők fellépését, ezért ez irányú képességek fejlesztése sem maradhat el a számos más területtől.

A 2009-es *Strasbourg–Kehl* NATO-csúcstalálkozón[23] a Szövetség megerősítette a stratégiai elképzelését Afganisztánnal és Koszovóval kapcsolatosan, illetve a terrorcselekmények, tömegpusztító fegyverek elleni fellépéssel összefüggésben. Az egyeztetések értelmében továbbra is **kiemelten kell kezelni és folytatni az addigi technológiai fejlesztéseket**, és nagy hangsúlyt kell fektetni a NATO missziók támogatása érdekében az **információszerzésre**, és a megszerzett **adatok megosztására**. A **telepíthető, fenntartható, rugalmas erők** alkalmazását tovább kell erősíteni, és törekedni kell az esetleges hiányosságok megszüntetésére. A Szövetség és a tagországok informatikai hálózatainak nagyobb védelme

[21] Network Enabled Capability (hálózat alapú képesség), amelyet az Egyesült Királyság Védelmi Minisztériuma fogalmazott meg, és nagymértékben megegyezik az amerikai Network-Centric Warfare - Hálózat Központú Hadviselés fogalmával.
[22] 2008. április 2–4.
[23] 2009. április 3–4.

érdekében az **informatikai- és kommunikációs eszközök fejlesztésére** különös figyelmet kell fordítani, mivel ez a terület szintén előtérbe került a jelenlegi kockázatok „listáján".

A NATO-csúcsértekezleteken megtárgyalt és meghatározott képességek az adott időszak változásait, a missziós tevékenységek során szerzett tapasztalatokat figyelembe véve kerültek meghatározásra. **Meglátásom szerint az „élethosszig tartó tanulás" mintája alapján, a folyamatosan megjelenő új kihívásokra történő gyors és hatékony reagálás csak akkor valósulhat meg, ha felismerjük azokat az irányokat, amelyek elősegítik e törekvéseinket, és képesek vagyunk meghatározni azokat az elveket és eszközöket, amelyek felhasználásával elérhetőek a kitűzött célok.** Ez természetesen minden NATO tagállam alapvető feladata, amely a folyamatos fejlesztéseket nagymértékben meghatározza.

3. Az MH lehetséges nemzetközi feladatai, a híradó és informatikai támogatás definíciója

A Magyar Köztársaság NATO műveletekben való részvétele – várhatóan – a jövőben is meghatározó lesz. Az előző alfejezetben leírtaknak megfelelően, az V. cikkely és a nem V. cikkely szerinti műveletekben való részvétel alapvető kritériuma a képességeknek, kihívásoknak való megfelelés. Az ország biztonságát fenyegető globális, regionális és közvetlen környezetből származó fenyegetések nagymértékben befolyásolják a stratégiánkat. A Magyar Köztársaság Nemzeti Katonai Stratégiájában megfogalmazottak szerint a honvédelem két pillére a nemzeti önerő és a szövetségi együttműködés. Az MH feladatai e két területnek megfelelően tevődik össze, az előzőekben tárgyalt képességekhez és fejlesztésekhez hasonlóan. A magyar katonai erők külföldi alkalmazására minden esetben nemzetközi felhatalmazást követően kerülhet sor, amelyet jól tükröz az eddigi missziós tevékenységünk is. Az MH nemzetközi műveletekben való részvétele mindenkor valamilyen együttműködés keretén belül valósul meg, amellyel közvetve vagy közvetlenül szavatolja az országunk és a Szövetség védelmét. A Magyar Köztársaság nemzeti biztonsági stratégiája[24] felsorolja azokat a kihívásokat, amelyek meghatározzák a feladatokat a biztonság megteremtése, megóvása érdekében. **A legfontosabb kihívásoknak a tárgyalt témához kapcsolódóan az úgynevezett globális kihívásokat tartom, amely csoportjába a terrorizmus, a tömegpusztító fegyverek elterjedése az instabil régiók veszélyei, az illegális migráció, a gazdasági instabilitás, az információs társadalom kihívásai és a globális természeti- és civilizációs veszélyforrások állnak.** Ezek megakadályozása és elterjedése érdekében mind a Szövetség, mind az ország olyan haderőt tart fenn, amely többnemzeti együttműködésben, hagyományos és aszimmetrikus hadviselés kereti között képes reagálni a kialakult helyzetre. A következőkben meg kell vizsgálni a Magyar Honvédség lehetséges feladatait, amely alapdokumentuma a már említett Magyar Köztársaság nemzeti katonai stratégiája és a Magyar Honvédség Összhaderőnemi Doktrínája.

