Védelmi infokommunikációs hálózatok és rendszerek
-szakmai felkészítés-

Defence infocommunication network and system
-professional training-

Farkas Tibor[1]

Absztrakt

A vezetés és irányítási tevékenységek infokommunikációs támogatása a különböző nemzeti- és nemzetközi válsághelyzetek, vészhelyzeti események során kiemelt jelentőséggel bír. A különböző szintű kormányzati vezetés és a védelmi szervezetek (rendőrség, katasztrófavédelem, honvédség…) közötti együttműködés kulcskérdése a rendelkezésre álló infokommunikációs rendszer, valamint a magasan képzett felhasználók és az üzemeltető szakállomány. Jelen közleményben a szerző behatárolja a szakállomány képzéséhez szükséges alapvető ismeretanyagot. „Jelen közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült”

Kulcsszavak: *Védelmi szektor, infokommunikáció, kormányzati IKT rendszerek, felkészítés*

Abstract

The infocommunication support of command and control in different national and international level crises, danger situations and other emergency events is priority. The infocommunication system and the high educated users and maintenance staff are the key element of the cooperation between each level of defence organisations (police, disaster management, army, etc.) In this publication the author specifies the fundamentals and basic knowledge material of a possible training for users and operators. “This article was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.”

Keywords: *Defence sector, infocommunication, governmental ICT system, training*

Bevezetés

A szerző korábbi közleményeiben (Farkas & Hronyecz, 2018) (Farkas & Prisznyák, 2017) megvizsgálta és elemezte mindazon tevékenységeket, amelyek során a különböző védelmi és kormányzati szervezetek együttműködése kulcsfontosságú a nemzeti biztonság megteremtésében, annak folyamatos fenntartásában. A különböző katasztrófahelyzetek mellett a mindennapi éltben is szükséges a kormányzati, közigazgatási szervezetek közötti együttműködés, amely biztosítja a lakosság széleskörű közigazgatási és egyéb kiszolgálását, támogatását, amely a fenntartható állam folytonosságának egyik alapvetése.

A magyar kormány elismerve a hazai IKT (Infokommunikációs Technológia) ágazat jelentőségét, és annak pozitív hatását a gazdasági és társadalmi fejlődésre, a 1069/2014. (II. 19.) Korm. határozatban elfogadta a „Nemzeti Infokommunikációs Stratégia 2014 – 2020” dokumentumot, amelynek célját az alábbiak szerint határozza meg: *„Jelen stratégia célja, hogy átfogó képet adjon a magyar információs társadalom és IKT-piac jelenlegi helyzetéről, megfogalmazza a kívánatos célállapotot, és a 2014-20-as uniós tervezési ciklussal egybeeső időtávra szakmai irányokat, fejlesztési súlypontokat jelöljön ki az infokommunikációs területre vonatkozóan.”* (Magyar Kormány, 2014, p. 4)

[1] Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Híradó Tanszék, egyetemi docens
ORCID: 0000-0002-8868-9628; farkas.tibor@uni-nke.hu

Természetesen ez a fejlesztési, fejlődési tendencia igaz kell, hogy legyen az összes kormányzati és közigazgatási szervezet tevékenységére, azok infokommunikációs hálózatára és szolgáltatásaira is egyaránt.

Az előzőkhez hasonlóan a védelmi szervezetek infokommunikációs rendszereinek szintén biztosítania kell a megfelelő szintű hozzáférést az adatokhoz, információkhoz a résztvevő szervezetek teljes állománya részére az adott művelet, feladat teljes spektrumárban. Az infokommunikációs rendszereknek tehát olyan szintű támogatást kell nyújtaniuk, amelyek képesek a folyamatos információáramlás biztosítására, kiszolgálja a felhasználókat, és megteremti az együttműködés lehetőségét a különböző szervezetek között, amelyet az interoperabilitási képességük biztosít. Természetesen ezek a legalapvető képességei a hálózatoknak, amelyeket további képességekkel kell kiegészíteni, ezek közül az egyik a biztonság. A hálózatok, az információk biztonsága napjaink egyik legjelentősebb kritériumkövetelménye, amely helyi és központi, centralizált védelemmel kell megvalósítani. A másik követelmény a magasan képzett, széleskörű rendszerismerettel rendelkező üzemeltető állomány, melynek tagjai képesek a rendszer megszervezésére és a felhasználás teljes ideje alatt az üzemeltetésre. Ez utóbbi megvalósításának egyik alapvető eleme a megfelelő szakmai alappal rendelkező szakemberek továbbképzése a közigazgatási és a védelmi szektor infokommunikációs rendszereinek üzemeltetése területén. Ennek megfelelően az üzemeltető és felhasználó állomány alapszintű felkészítését már az egyetemi alapképzés alatt meg kell kezdeni. A Nemzeti Közszolgálati Egyetem (a továbbiakban: NKE) ennek kiváló bázisa lehet, mivel a védelmi szektor minden szervezetének különböző szintű képzése, felkészítése jelen van az egyetemen. *„Létrehozása megteremtette az egységes közszolgálati alapképzések strukturális, intézményi és személyzeti feltételeit. Az egyetem elsődleges célja a polgári közigazgatás, a rendvédelem, a honvédelem és a nemzetbiztonsági szolgálatok személyi állományának magas színvonalú képzése, ezzel együtt az egységesülő közszolgálati életpályák közötti átjárhatóság megteremtésének támogatása a képzések oldaláról.”* (Magyarország Kormánya, 2014, p. 20)

