HADMÉRNÖK

KATONAI MŰSZAKI TUDOMÁNYOK ONLINE

XI. Évfolyam 2. szám 2016. június

NKE
BUDAPEST

A szerkesztőség elérhetősége:
Nemzeti Közszolgálati Egyetem,
1101. Budapest, Hungária krt. 9-11. A. épület 9. emelet, 901. iroda
Postacím: 1581. Budapest Pf.:15.
Telefon: +36-1-432-9000 /29-289/ *Fax:* +36-1-432-9025 *HM:* 29-289
e-mail: hadmernok@uni-nke.hu web: http://hadmernok.hu

Kiadó: Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
ISSN 1788-1919

Jelen számban megjelent írások szerzői:

Csanádi Győző – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Csősz László – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Fehér Judit – Belügyminisztérium, Informatikai Főosztály
Felhősi László
Fialka György – Óbudai Egyetem, BDI doktorandusz
Gávay György – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. habil. Grósz Zoltán – Nemzeti Közszolgálati Egyetem, KVI egyetemi docens
Dr. habil. Gyarmati József – Nemzeti Közszolgálati Egyetem, HHK egyetemi docens
Prof. Dr. Haig Zsolt – Nemzeti Közszolgálati Egyetem, HHK egyetemi tanár
Kaluzsa Anikó – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Dr. habil. Kóródi Gyula – Nemzeti Közszolgálati Egyetem, KVI egyetemi docens
Dr. habil. Kovács Tibor – Óbudai Egyetem, BGK egyetemi docens
Dr. Kuti Rajmund – Széchenyi István Egyetem, MÉK, adjunktus
Mohai Ágota
Molnár Robin – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Nagy Dániel – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Pál Angéla
Papp Gergely – Nemzeti Közszolgálati Egyetem, KDI doktorandusz
Sági Gábor – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Som Zoltán – Nemzeti Közszolgálati Egyetem, KDI doktorandusz
Dr. Szabó József
Szendi József – Nemzeti Közszolgálati Egyetem, KMDI doktorandusz
Takács Krisztina – Gy-M-S Megyei Kormányhivatal
Dr. Teknős László – Nemzeti Közszolgálati Egyetem, KVI tanársegéd
Dr. Tick Andrea – Budapesti Gazdasági Egyetem, KKK egyetemi docens
Tóth József – Nemzeti Közszolgálati Egyetem, HHK tanársegéd
Dr. Vég Róbert – Nemzeti Közszolgálati Egyetem, HHK egyetemi docens
Vinnai Dalma

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

György Fialka - Tibor Kovács
gyorgyfialka@gmail.com - kovacs.tibor@bgk.uni-obuda.hu

THE CORRELATION AMONG TECHNICAL PARAMETERS, CONDITIONS OF APPLICATION AND BIOMETRICAL IDENTIFICATION

Abstract

The specifications indicated by the manufacturers in manuals can be different in the practice depending on the environment. Sometimes, if we want to install a biometric system, we just buy one reader, and we make tests for about six months to make sure the device is operating as it requested. Mostly we find problems about installations. An average sized system is very costly, for that raison it is indispensable to know how its elements work in a testing environment. We examined four biometrical devices and we are publishing the test results. We hope it can help to the companies to choose the adequate device.

A gyártók által kiadott felhasználói könyvekben megadott specifikációk a gyakorlatban - alkalmazási környezettől függően – eltérők lehetnek a leírtaktól. Számos esetben, ha installálni szeretnénk egy biometrikus rendszert, beszerzünk egy eszközt, és teszteljük fél évig csak azért, hogy meggyőződjünk róla: az akként működik, ahogy azt megadták. Gyakran gondokkal szembesülünk már az installáláskor is. Egy közepes méretű rendszer nagyon költséges tud lenni, ezért aztán fontos ismerni, hogy annak elemei tesztkörnyezetben miként viselkednek. Négy konkrét biometrikus eszközt teszteltünk és publikáljuk az eredményeket. Reméljük mindez segítségére lesz a felhasználóknak abban, hogy a számukra megfelelő eszközt ki tudják választani.

Keywords: *biometrics, fingerprint, hand geometry, iris recognition, palm vein, template, enrollment ~ biometria, ujjnyomat, kézgeometria, írisz-azonosítás, tenyérérhálózat, minta, felvétel*

INTRODUCTION

The man goal of the authors is do not sell any products but to test the biometric based devices and publish the test results.

The *Table 1* shows some important biometric devices' parameters (specifications) given by the manufacturer.

How are these devices working? First users should be registrated in the device. It means that some information will be stored in the device, like username, user ID or the fingerprint or other templates. When the user identifying her/himself the device compares his/her biometric data to the stored one. If these are origins from the same person, the identification - theoretically - will be successful. The device is "able" to find individual characteristics in the biometric pattern like points, intersections, crossings, characteristics, etc. All of these individual points have a relative coordinate. After each scanning the device can found several points but in the practice these points aren't sometimes the same. If the most of the typical points are the same the identification will be successful, otherwise denied.

			FINGERPRINT IDENTIFICATION				OTHER BIOMETRICAL IDENTIFICATION			
							Hand-geometry	Iris	Finger vein	Palm vein
	Model[1]		**Suprema BioEntry Plus**[2]	FingerKey DX	L1-4G V-flex	Bioscrypt V-Pass	**HandKey II**	**Panasonic BM-ET330**	L1-4G	**INTUS**
PARAMETERS[3]	**FAR**[4] [%]		n/a	n/a	n/a	0.2	0.1	1/1.200.000	n/a	1/12.000
	FRR[5] [%]		n/a	n/a	n/a	1	0.1	< 1	n/a	0.01
	Max User Number (N)		5.000	250	n/a	n/a	512	1.000	n/a	Unlimited
	Extended		n/a	500 – 2.000	n/a	n/a	1.000	5.025	n/a	n/a
	Template[6] **Storage Capacity**		10.000	2 per user	10.000 in 1:N 100.000 in 1:1	100 (max 200)	as user number	as user number	10.000 in 1:N 500.000 in 1:1	Unlimited
	Identification time		2.000 match in 1s	≤ 2s	< 1s for 100 user database	< 1s	< 1s	approx. 1s	Searches 6.000 templates ps	< 1s
	Ports	Ethernet	✔	✔	✔		✔	✔	✔	✔
		RS485	✔	2x	✔	✔	✔		✔	
		RS232		✔	✔	✔	✔			
		Wiegand				✔				✔
		Other			USB			Video Camera	WLAN	Lbus

Table 1: Specifications of biometrical identification devices (data from manufacturers)

[1] http://www.thaiprintex.com/BioEntry.html
http://www.eyenetwatch.com/pdf/suprema/bioentry_plus.pdf
http://security.ingersollrand.com/Downloads/Literature/Documents/Fingerkey%20DX.pdf
www.l1id.com/files/428-L1VFlex4GDatasheet_%20032409_.pdf
http://emssa.net/source/content/L1/V-Flex/Bioscrypt%20-%20Flex.pdf
http://www.securitystoreusa.com/Honeywell-Access-NC-HG4II-HandKey-II-Standalone-Ha-p/481976.htm
http://www.panasonic.com/business/security/bm-et300_demo/iris.html
http://www.identix.com/pages/735-4g-finger-vein-reader
http://hk.search.yahoo.com/search;_ylt=Axt7wJ8Aiv5N1goAkKizygt.?p=fingervein+L1%2C+PDF&fr2=sb-top&fr=FP-tab-web-t&rd=r1
http://www.pcs.com/uploads/tx_nppcsproducts/INTUS_1600PS_presentation_P_en.pdf

[2] Models marked with bold letters are analyzed in detail

[3] Access control biometrics user guide – British security industry association, Form No.181, Issue 2, May 2010

[4] FAR: False Acceptance Rate, it shows how much non-user can enroll successfully out of 100 users

[5] FRR: False Rejection Rate, it shows how much user can not enroll successfully out of 100 users

[6] The code of the biometric pattern

Next we shortly present our experiences, tests and possible resolutions of a fingerprint, a handgeometry, an iris and a palmvein instrument.

SUPREMA BIOENTRY PLUS (FINGERPRINT IDENTIFICATION DEVICE)

According to the manufacturer data sheet the identification time is less than 1s, if the number of matches is not more than 2.000. The sensor resolution is 500 dpi and the device can store 10.000 templates (max user number is 5.000).

It can use two type of RF card: Proximity (125 kHz EM) and Mifare (13.56 MHz).

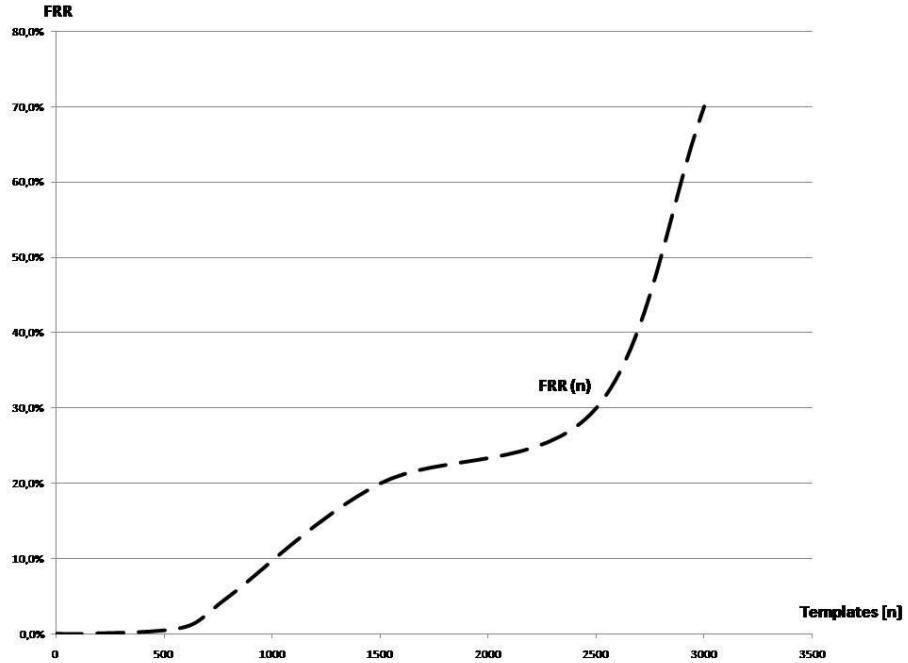
The three operation modes are Fingerprint, RF card, RF card + fingerprint.

The network interface is TCP/IP and RS485. The Wiegand output can be configurable up to 64 bits. [1]

In laboratory and when the users number was no more than 20 (approx. 150 templates) the device was fast and it had practically zero false rejection rate (FRR). The identification time was in accordance with the one given by the manufacturer.

Next we started use the instrument as a part of an access control system (the users could choose between biometric identification and well known chip-card). We registered 150-200 users a day.

When the number of the templates has been crossed 600, the false rejection rate has been appeared and started to linearly increase. Above 800 templates, the FRR was more than 5 %. Over 1.500 templates, the devices practically became useless (the FRR was over 20 %, so we had to open the entrances without any controlling of the incoming crowd). We made statistics every day and we sometimes achieved 70 % false rejection rate (see Graph 2).



Graph 2: FRR number in different template numbers (n) in case of Suprema Bio Entry Plus in a real environment (made by the authors)

The method of enrollment a fingerprint template was the following: first we recorded a template to the device (during these tests, we scanned the left middle finger). It was the reference. Later we carried 4 enrollments a day by various conditions out (the measurements were completed in different time and seasons). We immediately recognized if the scanned finger is in a different position from the original position the result was even worst.

In laboratory we found the average enrolled individual points 19.9, consequently the device operated adequately (see Fig. 3, the numbers under each small image show the quantity of congruent point comparing the original template to the captured one).

