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)