Az NKE vízióját az NKE Intézményfejlesztési Terv az alábbiak szerint határozza meg: „*Az NKE „Az együttműködés Egyeteme” („University of cooperation”), a társadalmi igények, nemzetstratégiai-kormányzati célok és az egyetemi autonómia közötti hatékony együttműködés modellje. Az IFT középtávú víziója, hogy az NKE legyen*

- *Magyarország egyik legjobb és legvonzóbb egyeteme;*
- *a magyar közszolgálat fejlesztésének, a közszolgálati életpályának stabil oktatási és kutatási bázisa;*
- *a hazai és a külhoni magyar nyelvű felsőoktatás elkötelezett támogatója;*
- *Európa és a világ vezető egyetemeivel szövetségben aktív részese a nemzetközi felsőoktatási és tudományos kapcsolatoknak.”* (Nemzeti Közszolgálati Egyetem, 2017, p. 4)

Az egyetemnek jelentős feladata van mind a közigazgatás, mind a védelemigazgatás területén a képzés és felkészítés viszonyrendszerében. Az előzőekben tárgyalt védelmi tevékenységeket irányító védelmi igazgatás részét képezi a közigazgatásnak, így a védelmi szervezetek (honvédség, rendőrség, katasztrófavédelem, …) felkészítése is az egyetem feladatai közé tartozik. *„A védelmi igazgatás a közigazgatás részét képező feladat- és szervezeti rendszer, továbbá az állam védelmi feladatainak megvalósítására létrehozott, valamint e feladatra kijelölt közigazgatási szervek által végzett tevékenységek összességeként magában foglalja a különleges jogrendre történő felkészülést, a különleges jogrendi időszakok és helyzetek honvédelmi, polgári védelmi, katasztrófavédelmi, védelemgazdasági, lakosság-ellátási feladatainak tervezésére, szervezésére, a feladatok végrehajtására irányuló állami tevékenységeket. […]. A védelmi igazgatás feladatainak koordinált és hatékony végrehajtása*

érdekében elengedhetetlen az érintett szervezetek közötti megfelelő színvonalú, biztonságos információáramlás, kommunikáció. […] A jövő kiemelten fontos stratégiai feladata a megkezdett fejlesztés kiterjesztése […] ezáltal garantálva a védelmi igazgatási feladatok megfelelő ellátásához nélkülözhetetlen, egységes alapú, hatékony információáramlást az ország egészére nézve." (Magyarország Kormánya, 2014, pp. 14-15)

Mindezek jól alátámasztják, hogy a NKE, mint a közigazgatási, kormányzati feladatokat ellátó szakemberek képzésének, felkészítésének és továbbképzésének bázisa.

Összefoglalva az előzőekben leírtakat az NKE által gondozott képzéseken magas színvonalú, a közigazgatásban és a védelemigazgatásban egyaránt helytálló szakembereket képeznek a felsőoktatás minden szintjén, különös figyelmet fordítva a további képesítések megszerzésére, a folyamatos tanulás és képzés figyelembe vételével. A képzések minden esetben megfelelnek az Nftv.-ben leírtaknak, az abban megfogalmazottaknak eleget tevő képesítést adnak, biztosítva a közszolgálati képzések folytonosságát, teljesen beépülve a továbbképzés rendszerébe.