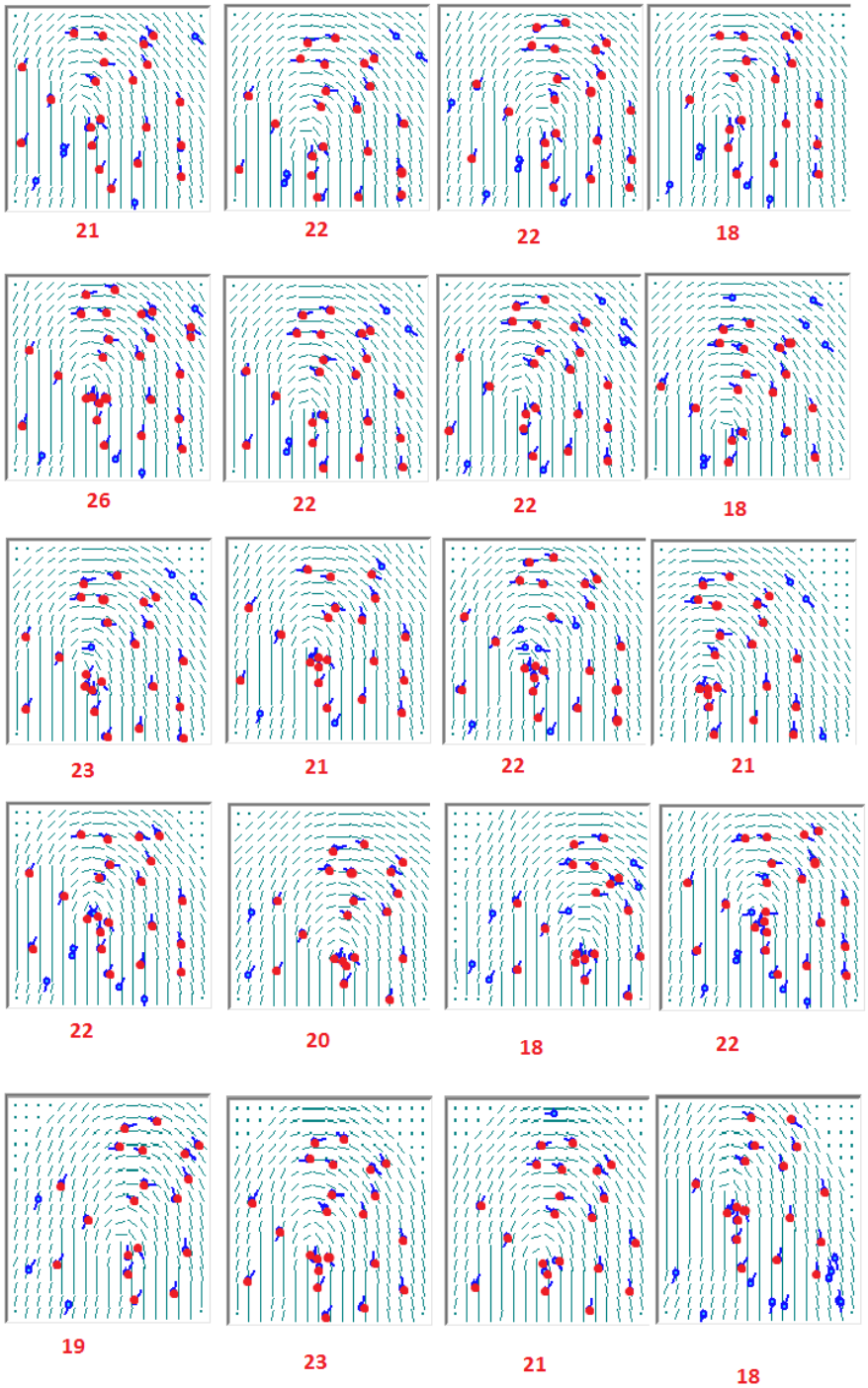


Fig. 3: Suprema BioEntry Plus test result (blue: reference points, red: enrolled points during identification; made by the authors)

HANDKEY II (HANDGEOMETRY IDENTIFICATION DEVICE)

The HandKey II is a fourth generation biometric access controller of recognition systems. The HandReader records and stores the three-dimensional shape of the hand for comparison and identity verification. Upon verification, the HandReader produces an output that can unlock a

door, send card format data to an access control panel, or communicate with a host computer. The HandReader also has auxiliary inputs and outputs that can be used to control other systems such as CCTV cameras and alarms.

The device is easy to use and has the minimal identification problems. The device has positioning pins which helps to keep the fingers in the correct position. This is the main point that makes the hand geometry successful. The hand and the fingers are in the same position in each scanning, and it makes the identification process successful.

The HandReader is an intelligent access control system that can operate as a stand-alone unit, in a network with other HandReaders, or in a network with a host computer. The maximum number of users depends on the license in the device (the typical user number is 256, 512, 9.728, 27.904 or 32.512).

We tested the Handkey II in 10 different industrial places and also in laboratory environment. The maximum user number was 1.500 (Transelectro Inc., Budapest, Hungary). The tests in real environment had 6.000 users who used the devices daily.

Some details given by the manufacturer:

- Network benefits without network wiring,
- Fits seamlessly into existing,
- Audit trails,
- Access profiles,
- Time zones,
- Alarm outputs.

The following problems were revealed:

- a couple of first time user is afraid to use the device,
- extreme hand size,
- identical twins,
- artificial nails,
- spreading infections.

In details:

We found 0.3 % of the users are afraid to use the device, because it has a brand new method never seen before. So they get used to it during a relatively long period of operation time.

The extreme hand size can be a challenge for this device. We experienced that extremely big or small hand size can lead to high false rejection rate. This problem can be resolved easily as we can set reject threshold to a less secure level for these samples, so the user can enter without any problem.

In case of twins the Handkey II accepts the other twin on the default reject threshold. We set the security level higher, so the device can distinguish twin-samples (this change is necessary only for the identical twin users, for other users, the default threshold level is used).

There is a serious problem as well, when a female user has extremely long artificial nails.

We heard of new virus types in the last years. We think the users are afraid to use the devices because it has hot points to spread the infections. We installed sanitizers close to the hand geometry reader and we informed the users how to use it. Nobody practically used them. Some users tried to enroll the sample without touching the surface (it is possible in case of this device, but it causes a longer identification time).

Some of the users found this device so fantastic they used more frequently it than it was necessary. This may cause huge logs, and incomprehensible statistics: if there is a time and attendance system controlled by the Handkey II, it will be hard to get the information from the mass of data.

The Handkey II resolves the problems of high amount of user by using the 1:N method. It means, that the user types his/her user ID number on the num pad of the device before matching. The device compares whether the template belongs to the given ID number (one comparison). This method has several advantages such as short matching time and good FAR and FFR values.

People may think that typing the user number can highly increase the time of the enrollment. Our experiences show the time of typing the user ID is negligible, so it does not mean a longer enrollment process.

PANASONIC IRIS READER (IRIS IDENTIFICATION)

When both eyes are reflected in the mirror the system automatically captures the iris images and completes recognition in 1 s (or less). The quick identification process prevents waiting in line.

The device is characterized by high security with false acceptance ratio as 1 in 1.2 million.

Iris recognition uses individual differences in the complex patterns found in the iris of the human eye to authenticate individual identities and it is the most precise of all biometric identification systems. The false acceptance ratio is so low that the probability of falsely identifying one individual as another is virtually zero.

Benefits of using Iris Technology are the following:

- The iris is a thin membrane on the interior of the eyeball. Iris patterns are extremely complex.
- Patterns are individual (even in fraternal or identical twins).
- Patterns are formed by six months after birth, stable after a year. They remain the same for life.
- Imitation is practically impossible.
- Patterns are easy to capture and encode. [3]

The most significant device features are:

- Iris recognition time: approx. 1.0 s (after iris image capturing until the recognition result is output).
- Eye image capturing range: approx. 30 cm to 40 cm (between the eyes and the mirror).
- Total number of users enrolled BM-ET330: 1.000 users max.
- Iris server: 5.025 users max.
- Angular field view horizontal: 115°, Vertical: 85° (fixed, video surveillance camera).
- False rejection rate: <1%. [4]

We had 150 users to test the device and 66 persons were using it daily. Only 10% of the users found, that device is hard to use (userfriendly device) and 86% of them that the device is sophistic and they like to use it. 20% of the users are mistrustful about this technology. [5]

The most serious problem is the lack of support. We found that sometimes the iris reader becomes unable to finish the booting process. That means the booting process started after we connect the device to the power but it never stop (even after hours). We successfully resolved the problems about the iris reader, however there was no support available anywhere (we tried to contact the Panasonic several times by email and by phone, but we could not find the adequate contact person for this device).

Another problem is to take the correct position in front of the camera for the new users. Our experiences show that it took about a half minute at least during the first week. Once the users had experience in this field and time of the identification has been reduced to 1-5 s

(practically the users know where the eyes should be located in front of the reader, namely eyes should be right in the opposite of the camera). The device can help to the user to get the correct position, arrows will be showed to the user which way should he/she move and the device gives verbal instructions.

We made tests in our Laboratory if the iris reader allows users to wear glasses or contact lenses. The environment was real, we tested the devices with 60 persons with different glasses and contact lenses. We found the glasses and the contact lenses will not make any negative effects in the process of identification. The users can wear these things during the identification.

People have different heights and therefore the device should be able to capture useful iris pictures for all kind of people. This device mechanically solves this problem, because there is a viewing angle of the camera that can be set easily by the user before identification.

The conclusion is easy to use this device, which can guarantee a low false acceptation rate. The first time it may be hard to found the correct position, so the time of the identification can be long at the first few weeks. When the user has a little practice by using the device, the identification is fast.

INTUS (PALM VEIN READER)

False acceptance rate is of this device no more than 0.00008%. An impressive level of security comparable to that of iris recognition is based on the highly complex vein pattern in the palm of the hand. Excellently suited for the unique identification of persons, this internal biometric feature provides optimum protection against tampering.

Palm vein authentication is based on the absorption of infrared radiation (heat radiation) in venous blood. A sensor illuminates the palm with infrared light and the oxygen-reduced blood in the veins absorbs the infrared rays. The sensor camera captures an image of the individual's vein pattern and converts it to a template.

The template is encrypted by the sensor and then saved to a database (for identification) or to a card or tag (for verification using "template on card"). [6]

The device requires a fast computer, otherwise the system produces a relative high false rejection rate. When we ordered the device, we found the hardware looks good at the first time because it is noiseless, it has no moving parts like hard-drive or fan (with the original hardware the device was slow and it had relative high false rejection rate).

The reader must be connected to the server with USB-cable. It can cause problems, because the maximum length of the USB cable is relatively short.

In case of wet or sweaty hands, the false rejection rate is relative high.

We tried the software with a more powerful computer with success. The card reader and the num pad become unfortunately useless. To have a better FRR and faster identification have to change the computer (but the num pad and the card reader will be lose).

We was trying to change the USB cable to a longer one and convert the data format to another twisted pair connection – without any success.

Conclusion the original server computer is extremely slow for this task even in case of small amount of users. A faster computer accomplishes without any problem the mission.

CONCLUSIONS

We found the basic, general and serious problem of the biometric identification is to positioning the members (of body) to the same position where the user placed during registration. The first template should be recorded in a well-positioned anyway and all the

following scanning should be perfectly in the same way positioned. Most of the devices cannot handle this problem, some of them can give signals to the user about where should he/she move to achieve better results. The best solution is that the device has a fix position we can stay in the same stable position.

Surprisingly the original server computer is slow for biometrical identification tasks. A faster computer accomplishes without any problem the mission.

References

[1] http://www.eyenetwatch.com/pdf/suprema/bioentry_plus.pdf

[2] http://www.securitystoreusa.com/Honeywell-Access-NC-HG4II-HandKey-II-Standalone-Ha-p/481976.htm

[3] http://www.panasonic.com/business/security/bm-et300_demo/iris.html

[4] http://product.yktworld.com/article/201008/20100816154200051 5.html

[5] Suplicz, S. – Fűzi, B.: Essay on access control systems managed by an iris identification device (aversiv reactions and attitudes of the users), Budapest Tech, 2007

[6] http://www.pcs.com/uploads/tx_nppcsproducts/INTUS_1600PS_B_en.pdf

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Mohai Ágota
mohai.agota@gmail.com

A JELZÉSI ZÓNÁK SZEREPE A TŰZJELZŐ BERENDEZÉSEKBEN

Absztrakt

A beépített tűzjelző berendezések tervezése nem csak villamos feladat, komplex tűzvédelmi koncepcióba ágyazott, a tervező által a többi tűzvédelmi területre is rálátást igénylő, igen összetett feladat. A tűzjelző berendezések tervezési koncepciójának alapját a védendő terület felosztása szerint csoportosított rendszerelemek adják. A terület megfelelően történő jelzési zónákra osztása kulcsfontosságú a rendszer későbbi megfelelő és rugalmas működését, működtetését tekintve. Ennek fontosságát, szerepét, és a jelzési zónák kijelölésével kapcsolatos problémákat szeretném jelen cikkben feldolgozni.

The planning of fire detection and fire alarm systems is not just an electrical task. It needs complex fire safety concept from the designer. He has to insight the other field of the fire protection of the building. The basic of the fire alarm system's planning is the method of the area's division into zones. This is the key of the good and flexible working and operation of the system in the future. In this article I would like to process this problem.