Megállapítható, hogy a többnemzeti műveletek keretein belül végrehajtásra kerülő válságreagáló műveletek híradó és informatikai támogatása kiemelt szerepet kell, hogy betöltsön a kijelölt, megszervezett és létrehozott erők kiképzésében, felkészítésében, technikai eszközökkel való ellátásában és a feladat végrehajtásban egyaránt. Minden művelet parancsnoki vezetése érdekében létrehozott, telepített és üzemeltetett híradó- és informatikai rendszernek alkalmasnak kell lennie a meghatározott feladat ellátásának támogatására az információk továbbítása céljából. **A folyamatos információcsere a csapatok vezetésének egyik alapvető és legfontosabb tényezője, amely időszakos kiesése is elkerülhetetlenül zavart okozhat.** A folyamatos és megbízható összeköttetés nélkül az alegységek vezetése és

[24] 2073/2004 . (IV. 15.) Kormányhatározat a Magyar Köztársaság nemzeti biztonsági stratégiájáról

irányítása nem lehetséges. Az alárendeltekkel, az elöljárókkal és együttműködőkkel való szoros kapcsolattartás megköveteli a híradó- és informatikai erők és eszközök hozzáértő felhasználását. **Megbízható híradás nélkül a parancsnokok és törzsek nem képesek az alárendelteket vezetni, és erőkifejtésüket a feladat végrehajtására irányítani**. A kommunikáció biztosítása érdekében a szakállomány részére minden esetben meg kell határozni a pontos feladatokat, és részletes tervet kell készíteni, amely a változásokat rugalmasan kezelni. Ezek a megállapítások különösen igazak a missziós feladatok ellátására létrehozott erők vezetése esetén, amely több problémát, és szervezési nehézséget is felvet a kialakításra kerülő kommunikációs rendszer telepítése és üzemeltetése során.

A vezetés és irányítás megfelelő, minden oldalú támogatása nélkülözhetetlen a siker kivívásában. A vezetés és irányítást (C2)[25] az alábbiak szerint fogalmazza meg az MH Összhaderőnemi Doktrína : *„**Vezetés és irányítás** egymással szoros kapcsolatban lévő, de nem szinonim fogalmak. A vezetés jogi kategória, melynek gyakorlása egyszemélyi felelősséghez kötött. Az irányítás a parancsnok által gyakorolt jogkör, amely az alárendeltre átruházható. Ebben az esetben a parancsnok az irányítás kérdéseibe nem avatkozhat bele. **A vezetés és irányítás rendszerét a parancsnok és a törzs alkalmazza a hadműveletek előkészítése és végrehajtása során.**”[5]* A C2-nek megfelelően a mindenkori parancsnok, mint egyszemélyi vezető, és törzse részére olyan támogatást kell rendelkezésre bocsátani, amely minden esetben biztosítja a vezetés és irányítást. Az MH Összhaderőnemi Doktrínában foglaltaknak megfelelően: *„A **támogatás** valamely erőnek olyan tevékenysége, amellyel segít, véd, kiegészít vagy fenntart egy másik erőt. Az összhaderőnemi parancsnok támogatói viszonyt létesíthet a meglévő képességek időszakos fokozása érdekében, kiegészítő eszközökkel láthat el alárendelteket, ezáltal kombinálva a különböző eszközök hatását. **A támogatás lényegében olyan tevékenység, amely során a koordinációt végző parancsnok a rendelkezésre álló erőivel és eszközeivel segíti a feladatot végrehajtó erőket a harcfeladatok sikeres teljesítésében** anélkül, hogy a támogató erőket és eszközöket akár csak ideiglenesen is alárendelné nekik.”. […] A **harci támogatás a harcoló elemeknek nyújtott** tűztámogatásból és **egyéb műveleti közreműködésből áll.** Végezhetik az adott katonai kötelék saját szervezetszerű elemei, átalárendelt megerősítő vagy kijelölt támogató elemek. [6]*

Az MH Összhaderőnemi Doktrínában leírtakat figyelembe véve tehát a híradó és informatikai támogatás a parancsnok vezetés és irányításának olyan támogatása, amely biztosítja az alárendeltek vezetését annak folytonosságának fenntartásával. Az előző alfejezetben leírt lehetséges feladatok alapján meg kell határozni a nem háborús katonai műveletek válságreagáló műveleteinek híradó- és informatikai támogatását, mint tevékenységet. Ezek, és a katonai műveletek típusai alapján a nem háborús katonai műveletek híradása magába foglalja:

- a béketámogató műveletek híradó és informatikai támogatását;
- egyéb humanitárius műveleteknek, katasztrófák felszámolásának, kutató-mentő feladatoknak, befogadó nemzeti támogatásnak híradó- és informatikai támogatását;
- információs-, információ védelmi-, légtér-ellenőrzési műveletek híradó és informatikai támogatását.