A szakmai felkészítés alapjai

A legjelentősebb kutatási irányvonalakat, kutatási prioritásokat, amelyek az NKE által gondozott tudományágakban kerültek meghatározásra, a „Kutatási, fejlesztési és innovációs stratégia 2016-2020" dokumentum tartalmazza az alábbiak szerint, a hadtudományok vonatkozásában (Nemzeti Közszolgálati Egyetem, 2016, pp. 35-38):

- hadelmélet és hadviselés;
- stratégiakészítés és védelmi tervezés;
- a Magyar Honvédség jövőképe 2025;
- honvédelem és jó kormányzás;
- országvédelem;
- humán és személyügyi munka;
- nemzetközi válságkezelés és békefenntartás;
- hadtörténelem, hagyományőrzés, civil- katonai kapcsolatok.

A felsoroltak rövid és középtávú megvalósítása közvetlenül szolgálja Magyarország honvédelmi érdekeit és feladatait a hadtudomány előtt álló új kihívásoknak való megfelelést a védelempolitika és a haderőfejlesztés területén. A kutatási területek részletes meghatározását a Hadtudományi Szemlében megjelent cikk tartalmazza. (Boda J. et.al, 2016)

A Hadtudományi Kollégium mellett a Műszaki Tudományok Kollégium kiemelten kezeli a műszaki jellegű kutatásokat, azon belül pedig az infokommunikációs technológiákat. A műszaki tudományterületen a vonatkozó kutatási irányelveket az alábbiak szerint lehet meghatározni (Bleszity [et al.], 2016):

- digitális állam;
- kiberbiztonság;
- környezetbiztonság;
- katasztrófavédelem;
- védelmi célú műszaki kutatások;
- logisztika és közlekedés.

A rendészettudományok területén szintén jelentős kutatási területek kerültek megfogalmazásra, amelyeket négy fő irányban határoztak meg: *„A modern rendészet igényli a tudományok támogatását, a rendészettudomány pedig nem művelhető a gyakorlat ismerete nélkül. A tervezés során négy fő irányt határoztunk meg:*

- *a rendészeti közjog,*

- *a rendészeti szervezetrendszer,*
- *a rendészet működése,*
- *és a rendészet személyzete."* (Nemzeti Közszolgálati Egyetem, 2016, p. 66)

Az eddigiek alapján megállapítható, hogy az államtudományok és a műszaki tudományok kapcsolata szoros összefüggésben, egymást kiegészítve van jelen az NKE kutatási tevékenységében. A tárgyalt kutatási téma tehát jól illeszkedik az NKE kutatási területeihez, több kutatói részterületet is felölel a hatékony oktatás és a tudáskompetencia létrehozásával, amely az egyetem további megerősödését támogatja nemzeti és nemzetközi viszonylatban. Megítélésem szerint tehát a vizsgált, kutatott téma jól beilleszthető az NKE kutatási portfóliójába, ezen felül a kutatási eredmények tovább hasznosíthatók az államtudományok és a műszaki tudományok területén egyaránt.

A védelmi infokommunikációs infrastruktúra

A korszerű infokommunikációs eszközök, rendszerek alkalmazása elengedhetetlen az információ feldolgozásához és továbbításához, valamint a kormányzati irányítás és a szervezetek tevékenységének vezetése megvalósításához. Ahhoz, hogy a folyamatosan változó, bővülő kihívásoknak meg tudjunk felelni, elengedhetetlen a modern információs eszközök és rendszerek alkalmazása az irányítás és vezetés hatékony biztosítása, valamint a tevékenységek sikeres végrehajtása érdekében.

Magyarországon a kormányzati és a védelmi tevékenységet végrehajtó szervezeteinek infokommunikációs hálózata nem alkot egységes képet, mivel egyes elemei központi üzemeltetés alatt állnak, bizonyos részei pedig az adott szervezet felügyelete alatt. Ez természetesen alrendszereit és az egyes funkcióit (pl. információbiztonság) tekintve eltérő lehet, valamint vegyes felügyeletet igényel.

Az információtechnológia fejlődésével folyamatosan változnak mindazon lehetőségek, amelyek egy adott infokommunikációs rendszer nyújt a felhasználók számára, valamint azok a lehetőségek, amelyek a megbízható rendszerüzemeltetést biztosítják. Ennek megfelelően a kiszolgált szervezetek megbízhatósága és rendelkezésre állása is jelentősen javulhat az elvárásoknak megfelelően.