Kulcsszavak: *tűz, tűzbiztonság, tűzjelző berendezés, jelzési zóna, riasztási zóna ~ fire, fire safety, fire alarm system, detection zone, alarm zone*

BEVEZETÉS

Az objektumok védelme összetett feladat. A védelem bármely részelemének hiánya vagy gyengesége kihat a teljes biztonsági rendszer hatékonyságára, ugyanakkor gyakran bonyolult biztonsági alrendszereket kell üzemeltetni egymással összehangoltan (beléptető rendszer; biztonsági monitoring rendszer, tűzjelző berendezések stb.). A zavarmentes működés követelményeinek biztosítása létfontosságú. [1]

Az elektronikus tűzjelző rendszer a tágabb értelemben értelmezett elektronikus vagyonvédelem fontos területe. Az automatikus tűzjelző rendszer érzékel, jelez és riaszt még a tűz kifejlődésének kezdeti szakaszában. Így lehetőséget biztosít nagyobb károk megelőzésére, még kezdődő tűz időbeni lokalizálására és eloltására. [2]

A beépített tűzjelző berendezések (továbbiakban TJB) tervezése összetett feladat, melynek során kiemelkedő szerepe van a jelzési és riasztási zónák meghatározásának, kialakításának. A gyakorlat azt mutatja, hogy a tervezők körében eltérő a zónásítás fontosságának megítélése. A jelzési zónák kijelölése sokszor elnagyolt, átgondolatlan, vagy nem is történik meg a tervezési fázisban. Cikkem célja elsősorban a jelzési-, illetve érintőlegesen a riasztási zónák szerepének, gyakorlati jelentőségének és kijelölésük tervezői gyakorlatának a vizsgálata több szempontból.

A JELZÉSI ZÓNÁK SZEREPE

A zóna fogalma jelenleg nem szerepel a hatályos OTSZ-ben [3], az átkerült a vonatkozó Tűzvédelmi Műszaki Irányelvbe [4; 5], az alábbiak szerint:

"A zóna: a védett helyszín területileg elkülönített része, melyen belül – más részektől függetlenül – bizonyos funkciókat végre lehet hajtani az alábbiak figyelembevételével:
a) a funkció különösen az alábbi lehet:
aa) a tűz bekövetkeztének jelzése (jelzési zóna),
ab) tűzriasztások, vezérlések kiadása (riasztási zóna),
b) a jelzési és riasztási zónáknak nem kell azonosaknak lenniük."

Ezen kívül megtaláljuk a zónák fogalmát az MSZ EN 54-2:2009 szabványban [5; 10] is előzőtől kicsit eltérően, de annak nem ellentmondva:

"zóna: A védett létesítmény olyan földrajzi területrésze, amelyben egy vagy több pont van telepítve, és amelyre egy közös zónakijelzést alkalmaznak."

Fenti definíciókból egyértelműen következik, hogy tűzjelző berendezés tervezése során a védendő létesítményt valamilyen szempontok alapján területekre osztjuk. A szabvány [5] ki is mondja, hogy a tűzjelző központban (továbbiakban TJK) gondoskodni kell arról, hogy a pontokról jövő jelek zónák szerint csoportosíthatók legyenek.

A definíciókból nem következik egyértelműen, de a védett terület zónákra osztása alapvetően befolyásolja, segíti [5]

- a tűzriasztás forrásának gyors helymeghatározását, beazonosíthatóságát;
- a tűz méretének felbecsülését és növekedési sebességének megfigyelését;
- a telepített rendszer felosztását a riasztás szervezésének és a tűzvédelmi intézkedéseknek a céljából, és
- a hibák korlátozását a rendszeren belül.

A fenti célok elérése érdekében létrehozandó jelzési zónák kialakításának szempontjai összetettek. A vonatkozó tűzvédelmi irányelv [4; 9] úgy fogalmaz, hogy *"A megfelelő jelzési zónakiosztás segítségével a tűzjelzés helye gyorsan és egyértelműen azonosítható a TJK kijelzései alapján."*

A JELZÉSI ZÓNÁK KIALAKÍTÁSA

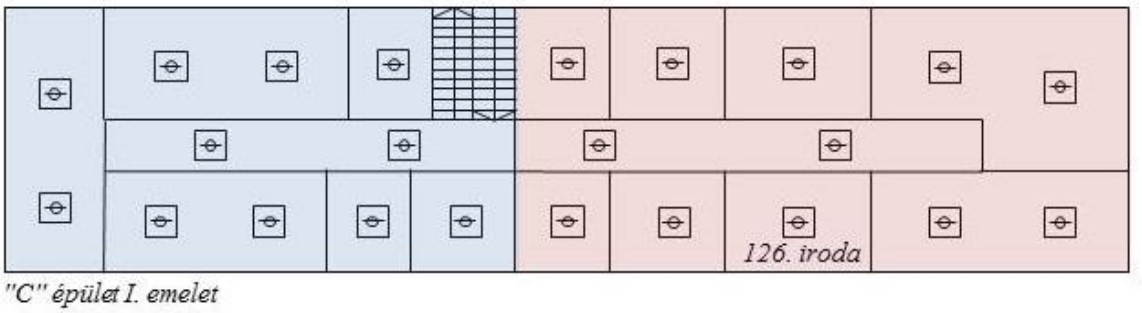
Bár a szabvány [5] a zónákba való csoportosítás részletes követelményeit az alkalmazási útmutatókra bízza, tapasztalatom szerint az egyes gyártók tervezési segédletei vagy sehogy, vagy csak nagyon felületesen tárgyalják ezt a kérdést. A TvMI [4; 9] megad olyan alapvető és általános szempontokat, amiket a jelzési zónák kijelölése során érdemes figyelembe venni. Ezek a szempontok a következők:

- az épület belső elrendezése,
- minden olyan tényező, amely a kiürítést vagy a tűz felderítését gátolja,
- a riasztási zónák kialakítása, és
- az esetleges veszélyes környezetek jelenléte.

Ha a fenti szempontokat tovább elemezzük, az épület belső elrendezésénél figyelembe kell venni például

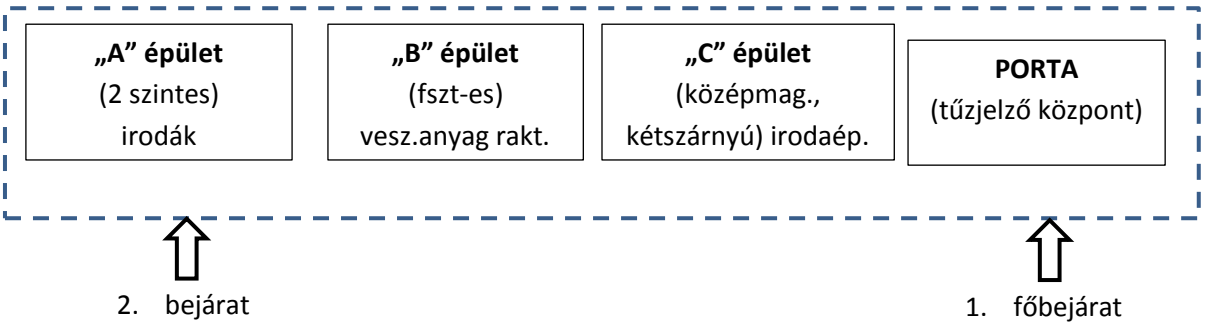
- a szintszámot (a TvMI [4] 6.4.1. pontja alapján minden egyes zóna az épületnek csak egyetlen szintje lehet néhány kivételtől eltekintve, mint a lépcsőház, liftakna stb.),
- a lépcsőház elhelyezkedését, és ettől függően az egyes területek megközelítési lehetőségeit,
- ha van menekülésre is igénybe vehető biztonsági felvonó, akkor annak az elhelyezkedését,
- több épület, épületrész- vagy szárny esetén azok elhelyezkedését, megközelíthetőségét, vagy
- ha a létesítmény több területre van osztva, amiket esetleg különböző szervezetek, bérlők használnak, akkor azt is.

Egy többszintes, kétszárnyú irodaépületnél egy adott szintre vonatkozóan, példaként az 1. ábra szerint lehet kialakítani a jelzési zónákat.



1. ábra Példa jelzési zónák kialakítására (saját ábra)

További szempontként említhetjük, elsősorban nagyobb létesítmények esetén a beavatkozó erők a tűz helyétől függő, eltérő megközelítési irányt is. A 2. ábrán vázolt létesítmény esetében például az „A” épület esetén a 2. bejáraton, míg a „C” épületből jövő tűzjelzés esetén a főbejáraton keresztül történő megközelítés a célszerűbb.



2. ábra Minta épület (saját ábra)

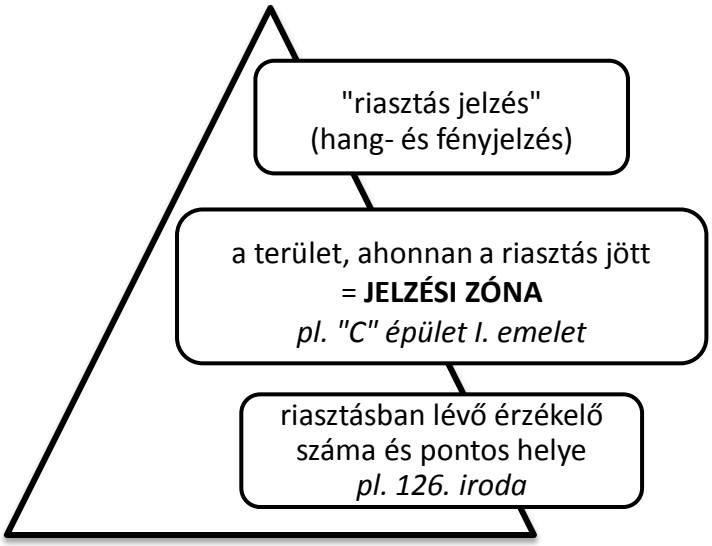
A kiürítést vagy a tűz felderítését gátló tényező lehet például olyan terület, ahová a bejutás korlátozott, feltételekhez kötött. Titkos adatok tárolására szolgáló helyiségekbe, vagy nagyfeszültségű terekbe a bejutás sokszor még a felügyeletet ellátó személynek is csak külön kulccsal, kóddal, felügyelő személy kíséretében lehetséges. Mivel ezek mind a felderítési időt és a további intézkedésekig eltelt időt növelik, célszerű ezen tereket eleve külön jelzési zónába tenni, hogy az onnan jövő tűzjelzésre minél gyorsabban a megfelelő intézkedéseket el lehessen indítani.

Hasonló megfontolásból a veszélyes környezet is kiemelten kezelendő szempont a zónásításnál. Egyrészt lehetnek olyan területek, ahonnan könnyen veszélyes kémiai, biológiai anyagok juthatnak a környezetbe. Ide a belépés általában zsilipen keresztül, védőruhában lehetséges olyan személy kíséretében, aki ismeri a technológiát, az ott használt anyagokat. De olyan veszélyes anyagok tárolásánál is más hozzáállás szükséges a felderítő személy és a beavatkozó erők részéről, amelyek oltása különleges megoldást vagy eszközöket igényel (pl. vízzel nem oltható anyagok oltása, radioaktív anyagok jelenléte). A 2. ábrán például másfajta beavatkozást igényelhet egy irodai használat, mint egy veszélyes anyag tároló raktár. Más tűzoltó taktikát alkalmazunk a földszintes vagy középmagas épület esetén is.

További meghatározó szempont a zónásítás során, – a 2. ábra példáját is tekintve – a riasztás szervezés és tűzvédelmi intézkedések szempontjából a riasztási zónák kialakítása. Egy olyan létesítményben, ahol az automatikusan indítandó tűzeseti vezérlések nem bármely érzékelőről vagy kézi jelzésadóról jövő tűzjelzésre (összesített tűzjelzés) indulnak, ezt szintén figyelembe kell venni. Ha a 2. ábrán látható példánál maradunk, akkor a hangjelzők indításához, a hő- és füstelvezetés indításához, a liftek vezérléséhez, a füstmentes lépcsőház túlnyomásos ventilátorának indításához stb. elsődleges információ az, hogy melyik épület melyik szintjéről, területéről jött a jelzés. Ezt a jelzési zónák megfelelő kialakításával tudjuk biztosítani. A TJK programozása során adott területhez tartózó és ugyanazon vezérléseket kiváltandó eszközöket tartalmazó zónákat logikailag összerendeljük adott vezérlésekkel. Ekkor válhatnak fontossá - elsősorban nagyobb, vagy több épületre kiterjedő rendszerek esetén - a riasztási zónák. Több épület védelmét ellátó TJB esetén célszerűen csak abban az épületben szólaltatjuk meg a hangjelzőket, indítjuk a tűzeseti vezérléseket, ahonnan a tűzjelzés érkezett.

