HADTUDOMÁNYI SZEMLE
13. évfolyam (2020) 1. szám 37–48. • DOI: 10.32563/hsz.2020.1.3

Farkas Tibor[1]

Védelmi infokommunikációs hálózatok és rendszerek – szakmai felkészítés

Defence Infocommunication Network and System – Professional Training

Absztrakt

A vezetési 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.

Kulcsszavak: *védelmi szektor, infokommunikáció, kormányzati IKT-rendszerek, felkészítés*

Abstract

The infocommunication support of command and control in different national and international crises, danger situations and other emergency events is a priority. The infocommunication system and the highly educated users and maintenance staff are the key elements of the cooperation between the government and each level of defence organisation (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.

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

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

Bevezetés

A szerző korábbi közleményeiben[2] 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 életben is szükséges a kormányzati, közigazgatási szervezetek közötti együttműködés, amely biztosítja a lakosság széles körű közigazgatási és egyéb kiszolgálását, támogatását, amely a fenntartható állam folytonosságának egyik alapvetése.

A magyar kormány elismerve a hazai IKT (Infokommunikációs Technológia, a továbbiakban: IKT) ágazat jelentőségét és annak pozitív hatását a gazdasági és társadalmi fejlődésre, az 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."[3]

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

Az előzőekhez hasonlóan a védelmi szervezetek infokommunikációs rendszereinek szintén biztosítania kell a megfelelő szintű hozzáférést az adatokhoz, információkhoz a részt vevő szervezetek teljes állománya részére az adott művelet, feladat teljes spektrumában. Az infokommunikációs rendszereknek tehát olyan szintű támogatást kell nyújtaniuk, amely képes a folyamatos információáramlás biztosítására, kiszolgálja a felhasználókat és megteremti az együttműködés lehetőségét a különböző szervezetek között, amelyet az interoperabilitási képességük biztosít. Természetesen ezek a legalapvetőbb képességei a hálózatoknak, amelyeket további képességekkel kell kiegészíteni, ezek közül az egyik a biztonság. A hálózatok, az információk biztonsága napjaink egyik legjelentősebb kritériumkövetelménye, amelyet helyi és központi, centralizált védelemmel kell megvalósítani. A másik követelmény a magasan képzett, széles körű rendszerismerettel rendelkező üzemeltetőállomány, amelynek 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 ismerete 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 itt a védelmi szektor minden szervezetének különböző szintű képzése, felkészítése jelen van. „Létrehozása megteremtette az egységes közszolgálati alapképzések strukturális, intézményi és személyzeti feltételeit.

[2] Farkas, Tibor – Hronyecz, Erika: Info-communication experts in the defence sector: Vocational training program, Fiatal Műszakiak Tudományos Ülésszaka, Kolozsvár, Erdélyi Múzeum-Egyesület, 2018, 75–79.; Farkas Tibor – Prisznyák Szabolcs: Kormányzati célú infokommunikációs hálózatok: A rendészeti szervek infokommunikációs rendszere, *Hadtudományi Szemle,* 10 (2017/4.) 583–596.

[3] Nemzeti Infokommunikációs Stratégia 2014–2020., Magyar Kormány, Budapest, 2014, 4.

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."[4] 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."[5]

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, lakosságellátási 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."[6]

Mindezek jól alátámasztják, hogy az NKE 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 figyelembevételével. A képzések minden esetben megfelelnek az Nftv.-ben (2011. évi CCIV. törvény a nemzeti felsőoktatásról) leírtaknak, az abban megfogalmazottaknak eleget tevő képesítést adnak, a továbbképzés rendszerébe teljesen beépülve biztosítják a közszolgálati képzések folytonosságát.