A szerző korábbi kutatásai és azok eredményei bizonyítják, hogy a kormányzati infokommunikációs rendszereknek magas rendelkezésre állással, kiemelt biztonsággal és nagyfokú együttműködési képességekkel kell rendelkezniük annak érdekében, hogy az alaprendeltetésükből eredő feladataikat el tudják látni, valamint hogy a különböző védelmi szervezetek képesek legyenek együttműködni, egymást kiszolgálni az adott védelmi tevékenységek során. (Farkas & Hronyecz, 2017), (Farkas, 2016) (Farkas & Hronyecz, 2016)

Ennek megfelelően a kapcsolódó kutatások során az alábbi rendszerek, alrendszerek feldolgozása szükséges:

- a szolgáltatásokat biztosító infokommunikációs rendszerek;
- az egyes, speciális üzemeltetésű és rendeltetésű alrendszerek;
- a rendszerek nyújtotta szolgáltatások;
- a rendszereket alkotó technikai eszközök és technológiák.

A kormányzati szintű irányítás és vezetés a kormányzati infokommunikációs rendszerek felhasználásával kerül végrehajtásra, amelyet a 346/2010. (XII.28) Korm. rendelet a kormányzati célú hálózatokról, valamint a 88/2016. (VII. 13.) Korm. rendelet a kormányzati célú hálózatokról szóló 346/2010. (XII. 28.) Korm. rendelet módosításáról című dokumentumok határoznak meg alapvetően. A rendelet alapján kormányzati célú hálózatnak minősül az 1. mellékletében felsorolt elektronikus hírközlő hálózatok, amelyek a következők:

- Nemzeti Távközlési Gerinchálózat (korábban Elektronikus Kormányzati Gerinchálózat);
- Egységes Digitális Rádiótávközlő Rendszer;
- Zártcélú Rendészeti Hálózat;
- Köznet;
- K-600/KTIR Hírközlési és Informatikai Rendszer.

A kormányzati célú rendszerek másik, elkülönített eleme a *Magyar Honvédség hálózata*, amely teljesen más szervezési elven alapul, illetve nem az NTG-t használja felületként. Függetlenül működik tőle, de a hálózat beintegrálását biztosítja a kormányzati rendszerbe egy kapcsolódási felületen. Ezáltal tehát a teljesen eltérő felépítésű és szolgáltatást nyújtó rendszerről van szó, amely biztosítja a honvédség és szervezetei részére az infokommunikációs szolgáltatásokat.

Látható tehát, hogy nagy számú hálózatok vannak jelen a kormányzati infokommunikációs rendszerben, amelyek széleskörű támogatást kell, hogy nyújtsanak a felhasználók részére a különböző szolgáltatások elérése céljából. Megítélésem szerint a védelmi feladatok ellátása során az üzemeltető szakállomány ezen elemek ismeretének birtokában megfelelő szélességben biztosítják a felhasználók részére a magas fokú rendelkezésre állást.

Ennek megfelelően az alábbi célrendszereket, szolgáltatásokat és infokommunikációs képességeket lehet meghatározni, illetve az üzemeltető állománynak ezen rendszereket kell folyamatosan fenntartaniuk, egyes esetekben pedig az ezekből nyert információkat kell továbbítaniuk a megfelelő ún. belső vagy külső együttműködő szervezeteknek. (Az alábbi felsorolás a teljesség igénye nélkül kerül feltüntetésre.)

A *Magyar Honvédség* infokommunikációs hálózata mind a felépítésében, mind üzemeltetésében nagymértékben eltér a többi kormányzati hálózattól. Megítélésem szerint minimálisan az alábbi elemeket, alrendszereket lehet elkülöníteni:

- MH távhívó hálózata;
- MH internet és intranet szolgáltatása;
- bérelt vonali szolgáltatások;
- műholdas szolgáltatások (VSAT, műholdas telefon);
- MH C2 (Command and Control: Vezetés és Irányítási) rendszer;
- Blueforce Tracking System (Saját Erő Követő Rendszer);
- MH KGIR (Költségvetés Gazdálkodási Információs Rendszer) rendszer;
- tábori (telepíthető) alaphírhálózat;
- VTC rendszer (Video Teleconferencing: Videókonferencia szolgáltatás);
- JTRS (Joint Tactical Radio System: Összhaderőnemi Harcászati Rádiórendszer);
- NIAR (NATO Irodaautomatizálási Rendszer);
- levelező rendszer;
- Magyar Honvédség Védett Vezetési és Irányítási Rendszer;
- határvédelmi rendszer informatikai szolgáltatásai.