A JELZÉSI ZÓNÁK KIALAKÍTÁSA KÜLÖNBÖZŐ TŰZJELZŐ BERENDEZÉSEKBEN

A gyorsabb beazoníthatóságot a bemeneti eszközök zónákba szervezése úgy segíti, hogy vészhelyzetben – amilyen egy tűzjelző központ felügyeletét ellátó személy szempontjából egy bejövő és kezelendő riasztás jelzés is, – a tűzjelző központ egyszerűbb, átfogóbb, gyorsabban feldolgozható és azonosítható információt közöl a riasztás jelzést fogadó személlyel. A tűzjelző központon szabvány [5] szerint megjelenítendő információ az emberi gondolkodás számára egyértelműbb, elsődleges információt kell, hogy tartalmazzon. Ez a riasztásban lévő érzékelőt vagy kézi jelzésadót tartalmazó jelzési zóna száma és neve (3. ábra).

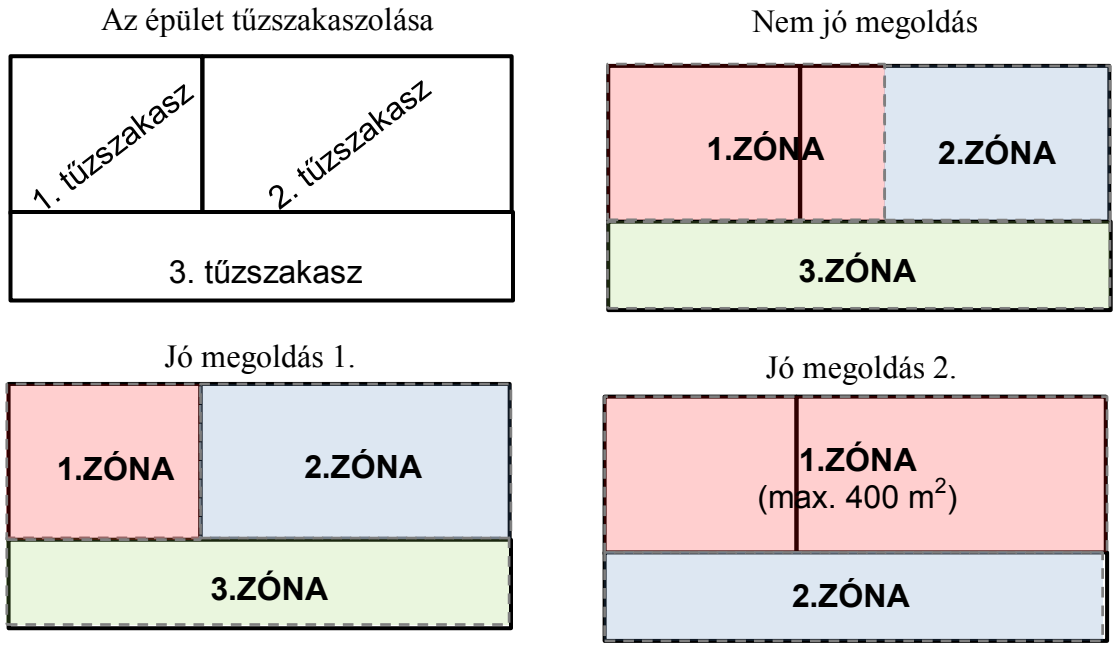


3. ábra Riasztás jelzés általános feldolgozási hierarchiája címzett TJB esetén (saját készítés)

Címzett rendszerek esetén a TJK képes magának a riasztásban lévő érzékelőnek a számát és nevét is megjeleníteni (automatikusan vagy külső beavatkozást követően), de vészhelyzetben hasznosabb elsődleges információt jelent egy hierarchikusan magasabb szintű kategória megjelenítése (3. ábra). Például egy több épületet tartalmazó létesítmény esetén, ahol egy külön portaépületben van a TJK (2. ábra), a riasztás jelzést fogadó személy számára fontosabb információ, hogy „A", „B" vagy „C" épületből jött-e a tűzjelzés, mint az, hogy a 126. irodából (1. és 2. ábra). Pláne igaz ez, ha esetleg több épületben, pl. „A" és „C" épületben is van 126. iroda. Elsődleges információként tehát a hierarchikus megközelítést tekintve hasznosabb a jelzés gyors beazonosíthatóságát tekintve a jelzési zóna kijelzése. Ez feltételezi, hogy a jelzési zónákat átgondoltan jelöltük ki.

A tűzjelző rendszerek tervezése során kiemelkedő szempont a hibák korlátozása. A hibakorlátozás lehetőségei közül az egyik legkézenfekvőbb a jelzőáramkörben bekövetkező zárlatok és szakadások negatív hatásának minél kisebb területre korlátozása. Ennek egyik eszköze, hogy kijelöljük azokat a maximális területeket, amelyeknél nagyobbra az egyes hibatípusok hatása már nem terjedhet ki. Ezt a területi, illetve rendszerelem-szám szerinti korlátozási kategóriát szintén a bemeneti eszközök jelzési zónákba szervezése teszi lehetővé. Az előírások [4] szerint ugyanis alapvetően korlátozva van a jelzési zónák területe (max. 1600 m2), illetve az egy jelzési zónába szervezhető eszközök száma (32 db). Szakadás esetén hagyományos rendszereknél (5. ábra) így eleve nem eshet ki a működésből ennél nagyobb terület vagy több eszköz. Az analóg címzett rendszerek visszatérő jelzőáramköri kialakítása a szakadás hatását megoldja, mert egyszeres szakadás esetén a TJK másik irányból is eléri az eszközöket, egy eszköz sem esik ki a működésből. Zárlat esetén pedig, mivel címzett rendszereknél legalább a zónahatárokra izolátort (vagyis zárlatszakaszolót) kell tervezni, szintén nem eshet ki 1600 m2-nél, illetve 32 db eszköznél több a működésből.

Ezen felül a jelzési zónáknak igazodniuk kell az épület tűzszakaszolásához is. Ha egy zóna több tűzszakasz védelmét látja el, akkor a zóna az érintett tűzszakaszokat teljesen lefedi, és az így kialakított jelzési zóna alapterülete nem lehet nagyobb 400 m2-nél [4] (4. ábra).



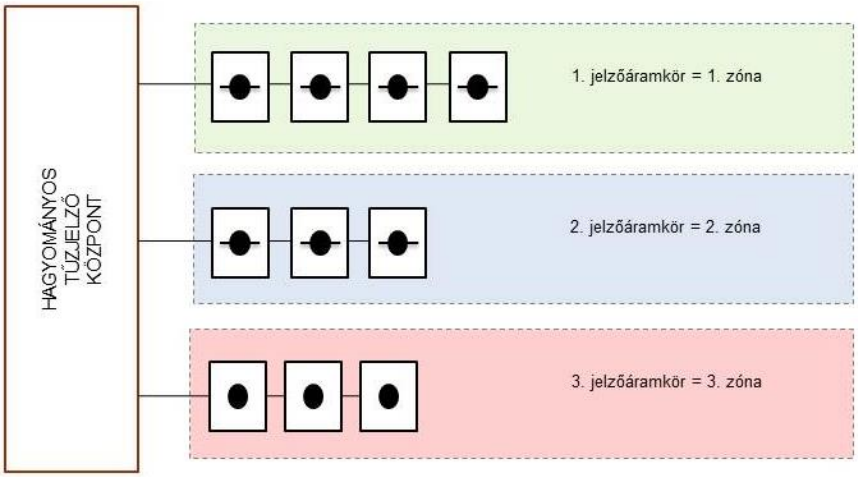
4. ábra Zónák igazodása a tűzszakasz határokhoz (saját szerkesztés)

Ez szintén az épület építészeti és komplex tűzvédelmi koncepciójával összefüggő, azt alapvetően figyelembe vevő tervezői ismereteket és hozzáállást követel.

A JELZÉSI ZÓNÁK KIALAKÍTÁSA KÜLÖNBÖZŐ TJB-BEN

A bemeneti eszközök jelzési zónákba szervezésének lehetősége minden szabványos [4] tűzjelző rendszerben adott. Eleve külön kell e szempontból kezelnünk a hagyományos tűzjelző rendszereket (5. ábra).

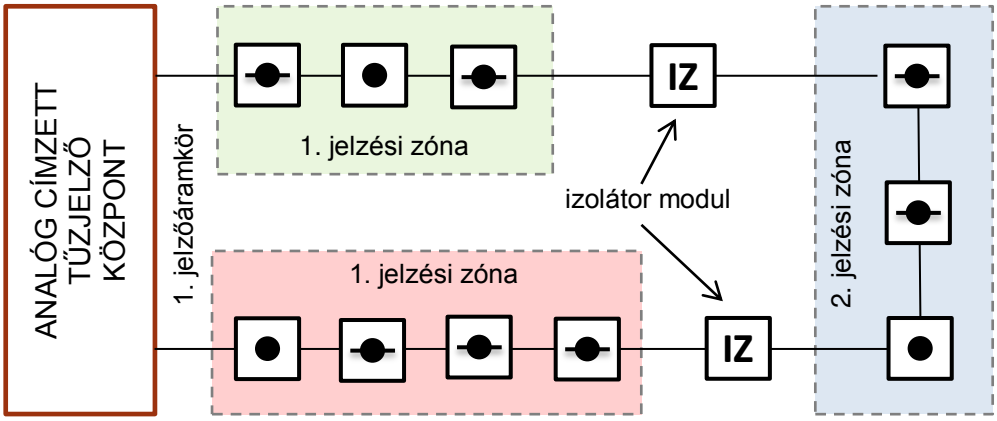
Hagyományos tűzjelző rendszerek esetében a tűzjelző központ nem tudja külön-külön megjeleníteni az egy jelzőáramkörbe kötött érzékelők jelzéseit, csak az adott jelzőáramkör jelzését (zónaszelektivitás), ezért a jelzőáramköröknek eleve alkalmazkodniuk kell a kijelölt zónákhoz. Ebből következik, hogy a tervezés kezdetén már alapvető szemponttá válik a jelzési zónák kijelölése a vonatkozó szempontok és előírások betartásával.



5. ábra Zónák kialakítása hagyományos tűzjelző rendszerekben (saját szerkesztés)

A címzett analóg tűzjelző rendszereknél már más a helyzet. Az egyes bemeneti eszközök címzettek, így azok jelzését a tűzjelző központ egyértelműen, eszközönként képes

megjeleníteni. A címzett analóg rendszereknél a működésükből adódóan – típustól függően - egy jelzőáramkör akár több száz eszközt is képes kezelni. Ebben az esetben az, hogy mely terület védelmét ellátó eszközöket tekintünk egy „területhez tartozónak”, azaz mely eszközöket sorolunk egy jelzési zónába, már nem függ a jelzőáramkör méretétől, nyomvonalától. Az egyes bemeneti eszközöket – automatikus tűzérzékelőket és kézi jelzésadókat – egyedi címeik segítségével szoftveres úton tudunk egy-egy „csoportba”, azaz jelzési zónába szervezni (6. ábra).



Megjegyzés: a példában a kézi jelzésadók beépített kétoldali izolátoros kivitelűek

6. ábra Zónák kialakítása analóg címzett tűzjelző rendszerekben (saját szerkesztés)

Az analóg címzett rendszerek között, gyártónként és rendszer típusonként eltérő lehet az elv, ahogy a bemeneti eszközöket hierarchikus szintekbe szervezik. Legegyszerűbb hierarchikus szervezési elv, amikor az egyes eszközöket egyedi címeik alapján jelzési zónákba szervezzük. Ez egyértelműen megfeleltethető a TvMI-ben [4] tárgyalt jelzési zónáknak.

Egyes tűzjelző rendszereknél azonban többszintű hierarchiát is módunkban áll alkalmazni. Ezen rendszerek esetében az érzékelőket csoportokba, a csoportokat pedig további területekbe stb. szervezhetjük (7. ábra).