[4] Nemzeti Infokommunikációs Stratégia 2014–2020., Magyar Kormány, Budapest, 2014, 20.
[5] Nemzeti Közszolgálati Egyetem Intézményfejlesztési Terv 2015–2020, 2017, 4. www.uni-nke.hu/document/uni-nke-hu/IFT_170615_1.pdf (Letöltve: 2019. 04. 05.)
[6] Nemzeti Infokommunikációs Stratégia 2014–2020., Magyar Kormány, Budapest, 2014, 14–15.

A szakmai felkészítés alapjai

A legjelentősebb kutatási irányvonalakat, kutatási prioritásokat, amelyeket az NKE által gondozott tudományágakban határoztak meg, a „Kutatási, fejlesztési és innovációs stratégia 2016–2020" című dokumentum tartalmazza az alábbiak szerint, a hadtudományok vonatkozásában:[7]

- 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 Szemlé*ben megjelent cikk tartalmazza.[8]

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:[9]

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

A rendészettudományok területén szintén jelentős kutatási területeket fogalmaztak meg, 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."[10]

[7] Nemzeti Közszolgálati Egyetem Kutatási, Fejlesztési és Innovációs Stratégia 2016–2020, Nemzeti Közszolgálati Egyetem, Budapest, 2016, 35–38.

[8] Boda József et al.: Fókusz és együttműködés. A hadtudomány kutatási feladata, *Honvédségi Szemle,* 144 (2016/3) 3–19.

[9] Bleszity János et al.: Műszaki kutatások és hatékony kormányzás, *Hadmérnök,* 11 (2016/3) 221–242.

[10] Nemzeti Közszolgálati Egyetem Kutatási, Fejlesztési és Innovációs Stratégia 2016–2020, Nemzeti Közszolgálati Egyetem, Budapest, 2016, 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, ezenfelül 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 tevékenysége vezetésének 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.

Magyarországon a kormányzati és a védelmi tevékenységet végrehajtó szervezetek 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 (például információbiztonság) tekintve eltérő lehet, valamint vegyes felügyeletet igényel.

Az információtechnológia fejlődésével folyamatosan változnak mindazon lehetőségek, amelyeket 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.[11]

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

- a szolgáltatásokat biztosító infokommunikációs rendszerek;
- az egyes, speciális üzemeltetésű és rendeltetésű alrendszerek;

[11] Farkas, Tibor – Hronyecz, Erika: 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, 2017, 353–358.; Farkas Tibor, A katasztrófavédelmi és válságkezelési tevékenységek általános elemzése az irányítás és az infokommunikációs támogatás tükrében, *Hadmérnök,* 11 (2016/3) 135–148.; Farkas, Tibor – Hronyecz, Erika: Basic information needs in disaster situations (capabilities and requirements), in: Bitay Enikő, (ed.), Proceedings of the XXI-th International Scientific Conference of Young Engineers, s.n., Kolozsvár, 2016, 153–156.

- a rendszerek nyújtotta szolgáltatások;
- a rendszereket alkotó technikai eszközök és technológiák.

A kormányzati szintű irányítást és vezetést a kormányzati infokommunikációs rendszerek felhasználásával hajtják végre, 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 jogszabályok határoznak meg alapvetően. A rendelet alapján kormányzati célú hálózatnak minősülnek az 1. mellékletében felsorolt elektronikus hírközlő hálózatok, amelyek a következők:

- Nemzeti Távközlési Gerinchálózat (NTG, 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 nagyszámú hálózatok vannak jelen a kormányzati infokommunikációs rendszerben, amelyek széles körű 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 biztosítja a felhasználók részére a magas fokú rendelkezésre állást.

Ennek megfelelően az alábbi célrendszereket, szolgáltatásokat és infokommunikációs képességeket lehet meghatározni, illetve az üzemeltetőállománynak ezeket a rendszereket kell folyamatosan fenntartania, egyes esetekben pedig az ezekből nyert információkat kell továbbítania a megfelelő úgynevezett belső vagy külső együttműködő szervezeteknek. (Az alábbi felsorolást a teljesség igénye nélkül tüntetem fel.)