A másik védelmi szervezet a *Rendőrség* szintén rendelkezik vezetékes és rádiófrekvenciás hírközlési, kapcsolástechnikai, távközlési és távadat-, informatikafeldolgozási, frekvenciahasználati, rejtjel-felügyeleti és ehhez kapcsolódó biztonságtechnikai feladatokkal, amelyek szintén számos, speciális célrendszert tartalmaznak, melyek közül néhányat az alábbi felsorolás tartalmaz (Robotzsaru integrált ügyviteli, ügyfeld. és elektronikus iratkezelő rendszer egységes és kötelező használatáról, jogosultsági rendjéről, az adatvédelem, valamint a rendszerfejl. előírásairól szóló 18/2011. (IX. 23.) ORFK ut. módosításáról, 2017):

- Robotzsaru (ügyviteli, ügyfeldolgozási és elektronikus iratkezelő rendszer) és alrendszerei;
- VÉDA (közlekedés ellenőrző rendszer);

- elektronikus feldolgozórendszer;
- AFIS (automatizált ujj és tenyérnyomat azonosító rendszer;
- ROVER (Rendőrségi Oktató-Vizsgáztató Egységes Rendszer);
- NOVA Integrált Rendszer (NIR-bejelentő portál);
- egyéb figyelő és érzékelő rendszerek

Az *Országos Katasztrófavédelmi Főigazgatóság* összetettségéből, komplex feladatrendszeréből adódóan általános és speciális célrendszerekkel rendelkezik. Távközlési, műveletirányítási, informatikai, valamint az egész országot lefedő mérő-, érzékelő-, lakosságriasztó-rendszereket tart fenn, végzi az ezekkel összefüggő adatkezelést. (Belügyminisztérium, 2012) Az alábbi alrendszerek tartoznak a legfontosabbak közé:

- katasztrófavédelmi informatikai rendszer;
- nagyobb tavaknál elhelyezett viharjelző rendszerek;
- lakossági tájékoztató rendszer;
- MoLaRi (Monitoring és Lakossági Riasztó rendszer)
- Marathon Terra (zártrendszerű kommunikációs csatorna)
- katasztrófavédelmi célú segélyhívó és információs rendszerek;
- különböző lakossági és egyéb riasztó rendszerek;
- ONER (Országos Nukleáris Baleset Elhárító Rendszer)
- OSJER (Országos Sugárfigyelő, Jelző és Ellenőrző Rendszer)
- egyéb katasztrófavédelmi információs rendszerek, vészhelyzeti és tájékoztató rendszerek.

A három kiemelt fontosságú szervezet mellett a *Büntetésvégrehajtás Országos Parancsnoksága* által felhasznált rendszerek az alábbiak lehetnek:

- számítástechnikai rendszerek;
- távközlési és biztonságtechnikai rendszerek;
- FŐNIX (nem minősített adatkezelést biztosító fogvatartotti nyilvántartás);
- FANY (Fogvatartotti Alapnyilvántartói Rendszer);
- biometrikus azonosítást megvalósító rendszerek;
- Marathon Terra (zártrendszerű kommunikációs csatorna);
- egyéb nyilvántartó rendszerek és technológiák.

Az előzőekben leírtak mellett más kormányzati, védelmi szervezetek által alkalmazott infokommunikációs, információs rendszert is be lehet illeszteni egy olyan tudástárba, amely annak érdekében kerül kialakításra, hogy az üzemeltető szakemberek és a felhasználók kellő szélességben átlássák az alkalmazott rendszereket a hatékonyság fokozása érdekében. A kormányzati, közigazgatási infokommunikációs rendszerek folyamatos fejlesztése, annak elterjedése biztosítja a társadalmi és szervezeti elvárások és igények kiszolgálását, valamint a jólétet. Ezáltal tehát a *kormányzati és önkormányzati rendszerek is fontos szerepet látnak el a tárgyalt tevékenység támogatásában.*

A felsorolt alrendszerek ismertetése mellett kiemelt hangsúlyt kell fektetni a különböző információbiztonsági kérdésekre is, amelyek mind a teljes hálózatot, mind a különböző alrendszereket is érintik.