<table>
<tr><th>"Szintek"</th><th>2-szintű hierarchia</th><th colspan="2">3-szintű hierarchia</th><th colspan="2">4-szintű hierarchia</th></tr>
<tr><td>4. szint</td><td rowspan="2"></td><td colspan="2" rowspan="2"></td><td>terület</td><td rowspan="2">"jelzési zóna"</td></tr>
<tr><td>3. szint</td><td>terület</td><td rowspan="2">"jelzési zóna"</td><td>szekció</td></tr>
<tr><td>2. szint</td><td>jelzési zóna</td><td>csoport</td><td colspan="2">zóna</td></tr>
<tr><td>1. szint</td><td>érzékelő/KJA</td><td colspan="2">érzékelő/KJA</td><td colspan="2">érzékelő/KJA</td></tr>
</table>

KJA: kézi jelzésadó

7. ábra A rendszerelemek szervezésének módjai (saját szerkesztés)

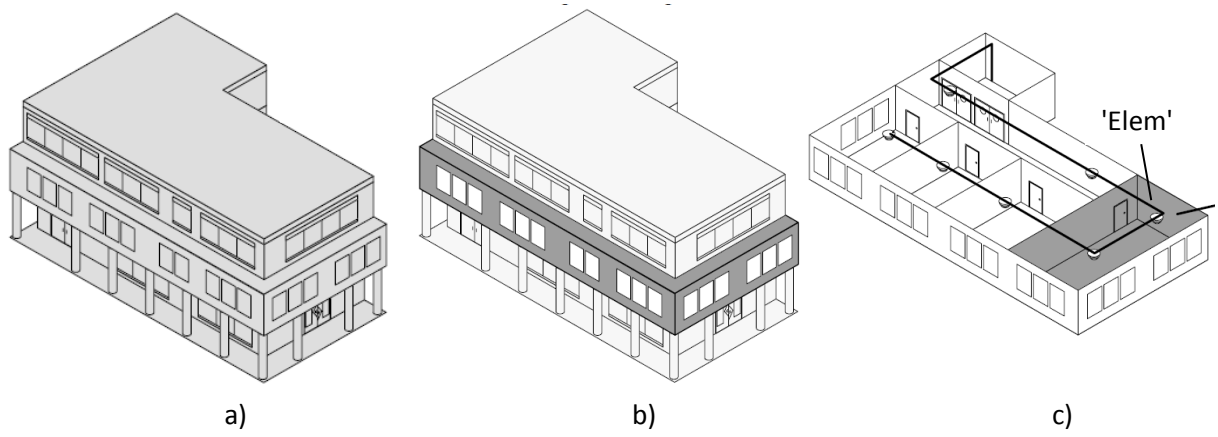
Egyes gyártók a saját rendszereikhez külön terminológiát dolgoznak ki. Az egyik, 4-szintű hierarchiát alkalmazó rendszer [6] például az alábbiak szerint kezeli a zónásítást.

4. szint: 'Area', vagyis 'Terület' (8.a. ábra), ami maga az épület, vagy nagyobb, összetett épületek esetén épületrész

3. szint: 'Section', vagyis 'Szekció' (8.b. ábra), ami az adott épület egy szintjét, vagy szárnyát jelenti

2. szint: 'Zone', vagyis 'Zóna' (8.c. ábra), ami ebben az értelemben egy helyiséget takar (ha a helyiség méretéből adódóan több érzékelőt tartalmaz, akkor ezek kerülnek egy zónába)

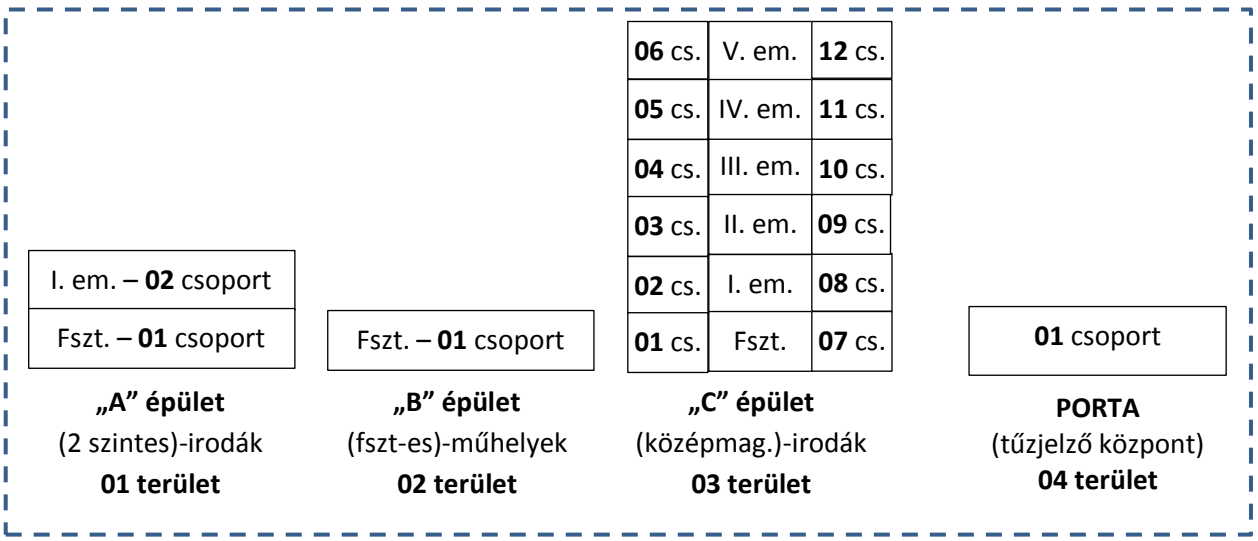
1. szint: 'Element', vagyis 'Elem' (8.c. ábra), ami már egy konkrét, saját egyedi címmel rendelkező automatikus érzékelő vagy kézi jelzésadó a rendszerben



8. ábra 4- szintű zónásítási terminológia [6]

Fenti terminológia, átgondolva a célját, illetve tudva azt, hogy a többszintű hierarchia szerint dolgozó rendszereknél megoldott általában az egyes szintekhez rendelve is a kikapcsolás, illetve teszt és egyéb funkciók, azt mondhatjuk, hogy a jó megoldásnak bizonyulnak. Zavaró és félreérthető viszont a helyiségenkénti csoportok 'zóna' elnevezése, ami természetesen nem feleltethető meg a szabvány és a tűzvédelmi irányelvekben leírt jelzési zónának. Hiszen a cikkben leírt célok és szempontok alapvetően nem helyiség nagyságrendű, hanem nagyobb területekhez köthetők.

Egy másik, 3-szintű hierarchikus megoldást [7] mutat a 8. ábra a mintaépületre alkalmazva. Ebben az esetben a 3. szint a 'Terület', 2. szint a 'Csoport, és 3. szint az 'Érzékelő'. Az előírások szerinti jelzési zónának a ’terület/csoport’ együttesen feleltethető meg. Vagyis pl. a „C” épület Fszt. jobb szárnya a 0308-as számú jelzési zóna lesz.



9. ábra Példa háromszintű hierarchia szerinti zónásításra (saját szerkesztés)

Míg az előző OTSZ [8] kötelezővé tette a zóna-térkép1 alkalmazását - szintszámtól, alapterülettől és a TJB eszközszámától függően - a nagyobb rendszerek esetén, addig mára a zóna-térkép alkalmazása sajnos csak ajánlás szintjén maradt meg a vonatkozó tűzvédelmi irányelvben [4]. Az utóbbi években elterjedő grafikus megjelenítők - bár nem szabványos eszközök, és csak igen szűk körben teszi a jogszabály [3] kötelezővé alkalmazásukat, - szintén hozzájárulnak ahhoz, hogy a tűzjelző rendszer és az általa megjelenített jelzések könnyebben áttekinthetőek és beazonosíthatóak legyenek, kezelésük gyorsabb és egyszerűbb legyen nagy rendszerek esetén is.

ÖSSZEFOGLALÁS

Bármely olyan objektum kialakításakor és későbbi működtetésekor, melyben ideiglenesen vagy üzemszerűen tárolt anyagok gyulladása veszélyforrást jelent, a belső terek és anyagok felügyeletének és ellenőrzésének javítása a felügyeleti és ellenőrző mechanizmusok alkalmazásának és technikai támogatottságának folyamatos vizsgálatát és tökéletesítését kívánja meg. [93]

Cikkemmel kiemeltem a tűzjelző berendezések tervezési folyamatából a jelzési zónák fontosságát, körüljárva azon szempontokat, amiket a jelzési zónák kijelölése során az előírásokban szereplő kevés információn felül fontosnak tarok. Áttekintettem azokat a gyakorlati megoldásokat, amelyekkel a tűzjelző berendezések gyártói igyekeznek a rendszer logikus felépítését, rugalmasságát növelni olyan alkalmazásoknál, ahol a rendszer méretéből adódóan a kétszintű hierarchia már kevésnek bizonyul. Egy tűzjelző berendezés gyors, könnyű és rugalmas működésének és kezelésének egyik alappillére a tervezési fázisban megfelelően átgondolt logikai felépítés. Ahhoz, hogy tervező az adott létesítményre tervezett rendszerrel a helyi sajátosságoknak és feltételeknek is legmegfelelőbb, optimális megoldást adjon, ismernie kell mind az adott TJB gyártó által létrehozott terminológiáját, mind a vonatkozó műszaki előírásokat, amiknek szintén meg kell felelni.

Felhasznált irodalom

[1] Berek Tamás - Horváth Tamás: Fizikai védelmi rendszerek dinamikusan változó környezetben Hadmérnök IX. Évfolyam 2. szám - 2014. Június 16.p. ISSN1788-1919

[2] Berek Lajos: Biztonságtechnika ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel jegyzete NKE 2014.

[3] 54/2014. (XII.5.) BM rendelettel kiadott Országos Tűzvédelmi Szabályzat

[4] TvMI 5.1: 2015.03.05. Beépített Tűzjelző Berendezés tervezése, telepítése Tűzvédelmi Műszaki Irányelv (OKF)

[5] MSZ EN 54-2: 2009 Tűzjelző berendezések, 2. rész: Tűzjelző központ

[6] Siemens Building Technologies Cerberus Division, Cerberus CS1145 Fire Detection system Operating instructions, Manual CS11.2 Section 7 http://itpg.com.au/image/data/ci1145%20-%20ep5%20(as4428)%20operation%20manual.pdf ((letöltve: 2016.01.03.)

[7] Dusan Ferbas, Jiri Sindelar: Modbus SecuriPro Protocol Bridge (Modbus050123) version 1.1. http://www.etech.cz/products_data/MoSec/Modbus_SecuriPro_bridge_en.pdf (letöltve: 2016.01.07.)

[8] 28/2011. (IX.6.) BM rendelettel kiadott Országos Tűzvédelmi Szabályzat

[1] zóna-térkép: az egyes zónák elhelyezkedését, területi határait és a zónák megközelítési útvonalait ábrázoló térkép [4; 5]

[9] Berek Tamás: Vagyonvédelmi koncepció kialakításának sajátosságai veszélyes anyagok vizsgálatát biztosító létesítmények esetében Hadmérnök VI. Évfolyam 4. szám - 2011. december ISSN1788-1919

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Felhősi László
ninjalacika@gmail.com

CMC – A CIVIL HARCOSOK KIHÍVÁSA

Absztrakt

Az alábbiakban a hazánkban még kevéssé ismert Civilian Military Combined (CMC) versenyt kívánom bemutatni, elsődlegesen annak a 8 hetes felkészülési programja okán, mivel azt igen használhatónak gondolom a Magyar Honvédség katonáinak általános fizikai felkészítése szempontjából is.

Below are still little known in our country Combined Military Civilian (CMC) I would like to introduce competition, primarily due to the eight-week preparation program, as it is very usable think the general physical preparation in the Hungarian Defense Forces soldiers as well.

Kulcsszavak: *CMC, akadályverseny, crossfit, futás, edzésterv ~ CMC, obstacle race, crossfit, running, training plan*

BEVEZETÉS

Napjainkban az extrém jellegű akadályfutások (Fighter's Run, Spartan Race, Brutálfutás) hazánkban is mind nagyobb népszerűségnek örvendenek. Az említett versenyek az olyan sportos civileket igyekeznek megszólítani, akik szeretnék magukat próbára tenni a katonai gyakorlópályákhoz hasonló, több kilométeres, komoly fizikai kihívást jelentő akadálypályákon. Tanulmányomban, a hazánkban még kevéssé ismert Civilian Military Combined (CMC) versenyt, illetve annak nyolc hetes felkészülési programját kívánom bemutatni. A témaválasztásom azért tarthat számot érdeklődésre, mivel a CMC felkészülési programja együttesen alkalmazza az atlétika, a súly-és erőemelés, a futás, és a torna sportágak egyes elemeit, így ez által egy nagy intenzitású, a funkcionális edzésmódszernek tekinthető. Ebből adódóan nagy örömre szolgálna, ha a publikációm - még ha kis mértékben is -, egyrészt hasznosíthatónak bizonyulna nem csupán a Magyar Honvédség kiképző és testnevelő szakemberei, hanem minden olyan olvasó számára is, akik érdeklődnek a megszokottól eltérő, újszerű, és nem mellékesen komoly és sokoldalú kihívások iránt.

AZ AKADÁLYFUTÁSOKRÓL ÁLTALÁBAN

Már az ókori történetírók feljegyzéseiből is tudjuk, hogy a hajdani görög vagy római gyalogos katonák erőnléti felkészítése milyen sokoldalú volt. A spártai katonáknak gyakori edzését jelentette a teljes fegyverzetben történő futás [1].

1913-ban - szintén katonai kiképzési célokra - George Herbert alkotta meg az első olyan edzésmódszert, amely írásos és rendszerezett formában fogalmazott meg hasznos útmutatásokat a katonák testkultúrájának, fizikai felkészültségének javítására. Herbert a katonák fizikai felkészítésének legfontosabb eszközét a saját testtel végezhető gyakorlatok mellett a futással kombinált akadálypályákban látta [2]. Természetesen az akadályokkal tűzdelt katonai gyakorlópályák jelentőségét más hadseregekben is idejekorán felfedezték.