A nem háborús katonai műveletek híradó- és informatikai támogatása tartalmazza mindazon híradó és informatikai erőket és eszközöket, amelyek békeidőszakban és az esetleges válságok kezelése során alkalmazásra kerülnek. Az előző alfejezetek alapján

[25] Command and control

megállapítható, hogy a nem háborús katonai műveletek híradó és informatikai támogatásának egyik részterülete a válságreagáló műveletek híradó támogatása, amely lehet katonai illetve nem katonai jellegű válságreagáló műveletek híradó és informatikai támogatása.

A híradás és az informatika összefonódása, konvergenciája elkerülhetetlen és szükséges a korszerű csapatvezetés megvalósítása és a növekvő igények teljesítése érdekében. Szöllősi Sándor mk. őrnagy doktori disszertációjában a következőképpen fogalmazta meg a folyamatot: *„[...] az informatika az élet minden területén, és egyre mélyebb technikai rétegekben történő megjelenése hosszabb távon a hagyományos értelemben vett távközlést magába olvasztja, átvéve annak minden szerepkörét és funkcióját.”* . *[7]* A híradás, mint a csapatvezetés alapvető eszköze az információk továbbításának biztosítására mára már nem teljes körű értelmezést ad a jelenlegi híradó és informatikai támogatásnak. A katonai informatika egyes megfogalmazások szerint a fegyveres erők eredményes működését biztosító informatikai rendszerek összessége.
A parancsnok vezetés és irányítása támogatásának érdekében híradó- és informatikai rendszer kerül megszervezésre, telepítésre és üzemeltetésre. Az előzőekben leírtak alapján, Prof. Dr. Munk Sándor ezredes a következőképpen írta le a híradó rendszer, informatikai rendszer és a híradó- és informatikai rendszer fogalmát: *„Az információs tevékenységeket megvalósító technikai rendszerekhez kapcsolódó, alapvető NATO fogalmak közé az information system, communication system, illetve a communication and information systems fogalmak tartoznak, amelyek definícióinak a NATO szabályozókban előforduló különböző változatai a következők:*
***"information system (IS):** Eszközök, módszerek és eljárások, illetve működtető személyzet, információfeldolgozási funkciók megvalósítására létrehozott rendszere.*
***"communication system (CS):** Eszközök, módszerek és eljárások, illetve működtető személyzet, információátviteli funkciók megvalósítására létrehozott rendszere.*
***"communication and information systems (CIS):** A kommunikációs és az információs rendszerek – eszközök, módszerek és eljárások, illetve működtető személyzet információátviteli, illetve információfeldolgozási funkciók megvalósítására létrehozott rendszereinek – összefoglaló megnevezése." [8]*

Hasonló megfogalmazásban értelmezhető a C2CS[26] kifejezés, amely szűkebb értelemben véve jellemzi a híradó rendszert. A C2CS tehát, a vezetés és irányítási kommunikációs (híradó) rendszer, amely a vezetés és irányításhoz szükséges információáramlást biztosítja. **A rögzítettek alapján konstatálható, hogy a NATO-ban alkalmazott kifejezések közel azonos irányelveket mutatnak, de minden kifejezés az adott szakterületre vonatkozóan ad szűkebb értelmezést.** Természetesen a szakirodalmak és más fejlett NATO hadseregek szakértői további megfogalmazásokat használnak a különböző képességű, de a híradó rendszereken alapuló rendszerek meghatározására. Ilyen a C4ISR[27] kifejezés, amely sokkal specializáltabb, összetettebb technikai eszközöket és eljárásokat csoportosít az adott feladat végrehajtásának támogatása céljából. Dr. Haig Zsolt az alábbiak szerint fogalmazta meg az információs fölény megszerzése érdekében alkalmazott C4ISR rendszerek fontosságát: *„Az információs fölény kialakulásához jelentős mértékben járul hozzá a legújabb információtechnológiai eszközök és vezetési módszerek alkalmazása. Ezért az információs fölény megszerzésének és megtartásának nélkülözhetetlen előfeltétele a korszerű, integrált vezetési, információs és felderítő rendszerek (C4ISR) széleskörű alkalmazása [...] Az információs fölény elérése és megtartása tehát szorosan függ a különböző szenzorok, felderítő*