A védelmi infokommunikációs hálózatokhoz kapcsolódó szakmai felkészítés

A védelmi tevékenységek humán oldalról történő támogatásának egyik jelentős területe a különböző, kapcsolódó szakmai felkészítés, ismeretmegosztás, amely megteremti az infokommunikációs támogatás alapjait. A védelmi infokommunikációs hálózatokhoz kapcsolódó szakmai felkészítés célja, hogy megismertesse a képzésben résztvevőket a

kormányzati infokommunikációs technológiák, rendszerek és hálózatok felépítésével és üzemeltetésével, valamint a különböző hálózatok közötti együttműködés megvalósításának lehetőségeiről és az infokommunikációs kompetenciafejlesztés jelentőségével, lehetőségeivel.

Egy lehetséges, kialakításra kerülő képzés tudásanyagának megismerését követően az ismeretek birtokában képesek lesznek az adott infokommunikációs szakterületen belül megjelenő szervezési, tervezési feladatok megértésére, az esetlegesen felmerülő problémák értelmezésére, valamint képesek lesznek a kor új kihívásainak és követelményeinek eleget tenni. Mindezek mellett olyan tudásra tesznek szert, amely birtokában megalapozott döntéseket tudnak hozni a szervezés, tervezés és üzemeltetés területén az ICT kompetencia fejlesztésének révén.

A felkészítést elvégző hallgató ennek megfelelően képes lesz:

- megérteni a kormányzati infokommunikációs rendszer szükségességét, helyét szerepét a nemzeti irányítás rendszerében;
- megérteni és felismerni, valamint magas szinten alkalmazni az egységes kormányzati infokommunikációs rendszer fontosságát, működésének jelentőségét;
- üzemeltetni az infokommunikációs rendszereket;
- átlátni a kormányzati szektor irányításának infokommunikációs támogatását, az egyes hálózatok sajátosságát és az együttműködés lehetőségét;
- magas szintű szakmai ismeretekkel tovább emelni a szektor infokommunikációs támogatását;
- a fejlesztési folyamatokba (megrendelés-fejlesztés-tesztüzem-képzés-átadás-monitoring) történő bedolgozásra, illetve részt venni azokban.

A képzés célcsoportja azok a hallgatók, akik a kormányzati (közigazgatási, honvédelmi, katasztrófavédelmi, büntetésvégrehajtási, rendőrségi, nemzetbiztonsági, stb.) infokommunikációs rendszereket felhasználják, esetleg üzemeltetik. Az ismeretanyagnak ötvöznie kell a konstruktív szervezési és tervezési módszereket és eljárásokat, valamint a kormányzati infokommunikációs szektor rendszereit, alrendszereit, ezáltal biztosítva a széleskörű ismeretanyag megszerzésének lehetőségét. A képzés minden esetben olyan szakemberek bevonásával valósulhat meg hatékonyan, akik speciális felkészültséggel, a szakterületen szerzett több éves szakmai gyakorlattal, fejlesztési tapasztalatokkal rendelkeznek.

A képzés ismeretanyaga jól elkülöníthető részterületből, ismeretkörből kell, hogy álljon, az általános védelmi és kormányzati ismeretektől kezdve a speciális célrendszerek üzemeltetéséig, az alábbiak szerint:

1. Kormányzati, közigazgatási, védelemigazgatási szervezetek tevékenysége, rendeltetése és feladatai

A magyar kormányzati rendszer és annak részterületei, szervezetei kiemelten fontos területe a képzésnek, hiszen ezek ismerete szükséges a vezetési és irányítási tevékenységek infokommunikációs támogatásához. Megfelelő alapismeretekkel kell rendelkeznie egy felhasználónak, üzemeltető szakembernek annak érdekében, hogy megfelelően átlássa az adott szervezet tevékenységéhez és irányításához szükséges leghatékonyabb rendszereket és hálózatokat, illetve azok tovább fejlesztésének lehetőségeit.

2. Alkalmazott infokommunikációs technológiai ismeretek

A második részterület a szakmai alapozó ismeret témaköre, amely napjaink legfontosabb technológiáinak, módszereinek és ismereteinek összefoglalását mutatja be. A témakör jelentőségét az határozza meg, hogy a képzésen résztvevők várhatóan különböző mélységű szakmai ismeretekkel rendelkeznek majd, így kiemelten fontos egy egységes kép kialakítása, amely az alapvető fogalmaktól kiindulva mutatja be a technológiákat és egyéb kapcsolódó alkalmazásokat. A részterület ismeretanyagához kell tartoznia a különböző szakmai menedzsment rendszereknek (rendszerek, alkalmazások, módszerek és ajánlások), az IKT-nak,

információs infrastruktúráknak és az alapvető kibervédelemnek, információbiztonságnak. Mivel az átviteli technológiák eltérőek a kormányzati rendszerekben is, így a spektrum menedzsment kiemelt részét kell, hogy képezze az ismeretkörnek.