Egészen a múlt század 90-es éveinek végéig a civilek számára leginkább elérhető versenyfajtát a hagyományos futás jelentette („traditional foot racing"). Ebben az időszakban jelentek meg először az ún. kalandfutások („adventure racing"), amelyekben ötvöződtek a futás, a lovaglás, az úszás vagy a hegymászás elemei. Az első, mai értelemben vett akadályfutást (obstacle race) az Angliában megrendezett Tough Guy Obstacle jelentette, amelyet aztán számos más, hasonló verseny követett (Metro Dash, Muddy Buddy Rebel Race, Ruckus Sports, Rugged Maniac, Rugged Warrior, Spartan Race, Tough Mudder, Warrior Dash [3].

Ezeknek a versenyeknek a közös sajátossága, hogy a rendezők és a résztvevők elsősorban kihívásként tekintenek arra, és így nem törekednek mindenáron a győzelemre. Éppen ezért az indulók gyakran csapatmunkában teljesítik azt, de nem ritka az sem, hogy az egymás számára teljesen ismeretlen indulók egyfajta ad hoc jelleggel segítik egymást [4].

Mint nevéből is sejthető, a Civilian Military Combined (CMC) létrejöttében is felismerhetőek katonai vonatkozások. Mindez annak köszönhető, hogy a CMC életre hívói az amerikai hadsereg veteránjai. A CMC egy legalább 8 kilométer hosszú, változatos akadályokkal megtűzdelt futóverseny. Egyedisége abban rejlik, hogy a futó versenyszám előtt teljesíteni kell az ún. PIT nevű tesztet. Ez egy 7 perces, magas intenzitású, funkcionális képességeket alaposan próbára tevő kihívás, amely a következő négy gyakorlatból tevődik össze. Ez a box jump (nők esetében 20 inches = 50,8 cm, férfiak esetében 30 inches = 76,2 cm magasság), felhúzás (nő – 95 pound/43 kg, férfi – 135 pound/61 kg), thruster (nő – 12 kg kettlebell, 79 kg, férfi – 16 kg kettlebell) és burpee. Ezeket a gyakorlatokat ún. AMRAP (As Many Reps As Possible) jelleggel kell teljesíteni, tehát 90 másodperc alatt törekedni kell a maximális ismétlési szám elérésére. Ezt követően 20 másodperc pihenő, majd pedig ismét következik a következő gyakorlat, szintén 90 másodperc ideig, szintén a már említett AMRAP jelleggel. 5 perc pihenést követően rajtol a már említett legalább 8 km-es akadályfutás, amely a pálya kialakításától függően 25 akadályt jelent. A verseny életre hívóinak nem titkolt célja az volt, hogy a PIT bevezetése révén egyenlő versenyfeltételek között tudják összemérni erejüket, edzettségüket az indulók, és a verseny végére eldönthető legyen, hogy ki a legjobb általános kondícióval rendelkező sportoló [5].

A CMC 8 HETES FELKÉSZÜLÉSI TERVE

A CMC egyediségét a már említett PIT jelenti, és éppen ezért a CMC elsősorban az olyan ún. hibrid atléták számára ideális, akik a futáshoz elengedhetetlenül szükséges állóképesség mellett erővel és erő állóképességi képességekkel is rendelkeznek. Egy CMC kihívás során tehát a szokványos futó edzésterveket követő sportolókat meglehetősen kellemetlen meglepetések érhetik, mivel ők a felsőtest vázizomzatának erősítésének kevés figyelmet szentelnek. Természetesen ezzel a CMC életre hívói is tisztában voltak, így megalkottak egy olyan 8 hetes edzéstervet, amely lehetőséget nyújt arra, hogy a jelöltek ne csupán a PIT-et tudják jó eredménnyel tudják teljesíteni, hanem még az azt követő több kilométeres akadálypályára is maradjon erejük.

Az említett két hónapos felkészülési terv heti 6 edzésnap és egy pihenőnap felépítést követi. A szisztematikusan felépített, egyre nehezedő edzések során az állóképesség, az erő,

az erő-állóképesség és a metabolikus kondíció fejlesztésére egyaránt törekednek. A lenti saját készítésű táblázat szemlélteti az említett képességek fejlesztésére irányuló edzések jellegét, típusát [6].

1. táblázat. A CMC edzéstervének felépítése

1. nap	2. nap	3. nap	4. nap	5. nap	6. nap	7. nap
Erő	Erő-állóképesség	Erő	Erő	Erő	Erő-állóképesség	Pihenés
Crossfit WOD	Futás	Metabolikus kondicionálás	Futás	Metabolikus kondicionálás	Futás	

Mint látható, a felkészülés során a komoly figyelmet fordítanak az erő fejlesztésére. Ez nem meglepő, hiszen a nyolc kilométeres akadályfutás során számos olyan kihívás leküzdése szükséges, amely során a kar és a felsőtest izomzatának kell fejlettsége elengedhetetlen (kötél, ill. palánkmászás, nehéz tárgyak cipelése stb.). Az erőedzések során a súly, ill. erőemelésből ismert alapgyakorlatok (mellről nyomás, fekve nyomás, guggolás, felhúzás) kell végrehajtani, alacsony ismétlési számban (1-5 ismétlés), tetszőleges pihenőidőkkel.

Az erő mellett az állóképesség fejlesztését nagyszerűen szolgáló futás is hangsúlyos részét képezi a CMC felkészülési tervének. A futóedzések jellegüket tekintve jellemzően kétfélék lehetnek. Az ún. hosszú futás során egy adott távot vagy meghatározott időtartamot kell képesnek lennie egyenletes iramban lefutnia a sportolónak. Beszélhetünk ugyanakkor sprint jellegű edzésekről is, amikor 400, ill. 800 méteres etapokat kell edzésről-edzésre nagyobb ismétlési számban és az etapok közötti rövidebb pihenőidőkkel teljesíteni

A metabolikus kondicionálás kategóriájába tartozó edzések lényegében olyan magas intenzitású anaerob edzések, amelyek egyrészt fejlesztik a hosszú távú állóképességet, valamint alkalmassá teszik a sportolót a már megszerzett erőszint megtartására. A metabolikus edzések a gyakorlatban kisebb súllyal vagy szabadsúllyal végrehajtott köredzések, amely során magas ismétlési számot kell végrehajtani a lehetőség szerinti minél rövidebb pihenőidővel. Mondhatjuk azt is, hogy a metabolikus edzések jelentik a belépőt az AMRAP jellegű kihívások sikeres teljesítésének irányába [7].

A CMC felkészítésének részét képezik még a Crossfit-ből ismert ún. WOD-ok („Workout of the Day”). A Crossfitben - mint nevéből is látható -, a WOD a nap edzését is jelenti. Ezek olyan különböző crossfit gyakorlatokból álló komplex feladatok, amelyek általában az erőszint felmérésére szolgálnak [8].

A CMC nyolc hetes, e cikk szerzője által magyar nyelvre lefordított, ill. a könnyebb értelmezés érdekében jegyzetekkel ellátott felkészülési terve a következő linkről letölthető: https://drive.google.com/file/d/0BwNj6ehH1WhEV2QxamFuM0lPd2M/view?usp=sharing

ÖSSZEGZÉS

Saját tapasztalataim szerint a CMC felkészülési terve sok hasonlóságot mutat a crossfitből megismert edzéstervekkel. Lényeges különbség azonban, hogy az előbbi a futásra nagyobb hangsúlyt helyez, valamint az is eltérés, hogy a CMC edzésprogram célirányosan a már említett PIT gyakorlatok minél nagyobb ismétlési számú teljesítését célozza.

Tekintettel arra, hogy a CMC versenysorozatot az USA-n kívül még nem rendezik meg, így meglehetősen kevés az esély arra, hogy valaki kimondottan egy CMC versenyre való felkészülés céljából hajtsa végre a két hónapos programot. A CMC felkészülési tervét ugyanakkor nagyszerűen alkalmazhatónak gondolom egyéb más, hasonló kihívást jelentő futóversenyekre, vagy „embert próbáló”, kitartást, állóképességet, erőt egyaránt igénylő

próbatételekre készülők esetében is. Javasolni tudom minden olyan civil sportolónak és katonáknak, akik a futóteljesítményük javítása mellett szeretnék erőszintjüket is nagymértékben növelni. A felkészülési program hátránynak gondolom ugyanakkor azt, hogy intenzitása okán a „felesleges” izomtömeg leépülését eredményezheti. Komplexitás okán nagyon fontos az edzések közötti pihenőidők fokozott betartása a túledzés megelőzése okán. Elengedhetetlenül szükségesnek tartom az előzetes edzéstapasztalatot, a fokozott sérülésveszély elkerülése érdekében a súlyzós gyakorlatokat szabályos és biztonságos végrehajtásának ismeretét. Utóbbiak hiánya esetén egy szakképzett szakember, edző tanácsainak, útmutatásainak segítségül hívása erősen ajánlott.

További nehézséget okozhat továbbá az is, hogy rendelkezésre kell állnia a megfelelő felszerelésnek is (kétkezes súlyzórúd, kb. 100 kg súlytárcsa ill. kettlebell súlyzók). Sajnos az említett eszközök beszerzése költségesnek mondható.

Úgy gondolom, hogy az előbbiek okán vélhetően a CMC sohasem lesz igazi tömegsport, azonban a kihívásokat kedvelő és szerető, ambiciózus, saját határaikat kitolni kívánó sportemberek számára mindenképpen ajánlható.

Felhasznált irodalom

[1] Ancientmilitary.com: The Spartan Military. http://www.ancientmilitary.com/spartan-military.htm 2016. 02. 15.

[2] McKay, Brett – McKay, Kate: The History of Obstacle Courses for Military Fitness, Sport, and All-Around Toughness. http://www.artofmanliness.com/2015/09/10/the-history-of-obstacle-courses/ 2016. 02.15.

[3] Sands, Kathleen: Traditional Foot Racing v. Obstacle Racing. http://scholarsarchive.jwu.edu/cgi/viewcontent.cgi?article=1018&context=student_scholarship 2016. 02.15.

[4] Toughmudder.com: What is Though Mudder? https://toughmudder.com/events/what-is-tough-mudder 2016.02.15.

[5] Civilianmilitarycombine.com: The Pit. http://cmcrace.com/what-is-cmc/ http://www.civilianmilitarycombine.com/about/#tab2 2016. 02. 15.

[6] Civilianmilitarycombine.com: WOD - Week 1, Day 1. http://www.civilianmilitarycombine.com/wod-week-1-day-1/ 2015. 11. 09.

[6] Fitbuilder.hu: A metabolikus kondicionálás a gyakorlatban. http://www.fitbuilder.hu/cikk/A_metabolikus_kondicionalas_a_gyakorlatban.html 2015. 11. 09.

[7] Vitalzone.hu: CrossFit gyakorlatsorok (WOD's). http://www.vitalzone.hu/crossfit-gyakorlatsorok-wods-.html 2015. 11. 09.

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Gávay György
gavay.gyorgy@uni-nke.hu

A PIRANHA JÁRMŰVEK FEJLŐDÉSE A VÉDELMI ÉS ALKALMAZÓI IGÉNYEK TÜKRÉBEN

Absztrakt

Ez a publikáció a mai katonai célú védett csapatszállítás egyik legmeghatározóbb járműcsaládjának fejlődésével foglalkozik. Az első Piranha járművek mintegy negyven-negyvenöt éve lettek rendszerbe állítva, azóta több generáció került kifejlesztésre. A fejlesztés nem csak a generációk között, hanem egy adott generáció esetében is jelentős léptékű volt, erre jó példa a DVH azaz dupla „V" alakú törzs kialakítása a Piranha III alapokra épült Stryker járművek esetében.

This paper deals with the development of one of the most important vehicle families of the protected troop transport. Piranha vehicles are in service since 40-45 years and more generations were developed until these decades. Developement was significant regard with one generation, a very good example the DVH system wich was built into the Stryker vehicles. Stryker vehicles based on the Piranha III type.

Kulcsszavak: *Piranha járművek, ballisztikai védelem, IED elleni védelem, harcjárműfejlesztés, páncélozott csapatszállító jármű ~ Piranha vehicles, ballistic protection IED protection, combat vehicle development, armpred personel carrier*

BEVEZETÉS

A páncélozott kerekes járművek eredete, azok első felbukkanása nehezen meghatározható, de összességében elmondható, hogy a mai típusok gyökerei az 50-es, 60-as évekig nyúlnak vissza. Bár a kerekes járművek nagy részétől az USA gyorsan próbált megszabadulni a második világháború után, az elmúlt évtizedekben [1] ez a helyzet teljes mértékben megváltozott. A 2000-es évek elején több nemzet fegyveres erőinek vezetése is egyértelmű törekvéseket tett a lánctalpas, például az M113 csapatszállító eszközök lecserélésére. A gumikerekes járművek [2] előnyei a lánctalpas járművekhez képest a jellemzően alacsonyabb ár és fenntartási költség.