[26] C2CS: Command Control Communication System: vezetés és irányítási híradó rendszer
[27] C4ISR: (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance): vezetés, irányítás, kommunikáció, informatika, hírszerzés, megfigyelés, és felderítés

eszközök és rendszerek minőségétől, a vezetési folyamat gyorsaságától, a végrehajtó erők képességeitől és az eszközök egységes hálózatba kapcsolásától." [9]

A fent leírtak alapján fontos kiemelnünk, hogy ezek a rendszerek nem téveszthetők össze a Magyar Honvédség által újonnan hadrendbe állított, folyamatos fejlesztéseken végbemenő C2 rendszerével. **A C2 rendszer egy komplex parancsnoki vezetés-irányítási rendszer, amely olyan információk gyűjtését, feldolgozását és tárolását hivatott kiszolgálni, mely a parancsnok döntéshozatalát könnyíti és gyorsítja meg a hadműveleti feladatok végrehajtása során.** Kovács László már 2001-ben, konferencia előadásában rámutatott ennek fontosságára, és a két különböző rendszer határvonalának „összemosódására": *„A digitális hadszíntéren már-már elválaszthatatlanok a határok, hol kezdődik parancsnoki vezetési rendszer, és hol ér véget a kommunikációs rendszer, nem beszélve a digitális integráció következményeként mindezeket támogató informatikai rendszerekről. Ma már C4I és C4ISR (Command Control Communication Computer Intelligence Surveillance Reconnaissance) rendszerekről beszélünk, amelyek mintegy alapját képezve a digitális hadszíntéren folyó katonai tevékenységnek, egy kicsit megváltoztatják mind a kommunikációról, mind a vezetésről alkotott eddigi hagyományos nézeteinket." [10]*

Tehát a válságreagáló műveletek híradó- és informatikai rendszere azon eljárások, technikai eszközök és az azokat telepítő, üzemeltető személyzet komplex rendszertechnikai összessége, amely a válságreagáló műveletekben résztvevő erők belső-, a szervezetek közötti-, a nemzeti (honi)- és a hadműveleti elöljárók irányában biztosítja az információcserét és annak feldolgozását, a többnemzeti jellegből adódó követelmények megteremtése érdekében.

Összegzés, következtetések

Napjainkban a legnagyobb veszélyt a kisméretű fegyveres összecsapások jelentik, amelyek nem csupán a régió, de a világ biztonságát is nagymértékben befolyásolják. Ezen válságok rendezése korszerű szemléletet, és korszerű fegyverzettel, haditechnikai eszközökkel felszerelt erőket követel meg a NATO minden tagállamának haderejétől. A NATO megfogalmazása alapján **a válságok kezelése érdekében összetett, többfunkciós válságreagáló műveletek kerülnek végrehajtásra, amelyek a kialakult konfliktus kezelésére, esetlegesen megelőzésére, azaz válságkezelésre irányulnak, katonai, civil és egyéb rendészeti erők és eszközök felsorakoztatásával.**

A siker kivívásának alapvető eleme, hogy **a determinált célokhoz hozzá kell rendelni a válságreagáló erők képességeit.** A washingtoni szerződés és a NATO-csúcsértekezletek meghatározták azokat a főbb irányelveket, amelyek biztosítják a sikeres missziós tevékenységeket. A legalapvetőbb képességek mellett, mint a mobilitás, rugalmasság, telepíthetőség, **a fő hangsúly a korszerű infokommunikációs eszközökkel támogatott vezetésen van.** A NATO és a nemzeti fejlesztéseknek ezen elvárásoknak kell megfelelnie, amelyek természetesen a műveleti tapasztalatok alapján folyamatosan bővülnek, pontosításra kerülnek. **Ezért a folyamatosan megjelenő új kihívásokra történő gyors és hatékony reagálás érdekében képesnek kell lenni felismerni és meghatározni az irányelveket, eszközöket, amelyek alkalmazásával elérhetőek a kitűzött célok.** Mindezek mellett a magas fokú együttműködő képesség – technikai és személyi – elengedhetetlen eleme a többnemzeti műveletek sikerének.

A vállalt kötelezettségeknek megfelelően a Magyar Honvédség részt vesz különböző nemzetközi műveletekben. Hozzájárul a szövetséges küldetések ellátásához az arra kijelölt és felkészített katonai erők felajánlásával, elősegítve a terrorizmus elleni harc katonai feladatainak ellátását. Ezek elérése érdekében folyamatos fejlesztések kerülnek végrehajtásra, amelyek a válságreagáló műveletekben szolgálatot teljesítő alegységek védelmét, és a sokrétű feladatok ellátását biztosítja. **Az alegység folyamatos vezetése érdekében olyan híradó- és informatikai rendszert kell létrehozni, amely támogatja a parancsnoki vezetést a műveletek teljes spektrumában, biztosítja az információcserét, azok feldolgozását és esetleges tárolását a művelet végrehajtásának időtartamában.** A többnemzeti műveletek során megtervezésre, megszervezésre, telepítésre és üzemeltetésre kerülő híradó- és informatikai rendszer számos követelményeknek kell, hogy megfeleljen, amelyeket elsősorban a missziós tevékenységet ellátó erők képességei határoznak meg.