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: Vezetési és Irányítási) rendszer;
- Blueforce Tracking System (Sajáterő-követő Rendszer);

- MH KGIR (Költségvetésgazdálkodási Információs Rendszer) rendszer;
- tábori (telepíthető) alaphírhálózat;
- VTC-rendszer (Video Teleconferencing: Videókonferencia szolgáltatás);
- JTRS (Joint Tactical Radio System: Összhaderőnemi Harcászati Rádiórendszer);
- NIAR (NATO Irodaautomatizálási Rendszer);
- levelezőrendszer;
- 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, rejtjelfelügyeleti és ehhez kapcsolódó biztonságtechnikai feladatokkal, amelyek szintén számos, speciális célrendszert tartalmaznak, amelyek közül néhányat az alábbi felsorolás tartalmaz:[12]

- Robotzsaru (ügyviteli, ügyfeldolgozási és elektronikus iratkezelő rendszer) és alrendszerei;
- VÉDA (közlekedésellenőrző 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 érzékelőrendszerek.

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.[13] 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 (zárt rendszerű kommunikációs csatorna)
- katasztrófavédelmi célú segélyhívó és információs rendszerek;
- különböző lakossági és egyéb riasztórendszerek;
- ONER (Országos Nukleáris Baleset Elhárító Rendszer)
- OSJER (Országos Sugárfigyelő, Jelző és Ellenőrző Rendszer)
- egyéb katasztrófavédelmi információs rendszerek, vészhelyzeti és tájékoztató rendszerek.

[12] 18/2011. (IX. 23.) ORFK utasítás a Robotzsaru integrált ügyviteli, ügyfeldolgozó és elektronikus iratkezelő rendszer egységes és kötelező használatáról, jogosultsági rendjéről, az adatvédelem, valamint a rendszerfejlődés előírásairól.

[13] A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság Szervezeti és Működési Szabályzata, Belügyminisztérium, Budapest, 2012.

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 (zárt rendszerű kommunikációs csatorna);
- egyéb nyilvántartórendszerek és technológiák.

Az előzőekben leírtak mellett más kormányzati, védelmi szervezetek által alkalmazott infokommunikációs, információs rendszert is be lehet illeszteni egy olyan tudástárba, amelyet annak érdekében alakítanak ki, hogy az üzemeltető szakemberek és a felhasználók kellő szélességben átlássák az alkalmazott rendszereket a hatékonyság fokozása érdekében. A kormányzati, közigazgatási infokommunikációs rendszerek folyamatos fejlesztése, azok 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 érintik.

A védelmi infokommunikációs hálózatokhoz kapcsolódó szakmai felkészítés

A védelmi tevékenységek humán oldalról történő támogatásának egyik jelentős területe a kapcsolódó szakmai felkészítés, ismeretmegosztás, amely megteremti az infokommunikációs támogatás alapjait. A védelmi infokommunikációs hálózatokhoz kapcsolódó szakmai felkészítés célja, hogy megismertesse a képzésben részt vevőket a kormányzati infokommunikációs technológiák, rendszerek és hálózatok felépítésével és üzemeltetésével, a különböző hálózatok közötti együttműködés megvalósításának lehetőségeivel és az infokommunikációs kompetenciafejlesztés jelentőségével.

Egy lehetséges kialakított 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, amelynek 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;
- azokba bedolgozni, illetve részt venni a fejlesztési folyamatokban (megrendelés, fejlesztés, tesztüzem, képzés, átadás, monitoring).

A képzés célcsoportja azok a hallgatók, akik a kormányzati (közigazgatási, honvédelmi, katasztrófavédelmi, büntetés-végrehajtási, 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 széles körű ismeretanyag megszerzésének lehetőségét. A képzés minden esetben olyan szakemberek bevonásával valósulhat meg hatékonyan, akik speciális felkészültséggel, a szakterületen szerzett többéves szakmai gyakorlattal, fejlesztési tapasztalatokkal rendelkeznek.