A MOWAG[1] által gyártott Piranha család alapjaira épített járművek az elmúlt évtizedekben jelentős szerepet kaptak missziós területeken, számos változatot illetve

[1] A MOWAG Motorwagenfabrik AG-t 1950-ben alapította Walter Ruf gépészmérnök. Az elmúlt évtizedekben ez a cég meghatározó szerepet töltött be a világ hadszínterein, mivel a védett csapatszállítás,

utódtípust több hadsereg is rendszerbe állított. Az eszközök fejlődését alapvetően határozta és határozza meg a mai napig, a személyi állomány védelmére fordított fejlesztési munka.

A 70-es évek nyugati hadseregeinek csapatszállítással kapcsolatos igényei kevésbé ismertek, de sejthetően a hidegháborúnak köszönhetően az európai területek által támasztott követelmények, illetve a gazdaságos üzemeltetés játszotta a legnagyobb szerepet. A vietnámi háború után az USA fegyveres ereje csak az első öbölháborúban vállalt először meghatározó szerepet. A hidegháborúban a szembenálló felek páncélozott járművei között több, jellemzően kéttengelyes páncélozott szállító harcjármű típus is nagyon hasonló stílusjegyekkel, és műszaki paraméterekkel rendelkezett.

A Szovjetunió az afganisztáni háborúban szembesült azzal a ténnyel, hogy hadrendi felépítése[2] és az Európai hadszíntérre tervezett eszközei alkalmatlanak bizonyultak az új területen. Ez a megállapítás a helikopterekre és a teherautókra is igaz volt, több esetben szükségmegoldásként utólagos páncélozással próbálták meg növelni a logisztikai szállítmányok biztonságát. Az aszimmetrikus hadviselés megjelenésével már a váratlan támadásokra, csapdákra és előzetesen nehezen felderíthető, nagyobb tűzerejű fegyverek elleni védelemre kellett felkészíteni a járműveket. Az elterjedő támadási formák nem újszerűek. A gerilla harcmodor a háborúkkal, a telepített robbanóanyagok alkalmazása, vagy a zsákmányolt fegyverek alternatív alkalmazása azok megjelenésével egyidős.

A XXI. század elején nem a harcjármű-harcjármű elleni szimmetrikus hadviselés, hanem a nehezen felderíthető, de várhatóan nagy tűzerővel, hirtelen támadó kis létszámú ellenséges tevékenység a maghatározó. Nem szabad azonban megfeledkezni arról, hogy ez rövid időn belül megváltozhat, hiszen a közel keleten elhúzódó konfliktus, a világ vezető nagyhatalmai között is feszültséget okoz.

A cikk bemutatja a Piranha járműcsalád mintegy 40 éves fejlődését, generációról generációra. Az összegyűjtött információkból lehet következtetni az alkalmazási igényekre az adott időszakokban. A harcászati műszaki adatokat a publikáció végén lévő összefoglaló táblázat tartalmazza.

ÁLTALÁNOS SZEMPONTOK A VÉDETTSÉG MEGHATÁROZÁSÁRA

Egy harcjármű alkalmazhatóságában a védelmi és a mozgékonysági szempontok döntő szerepet kapnak. A haditechnikai eszközöket leíró szempontok meghatározásával és azok súlyának számításával a [3] és a [4] irodalmak foglalkoznak. Párhuzam vonható a harcjárművek és a harckocsik között, azzal a megkötéssel, hogy a ballisztikai védelem, és az akadályleküzdő képesség egyértelműen gyengébb egy kerekes harcjármű esetében. A védettségnek a járművet alkalmassá kell tennie arra, hogy a benne elhelyezkedő személyzetet és részegységeket megóvja az ellenség tűzeszközeinek hatásától, lehetővé tegye a túlélést. [5] A páncélzat kialakításakor a vastagság, az összetétel és a becsapódó lövedék, vagy repesz haladási irányára bezárt szög meghatározó. Ezért a harcjárművek frontpáncéljai a mai napig erősen döntöttek, és az alkalmazott lemezek is vastagabbak.

Az IED és akna elleni védelem az elmúlt évtizedekben vált kiemelkedően fontossá. [6] Ez az igény egy újnak tűnő konstrukciót hívott életre, mely alapja valójában egy 70-es évekbeli egyszerű megoldás. Egy vagy több „V” alakú lemezt illesztettek a páncélozott csapatszállító járművek szerkezetébe már a tervezésnél, vagy a meglévő eszközökre utólag. Ennek az elemnek a szerepe. hogy robbanás energiáját tereli el és csökkenti a járműre ható erőket.

---

járőrözés és felderítés járműveinek jelentős hányada fűződik a nevéhez. A MOWAG cég 2003 óta a General Defense Land System európai vállalatának a GDELS részévé vált. Forrás: GDELS.com

[2] Az ellenség harceljárás módjai ismertek voltak, felderítési adatok alapján a veszteség is kalkulálható volt a harcérintkezések előtt.

A védettség esetében meg kell még említeni a tömegpusztító fegyverek elleni védelmet illetve a tűzoltó berendezést, mely a fent már említett célokat szolgálja. A védettséghez szorosan kapcsolódik a tűzerő illetve a mozgékonyság kérdése is, az erre vonatkozó adatok minden esetben a harcászati, műszaki követelmények alapjait képezik. Az összefoglaló táblázatban ezeket az adatokat (a fellelhetőség függvényében) szerepeltetem.

PIRANHA I – LAV – LAV 25 – BISON – ASLAV

Az első Piranha I harcjármű [7] az 1970-es években lett kifejlesztve 4x4 és 6x6-os hajtásképletű változatban *(1. ábra)*. A 6x6-os változatból Kanada rendelt meg először 350 db-ot 1977-ben. Ekkor került bevezetésre a LAV (Light Armored Vehicle) azaz könnyű, páncélozott jármű elnevezés.

1. ábra, A Piranha I típus 4x4-es[3] és 6x6-os[4] változatai

Ezeknél a járműveknél, a mozgékonyság, és a gyalogság ellen jól alkalmazható fegyverek, és a tömegpusztító fegyverek elleni védelem volt a legfontosabb szempont. A jármű konstrukciójának alapjait a mai napig meghagyták, a vezető baloldalt elöl, mögötte a kezelőszemélyzet másik tagja, vagy parancsnok foglal helyet. A járműben elöl a jobb oldalon a motor és a váltó került beépítésre, amennyiben a motor mögött került kialakításra a parancsnok pozíciója az jelentősen növelte annak biztonságát. A deszant tér jól variálható, kialakítástól függően a szállított személyek egymásnak háttal középen, vagy egymással szemben a jármű szélén foglalnak helyet. A járműveket a kezdetektől fogva 11.00 R 16 méretű run-flat [8] abroncsokkal szerelték. A run-flat kialakítás lényege, hogy a kerékpántra szerelt gumiabroncsok lövedékállóak, defekttűrőek, vastag falúak, minden terepre alkalmasak. Jellegzetességük egy belső, tömör gumigyűrű, amelyen az abroncs kiszakadása, kilyukadása esetén is képes a jármű tovább haladni.

A jármű gyorsan sikeressé vált, a 8x8-as hajtásképletű változatból licenc alapján Kanada még mintegy 760 db-ot gyártott le 1988 közepéig. Később még 203 db eszközt rendelt a Kanadai hadsereg, melyek Bison *(2. ábra, első kép)* és Coyote néven 1997-ig kerültek bevezetésre és vannak rendszerben a mai napig.

Eredetileg is több feladatkör ellátására tervezték az eszközt, jó alap volt a következő speciális járművek számára:

- páncélozott szállító jármű, APC;
- gyalogsági harcjármű, IFV;
- fegyver hordozó jármű, weapon carrier;
- műszaki jármű;

[3] forrás: http://www.warwheels.net/images/Piranha1_4x4apcFOTI%20%282%29.jpg (letöltve: 2016.01.10.)
[4] forrás: http://www.warwheels.net/images/Piranha1_6x6apcFOTI%20%281%29.jpg (letöltve:2016.01.10.)

- sebesültkihordó eszköz.

A 8x8-as eszközök alkalmazhatóságára jó példa, hogy a későbbiekben Kanada 758 db LAV-t épített az USA tengerészgyalogságnak. [9]

2. ábra, A kanadai Bison[5] és az ausztrál ASLAV harcjárművek[6]

A Bison kivitelt több féle fegyverzettel is szerelték, az M2-es 12,7 mm-es géppuska a páncéltesten belülről is működtethető volt, mely jelentősen növelte a lövész biztonságát.

Az ausztrál kormány Kanadától kezdetben 15 db majd még 97 db Piranha I alapú ASLAV [10] járművet *(2. ábra, második kép)* rendelt meg, melyek 1994-től az ezredfordulóig le is lettek szállítva. Fegyverzetük többnyire 7,62 mm-es géppuska volt. A típus kétszemélyes toronnyal is szerelhető, melybe 25 mm-es Bushmaster gépágyú került beépítésre. Ugyanezzel a fegyverrel szerelt LAV jármű az LAV-25 nevet kapta. A járművet teljes acél páncél borította, mely védelmet nyújtott a kisebb kézifegyverek lövedékei és a repeszek ellen. A vezető kilátását három periszkóp tette lehetővé melyek a járművön elöl találhatóak. A periszkópok közül a középsőt passzív éjjellátóra lehet cserélni.

A motor Detroit Diesel 6V-53T melyhez Ailison 5+1 sebességes automataváltó kapcsolódik. A mozgékonyságot növelte, a jármű méretéhez képest alacsony tömege, mely a fegyverzettől függően 12 t körül maradt. A kerekek felfüggesztése mind a négy tengelyen független kialakítású. Az első két tengely kormányzott illetve a hajtása kapcsolható, a hátsó két tengely állandó hajtású. Az első két tengely acél csavarrugókkal, a hátsó két tengely torziós rugókkal van szerelve. Maximális rugóút 0,32 m minden tengelyen. A járműcsalád összes tagja úszóképes, vagy azzá tehető.

A védelem szempontjából a fejlesztés folyamatos volt az első konstrukció óta. Az oldallemezek az alapjárművön övvonal felett 30° -ban döntöttek, ezzel növelték az alap páncélzat ballisztikai védelmi képességeit. A döntött oldalpáncél jellemző például a BTR járművekre a mai napig.

[5] forrás:http://www.army.gov.au/Our-work/Equipment-and-clothing/Vehicles/ASLAV (letöltve: 2016.01.12.)
[6] forrás: http://www.military-today.com/apc/bison_l1.jpg (letöltve: 2016.01.12.)

PIRANHA II

A Piranha II- es járműveket a fellelhető irodalmak kevésbé tárgyalják. Nem volt kiemelkedően sikeres. A svájci hadsereg rendelt meg 205 db-ot 1995-ben, melyek 1996-ig rendszerbe is álltak, illetve Omán rendelt 80 db-ot hét különböző kivitelben [11] Ezek a járművek 1995 és 1997 között kerültek leszállításra. A páncélozott csapatszállító jármű (APC) kivitel 12,7 mm-es M2-es géppuskával, míg a fegyverhordozó (Weapon Carrier) változat 81 mm-es aknavetővel lett felszerelve. Megjelent a központi abroncsnyomás állító rendszer (CTIS) és a sivatagi kivitel elektronikus motorvezérlést, jobb szűrési hatásfokú levegőszűrőt kapott, illetve ABS - szel szerelt fékrendszer került beépítésre. A sivatagi kivitel fejlesztését az ALVIS cég bevonásával végezték.

3. ábra. Piranha II[7]

Ennél a típusnál az abroncsméret változtatásával lehetett emelni a hasmagasságon illetve növelni a lépcsőmászó képességet, a futóművet úgy alakították ki, hogy több abroncsméret is alkalmazható legyen.

A hajtásláncban volt komoly előrelépés. [12] Minden differenciálmű 100%-ban zárható, kétfokozatú osztóművet építettek be, illetve a teljes hajtáslánc zajemisszióját sikerült nagymértékben csökkenteni.

Ez a típus tulajdonképpen Piranha I és Piranha III típusok közötti rövid átmenetet képviselte. Az egyetlen szembetűnő változás a külső jegyek alapján a Piranha I típushoz képest, hogy a döntött oldalpáncélt egy idő után felváltotta a közel merőleges oldalfal.