3. Kormányzati infokommunikációs rendszerek

A képzés tananyagának harmadik, egyben legmeghatározóbb részterülete a konkrét szakmai ismeretek bemutatása. Az alapozó technológiai és hálózatmenedzsment területre építve be kell mutatni a kormányzati szintű infokommunikációs rendszereket, hálózatokat, azok felépítését és a legújabb műszaki megoldásokat, hálózat-, szolgáltatás- és alkalmazásfejlesztési elképzeléseket. Fontos, hogy az pontos tudás mellett a várható fejlesztéseket, preferált hálózattechnológiákat is ismertetni kell a társadalmi, közigazgatási, védelmi, EU-s fejlesztéseket. Cél, hogy a tudásanyag támogassa az egységes, központi közigazgatási és védelmi szolgáltatások infrastrukturális feltételeit az infokommunikációs infrastruktúra és az üzemeltetés területén, valamint megalapozza a kormányzati infokommunikációs szolgáltatások magas színvonalú biztonságának megteremtését.

A kormányzati szintű hálózatok ismertetésénél minden esetben ki kell térni a jogszabályi háttérre, a hálózati szerkezetre, a célokra és feladatokra, valamint az üzemeltetés részterületeire egyaránt. A hálózatfelügyelet és a hálózatbiztonság, valamint az interoperabilitás kérdésköre szintén jelentős területet ölel fel a tananyagban. A közös, egységes részt követően be kell mutatni a különböző alrendszereket, mint a rendőrség, honvédség, katasztrófavédelem, büntetésvégrehajtás és a közigazgatáshoz kapcsolódó hálózatokat, azok felépítését, működését, üzemeltetését és képességeit, kiemelve a hálózatokhoz tartozó speciális célrendszerekkel. A tananyag felépítése során törekedni kell arra, hogy az eltérő szervezetek hálózatainak ismertetése hasonló elven működjön a könnyebb megértést támogatva.

Összefoglalva, a képzés átfogó, komplex ismeretet nyújt a kormányzati szintű infokommunikációs rendszerekről, azok üzemeltetéséről, amely minden esetben a kapcsolódó törvényeket, szabályzókat, határozatokat figyelembe véve dolgozza fel az ismeretanyagot, kiegészítve a szakmai tapasztalatokkal és a legfrissebb vonatkozó kutatási eredményekkel. A képzés fontosságát tovább növeli, hogy az infokommunikációs rendszerek hozzáadott értéke jóval magasabb, mint más ágazatok esetében.

Következtetések

A különböző válság- és katasztrófahelyzetek felszámolása során közösen tevékenykedő szervezetek minden esetben együttműködve, de önálló feladatok végrehajtását látják el a saját speciális alaprendeltetésüknek megfelelően. Az egymást kiegészítő tevékenységek összehangolt vezetést és irányítást követelnek meg, amely magas szakmai tudást, felkészültséget kívánnak meg mind a vezetői, parancsnoki, mind a végrehajtó állománytól. A másik az együttműködést támogató képesség, a vezetést és irányítást támogató IKT rendszerek alkalmazása. A szakmai szervezetek rendelkeznek saját speciális célhálózatokkal, alrendszerekkel, amelyek kialakítása minden esetben a saját feladatellátásra lett optimalizálva. Ezek a rendszerek megfelelően működnek, a legtöbb esetben megfelelően támogatják az adott szervezet tevékenységét, vezetés és irányítását.

Meglátásom szerint, egy közös, a tevékenységeket támogató autonóm infokommunikációs rendszer kialakítására nincs sem szükség sem lehetőség, hanem a megfelelően összehangolt együttműködést, és az időbeni információmegosztást kell biztosítani. A korábbiakban vizsgált hazai katasztrófaesemények, valamint a migrációs helyzetre történő reagálás ezt alá is támasztja. Ennek megfelelően véleményem szerint, a katasztrófa és egyéb válsághelyzetek felszámolásának hatékonysága megteremthető és tovább növelhető:

- összehangolt vezetés és irányítással;
- a korszerű technikai, IKT eszközök alkalmazásával;

- a különböző adatbázisokból nyert információk megosztásával;
- és a felhasználók valamint az üzemeltetők magas szintű felkészítésével.