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

a) 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 továbbfejlesztésének lehetőségeit.
b) 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 részt vevők 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 menedzsmentrendszereknek (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 spektrummenedzsment kiemelt részét kell, hogy képezze az ismeretkörnek.

c) 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 a pontos tudás mellett ismertetni kell a várható fejlesztéseket, preferált hálózattechnológiákat, a társadalmi, közigazgatási, védelmi és európai uniós fejlesztéseket is. 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, büntetés-végrehajtás és a közigazgatáshoz kapcsolódó hálózatokat, azok felépítését, működését, üzemeltetését és képességeit, kiemelve a hálózatokhoz tartozó speciális célrendszereket. 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 kíván 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, vezetését 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 (például terrortámadás) milyen tartalékrendszerek 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 zárt célú 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.

Jelen közlemény a Bolyai János Kutatási Ösztöndíj támogatásával készült.

Felhasznált irodalom

A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság Szervezeti és Működési Szabályzata, Belügyminisztérium, Budapest, 2012.

Bleszity János – Földi László – Haig Zsolt – Nemeslaki András – Restás Ágoston: Műszaki kutatások és hatékony kormányzás, *Hadmérnök,* 11 (2016/3) 221–242.

Boda József – Boldizsár Gábor – Kovács László – Orosz Zoltán – Padányi József – Resperger István – Szenes Zoltán: Fókusz és együttműködés. A hadtudomány kutatási feladata, *Honvédségi Szemle,* 144 (2016/3) 3–19.

Farkas Tibor, A katasztrófavédelmi és válságkezelési tevékenységek általános elemzése az irányítás és az infokommunikációs támogatás tükrében, *Hadmérnök,* 11 (2016/3) 135–148.

Farkas, Tibor – Hronyecz, Erika: Basic information needs in disaster situations (capabilities and requirements), in: Bitay Enikő, (ed.), Proceedings of the XXI-th International Scientific Conference of Young Engineers, s.n., Kolozsvár, 2016, 153–156. DOI: https://doi.org/10.33895/mtk-2016.05.29

Farkas, Tibor – Hronyecz, Erika: 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, 2017, 353–358. DOI: https://ieeexplore.ieee.org/document/8080582

Farkas, Tibor – Hronyecz, Erika: Info-communication experts in the defence sector: Vocational training program, Fiatal Műszakiak Tudományos Ülésszaka, Kolozsvár, Erdélyi Múzeum-Egyesület, 2018, 75–79. DOI: https://doi.org/10.33894/mtk-2018.09.14

Farkas Tibor – Prisznyák Szabolcs: Kormányzati célú infokommunikációs hálózatok: A rendészeti szervek infokommunikációs rendszere, *Hadtudományi Szemle,* 10 (2017/4) 583–596.

Nemzeti Infokommunikációs Stratégia 2014–2020, Magyar Kormány, Budapest, 2014.

Nemzeti Közszolgálati Egyetem Kutatási, Fejlesztési és Innovációs Stratégia 2016–2020, Nemzeti Közszolgálati Egyetem, Budapest, 2016.

Nemzeti Közszolgálati Egyetem Intézményfejlesztési Terv 2015–2020, 2017, www.uni-nke.hu/document/uni-nke-hu/IFT_170615_1.pdf (Letöltve: 2019. 04. 05.)

Jogi források

346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról

88/2016. (VII. 13.) Korm. rendelet a kormányzati célú hálózatokról szóló 346/2010. (XII. 28.) Korm. rendelet módosításáról

18/2011. (IX. 23.) ORFK utasítás a Robotzsaru integrált ügyviteli, ügyfeldolgozó és elektronikus iratkezelő rendszer egységes és kötelező használatáról, jogosultsági rendjéről, az adatvédelem, valamint a rendszerfejlődés előírásairól