Az anyagban foglaltakkal kapcsolatos főbb megállapításaink, következtetéseink:

1. **A nemzetközi műveletek sikeres végrehajtása érdekében szövetségesi és nemzeti szinten egyaránt meg kell határozni mindazon képességeket, amelyek szavatolják az összetett feladatrendszer eredményes ellátást a hadműveleti területen.**
2. **A nemzetközi- és hazai missziós tapasztalatok alapján megállapítható, hogy kisméretű, többfunkciós képességekkel rendelkező, korszerű haditechnikai eszközökkel felszerelt katonai erőket (civil képességek kiegészítésével) kell létrehozni, amelyek a kor követelményeinek megfelelően, és az elvárásokhoz igazítva viszonylag kis anyagi ráfordítással továbbfejleszthetők, és a jellegükből adódóan képesek a konfliktusok felszámolására és hazai alkalmazásra egyaránt.**
3. **A legfontosabb képességek közé tartozik a gyors bevethetőség, a moduláris felépítés, expedíciós képesség, rugalmasság és a mindezt támogató, korszerű híradó- és informatikai rendszerrel való kiegészítés.**
4. **A modern híradó és informatikai eszközökkel megszervezett híradó- és informatikai rendszer támogatja a parancsnok és törzse részére a vezetést, amely a széleskörű információcserét és információfeldolgozást lehetővé téve elősegíti a siker kivívását. Ezen rendszerek kiemelt jellemzője kell, hogy legyen a nemzetközi együttműködő képesség, amely a többnemzeti jellegből adódóan releváns.**
5. **A válságreagáló műveletek híradó- és informatikai rendszere azon eljárások, technikai eszközök és az azokat telepítő, üzemeltető személyzet komplex rendszertechnikai összessége, amely a válságreagáló műveletekben résztvevő erők belső-, a szervezetek közötti-, a nemzeti (honi)- és a hadműveleti elöljárók irányában biztosítja az információcserét és annak feldolgozását, a többnemzeti jellegből adódó követelmények megteremtése érdekében.**

Hivatkozás- és irodalomjegyzék

[1] FM 100-7 DECISIVE FORCE: The Army In Theater Operations
Chapter 8: Military Operations Other Than War ; Headquarters Department of the Army Washington, DC, 1995

[2] Rábai Zsolt: Viták az új stratégiai koncepció körül
In.: A NATO formálódó új stratégiai koncepciója és Magyarország; Konferencia előadás 2010. március 25.; ZMNE Budapest

[3] Bencze B. – Hegedüs Z. – Kolossa S. – Padányi J. – Praveczki Z. – Szternák Gy.: A Válságreagáló műveletek elmélete és gyakorlata a 21. században

Egyetemi jegyzet; ZMNE Budapest 2004; p.: 66.
[4] Szenes Zoltán: A NATO-transzformáció hatása Magyarországra, a Magyar Honvédségre
In.:http://www.hm.gov.hu/hirek/kiadvanyok/uj_honvedsesegi_szemle/a_nato-transzformacio
[5] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás
Honvédelmi Minisztérium kiadványa, 2010; p.: 52.
[6] Ált/27 Magyar Honvédség Összhaderőnemi Doktrina 3. kiadás
Honvédelmi Minisztérium kiadványa, 2010; p.: 57-59.
[7] Szöllősi Sándor okl. mk. őrnagy: Konvergáló hálózatok fejlődési trendjei, a technikai alkalmazhatóság kérdései a Magyar Honvédség infokommunikációs rendszerében (doktori PhD értekezés) Budapest, 2007 p.: 6.
[8] Dr. Munk Sándor: Katonai informatika III. ZMNE, 126. oldal
[9] Dr. Haig Zsolt mk. alezredes: Az információs műveletek, a sigint és az elektronikai hadviselés kapcsolatrendszere
In.: Felderítő Szemle, VI. évfolyam különszám; Budapest, 2007 február, p. 30.
[10] Kovács László: Gondolatok napjaink technológiájáról és a digitális hadszíntér kapcsolatáról
In.: http://www.zmne.hu/tanszekek/ehc/konferencia/april2001/kovacs.html