A műveleti területen végrehajtott tevékenység vezetése mellett a magasabb szintű irányítást biztosító kormányzati IKT rendszerek esetében meg kell vizsgálni, hogy esetleges rendszerkiesés esetén (pl. terrortámadás) milyen tartalék rendszerek képesek üzemelni, amelyek felhasználásával a rendvédelmi és egyéb szervezetek képesek kommunikálni, információt cserélni. Meglátásom szerint ebben az esetben kiváló lehetőséget nyújt az elkülönült Magyar Honvédség zártcélú hálózata, amely az elkülönült elemek között biztosítja az információáramlást.

Összességében tehát kiemelten fontos egy meghatározó tudásanyag összeállítása, amely biztosítja a felkészítését a védelmi szektor állományának.

A kormányzati infokommunikációs felkészítés tehát minden esetben beilleszthető az NKE képzési rendszerébe, stabil és meghatározó részterületté válhat a képzéseken belül. Az eddig leírtaknak megfelelően a tananyag és az ismeretanyag megítélésem szerint az alábbi stratégiai irányelveket kell, hogy szem előtt tartsa:

- konstruktív tanítási módszereket alkalmazó;
- üzemeltetésorientált;
- egységes;
- szabványos,
- fenntartható;
- biztonságos;
- tudásközpontú.

Irodalomjegyzék

Belügyminisztérium, 2012. *A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság Szervezeti és Működési Szabályzata.* 2012 szerk. Budapest: BM.

Bleszity [et al.], 2016. Műszaki kutatások és hatékony kormányzás. *Hadmérnök,* pp. 221-242.

Boda J. et.al, 2016. Fókusz és együttműködés. A hadtudomány kutatási feladata. *Honvédségi Szemle,* pp. 3-19.

Farkas, T., 2016. A katasztrófavédelmi és válságkezelési tevékenységek általános elemzése az irányítás és az infokommunikációs támogatás tükrében. *Hadmérnök,* szeptember, Volume 3, pp. 135-148.

Farkas, T. & Hronyecz, E., 2016. Basic information needs in disaster situations (capabilities and requirements). In: B. Enikő, ed. *Proceedings of the XXI-th International Scientific Conference of Young Engineers.* Kolozsvár: s.n., pp. 153-156.

Farkas, T. & Hronyecz, E., 2017. Info-Communication Areas of Modernizing Field C2 Systems and Co mmand Posts in the Interest of Successful Home Defense- Peace Operations- and Disaster-Managem ent Tasks. In: S. Anikó, ed. *IEEE 15th International Symposium on Intelligent Systems and Informatics : SISY 2017.* Szabadka: s.n., pp. 353-358.

Farkas, T. & Hronyecz, E., 2018. *Info-communication experts in the defence sector:Vocational training program.* Cluj, Erdélyi Múzeum-Egyesület, pp. 75-79.

Farkas, T. & Hronyecz, E., 2018. *Info-communication experts in the defence sector:Vocational training program.* Cluj, Erdélyi Múzeum-Egyesület, pp. 75-79.

Farkas, T. & Prisznyák, S., 2017. Kormányzati célú infokommunikációs hálózatok: A rendészeti szervek infokommunikációs rendszere. *Hadtudományi Szemle,* 10.(4.), pp. 583-596.

Magyar Kormány, 2014. *Nemzeti Infokommunikációs Stratégia 2014-2020.* Budapest: ismeretlen szerző

Magyarország Kormánya, 2014. *Közigazgatás- és Közszolgáltatás-fejlesztési stratégia 2014-2020.* Budapest: ismeretlen szerző

Nemzeti Közszolgálati Egyetem, 2016. *Kutatási, Fejlesztési és Innovációs Stratégia 2016-2020,* Budapest: NKE.

Nemzeti Közszolgálati Egyetem, 2017. *Intézményfejlesztési Terv 2015-2020.* [Online] Available at: https://www.uni-nke.hu/document/uni-nke-hu/IFT_170615_1.pdf [Hozzáférés dátuma: 05 04 2019].

Robotzsaru integrált ügyviteli, ügyfeld. és elektronikus iratkezelő rendszer egységes és kötelező használatáról, jogosultsági rendjéről, az adatvédelem, valamint a rendszerfejl. előírásairól szóló 18/2011. (IX. 23.) ORFK ut. módosításáról (2017).