PIRANHA III ALAPÚ ESZKÖZÖK

[7] Forrás: http://www.armyrecognition.com/images/stories/europe/switzerland/wheeled_armoured/piranah_II_8x8/Piranha_II_Mowag_wheeled_armoured_vehicle_personnel_carrier_Switzerland_Swiss_Army_640.jpg (letöltve:2016.01.13)

A Piranha III jármű [13] térbeli kialakítása hasonlít a Piranha I és Piranha II járművekére. A motor és a nyomatékváltó a jármű jobb oldalán elöl, az erőátvitel alkatrészei a jármű hossztengelyének megfelelően futnak és a kerékfelfüggesztés minden futómű esetében független. A hasznos tér a lehető legnagyobbra lett kialakítva a jármű hátuljában, itt lehet elhelyezni a fegyverrendszereket és a személyi állományt. A deszant tagjai a jármű hátsó részében egymásnak háttal foglalnak helyet, a későbbi átalakítások során már a külön egyenként függesztett üléseken egymással szemben.

A járműből való ki és beszállást a hátsó oldalon elhelyezett ajtón, illetve a járműtest tetején elhelyezett három búvónyíláson lehet megoldani. A vezető kilátását segítő periszkópok ugyanolyan elrendezésűek, mint a Piranha I járműben, a középső ezek közül szintén éjjellátóra cserélhető.

Az ezredfordulón a békefenntartó, békekikényszerítő szerep, vált hangsúlyossá, a tervezőknek gondolni kellett arra, hogy egy jármű bárhol a világban bevethető legyen, akár egy 7,62 mm-es géppuskával felszerelt APC akár egy 105 mm-es löveggel szerelt változatról van szó. A szállíthatóság esetében alapvető szemponttá vált, hogy szállítható legyen C-130-as repülőgéppel is.

Az 1998-tól a Kanadai Hadsereg számára készült kanadai építésű Piranha III-asok a Kodiak, [14] illetve az LAV III nevet kapták. Ezeket már nem a Detroit Diesel hanem a Catarpillar motorokkal szerelték. Az első szállítmány 1998 elejétől 1999 végéig érkezett, majd a további hét évben még, mintegy 410 db lett rendszerbe állítva. Ismét igény mutatkozott a nagyobb terhelhetőségre, ezt meg is oldották, illetve kiegészítő ballisztikai védőelemeket is kifejlesztettek rá. Újratervezték a járműtestet, a terhelhetőség 6.000 kg-ra nőtt a 8x8-as verzió esetében, a belső hasznos tér pedig 11 m^3 –re.

A konstrukció jelentős fejlesztései a Piranha I családhoz képest:

- a járműtestet előre, hátra lehet dönteni a GDELS-MOWAG által fejlesztett hidropneumatikus, szintszabályozóval ellátott felfüggesztésnek köszönhetően;
- a vezető állítja be a szükséges keréknyomást (CTIS);
- ABS rendszerrel szerelt fékek;
- nagyobb hasznos terhelés;
- nagyobb abroncsok (minimum 12,00 R 16);
- növelt belső tér, a meredekebb oldalfalaknak köszönhetően.

A STRYKER HARCJÁRMŰ – AZ AMERIKAI HADERŐ IGÁSLOVA

A Piranha III alapú Stryker modelleket azért célszerű külön tárgyalni, mert a legnagyobb darabszámban készült verzióról van szó. Az elmúlt másfél évtizedben mintegy 3000 db-ot vásárolt az amerikai haderő. *(3. ábra)* Ennek az eszköznek a beszerzése és alkalmazása olyan vitát kavart a szakértők körében, melyre talán a világ harcjármű piacán még nem volt példa. A járművet az M113 lánctalpas páncélozott csapatszállító eszköz leváltására és egy új harcrendi elem felállításának alapjaként állította rendszerbe az amerikai hadsereg. Harcérintkezéshez, békefenntartó, békekikényszerítő feladatokhoz tervezett modern többcélú kerekes járműre volt szükség.

Az egyik legfontosabb célja az eszközök beszerzésének, és az új alegységek létrehozásának, hogy a világ bármely pontján 96 órán belül bevethetőek legyenek. [15] A Stryker típust az ICV (Interim Carrier Vehicle) azaz átmeneti szállító jármű névvel látták el, utalva arra, hogy repülőgéppel szállítás után rövid időn belül hajtsanak végre katonai

feladatot. A későbbiekben derült fény arra, hogy a járőrözési tevékenységek során mennyire sérülékeny az eszköz valójában.

A Defence News folyóirat cikkei között kutatva ennek a harcjárműnek az eddigi kritikáit, és fejlesztését nyomon lehet követni. A típus bevezetésekor Chester A. Kojro[8] élesen bírálta a jármű páncélvédelmét és mozgékonyságát. [17] Az előd és testvérmodellek darabszámát tekintve elsőre nehezen érthető a bírálat, de kiderült, hogy nem volt alaptalan. Az eredeti acélpáncél vastagsága fél coll, azaz 12,7 mm, de az összetétele nem ismert.[9] [18] A világ egyik vezető ballisztikai acél gyártója a Ruukki termékei között megtalálható Ramor 500 lemez esetében is 16 mm-es vastagságot írnak elő a Stanag 4569 Level 2 szint, azaz a 7,62 54R B32 páncéltörő lőszer lövedékének kivédésére. Ebből egyértelműen látszik, hogy a jármű alap ballisztikai védelme nem volt képes kivédeni a 14,5 mm-es AP lövedékeket, [19] ezért kiegészítő páncélzatra volt szükség. A ballisztikai védelem ilyen szintű igénye, már a 90-es évek végén a Fuchs járművek esetében is realizálódott a délszláv válság idején. Az igényekre hamar megszületett a válasz. A már említett Fuchs fejlesztést is végző IBD vállalt által kínált kerámia páncél egy teszt során 20 db 14,5 mm-es amerikai lőszer ellen nyújtott sikeresen védelmet. [20] A kiegészítő készlettel felszerelt a Stryker járművek többségének tömege nem lépte át a kritériumként meghatározott 38.000 fontot (kb 17 t) amely a C-130-as szállító repülőgépek terhelhetőségnek felsőhatára volt. A repeszek elleni védelmet is növelni kellett erre a legkézenfekvőbb megoldás volt, hogy „spall liner”-t (repeszfogó takaró vagy függöny) szereltek a belső térbe.

A ballisztikai védelem mellett az IED elleni védelem is égetően fontossá vált. Egy fegyveres beavatkozás áldozatainak valós adatait ritkán lehet fellelni, de a védelmi igények alátámasztása érdekében szükséges legalább példákat említeni. A Defense News 2004 végén megjelent cikkében konkrétan írnak Stryker járművekben életüket vesztett katonákról. [21]

4. ábra. Stryker 3 DVH[10]

A következő évből is van adat mely szerint Irakban az addigi 345 dokumentált ellenséges támadásban tizenheten meghaltak, és 28 eszközt vesztettek. A következő fellelt információ szerint [22] Afganisztánban az IED támadások miatt 2009-ben 21 katona veszette életét és

[8] Chester Anthony Kojro többek között az amerikai hadsereg páncélos iskolájának tesztelő és értékelő osztályának vezetője volt a 80-as években. Material analyst United States Army Engineer School, Fort Wood, Missouri, since 1988. [16]

[9] A homogén acélpáncélok esetében a szerző saját tapasztalata alapján az 550 HB felületi keménységű, 11,4 mm vastag lemezt a 7,62x54R B32 páncéltörő puskalőszer lövedéke 6-ból egy esetben átütötte. A lövedék sebessége torkolati szintnek felelt meg, sebessége 810-830 m/s volt.

[10] Forrás: http://media.defenceindustrydaily.com/images/LAND_M1126_DVH_GDLS_lg.jpg (Letöltve: 2016.01.10.)

több mint negyven sebesült meg az 5. SBCT[11] állományában. Ez a veszteség volt a fordulópont, amely a jármű törzsének áttervezéséhez vezetett. A veszteségek tovább nőttek, hiszen Kandahar-ban, 2009 júniusában a második gyalogos zászlóalj még 37 katonát veszített és a sebesültek száma 238-ra nőtt egy év alatt. A veszteséggé vált eszközök alsó páncélja a futóművet kivéve teljesen sík volt. A 4. ábra első képe egy IED támadás után készült egy kanadai Kodiak járműről. A robbanás megsértette a külső opcionális védőelemeket. Minden valószínűség szerint az anyaga kevlár, legalábbis a sárgás szín, és a felső levált réteg erre utal.

Az akna elleni védelmet az eredeti elképzelések szerint egy gyorsan felszerelhető készlettel már a 2000-es évek elejére megoldották, de erről nincsenek részletes információk, és nem jelenthetett megoldást, hiszen a DVH csak a 2000-es évek végén jelent meg.

2009-ben 805 Stryker fejlesztését nyerte el a JWF Defense Systems by General Dynamics Land Systems - Canada. [23] A GDLS szerződése alapján 352 majd 450 szereltek fel Stryker járműveket DVH -val (doubble V-hull). Ezeket követte 2010 júliusában még 300 db eszköz. Az átalakítás jelentős mértékű volt, a járműtest alsó felének átalakítása más módosításoknak is teret adott.

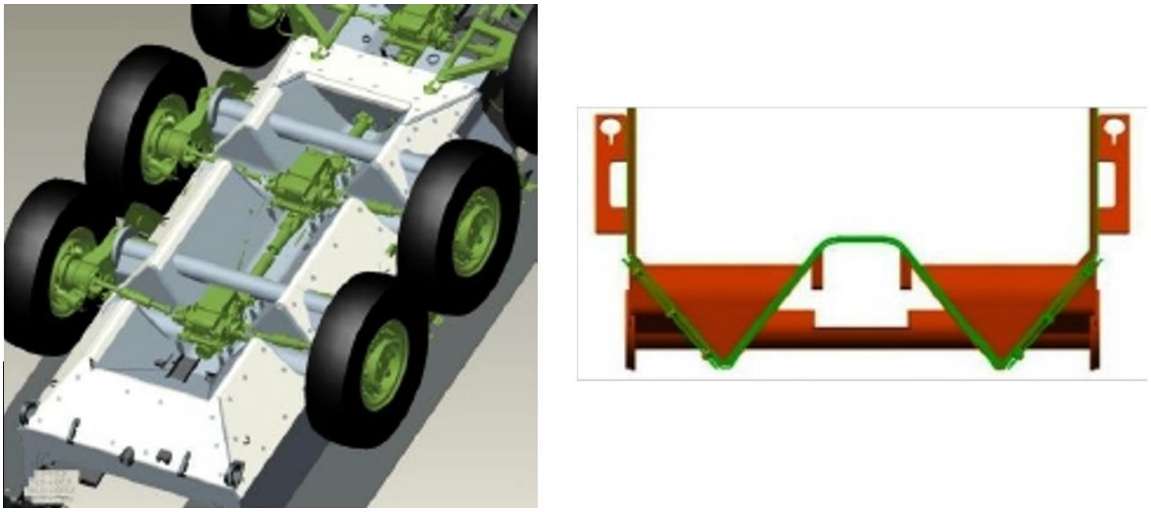
5. ábra. IED támadásban megsérült Kodiak[12] és Stryker ICV[13]

A DVH a jármű padlózatának teljes átalakítását jelentette. Már az 1970-es években, Afrikában alkalmazott megoldás volt a jármű hasán elhelyezett ék, vagy „V" alakú páncéllemez, amely képes volt elvezetni oldalirányba a jármű alatt elműködött robbanóanyag által keltett energiát. A Stryker járművek átalakításáról a GDLS által kiadott tájékoztató anyag részletesen beszámol, de a képek minősége a méretek miatt kifogásolható. [24] Az átalakítás lényegének az interneten talált vázlatrajz alapján való szemléltetés célú bemutatását elfogadhatónak találom, mivel a jármű futóművének elemei beazonosíthatóak, illetve a deszant tér alatti dupla „V" kialakítás megfelel a GDLS által kiadott anyagon szereplő vázlatrajzoknak. A DVH kialakítás olyan sikeres lett, hogy 2013-ban célul tűzték ki, hogy az Afganisztánban szolgáló LAV III járművek, majd később a teljes 550 db-ból álló kanadai flotta is megkapja.[25]

[11] Stryker Brigade Combat Team

[12] Forrás: http://www.armyrecognition.com/Amerique_du_nord/Canada/vehicules_a_roues/Bison_Coyote_Kodiak/Kodiak/Kodiak_Canada_news_02.jpg (letöltve: 2016.01.13.)

[13]Forrás: http://media.defenceindustrydaily.com/images/LAND_M1126_Stryker_ICV_IEDed_lg.jpg (letöltve:2015.11.14.)



6. ábra. Stryker DVH

A DVH rendszeren túl az eszközön belül az ülések a rugalmas felfüggesztéssel lettek a jármű oldalfalának belső felületére felszerelve. A kialakítás lényege, hogy a jármű alatti robbanás esetén a hirtelen gyorsulás nem közvetlenül az utasra hat, hanem van lehetőség csillapító elemek elhelyezésére az ülés és a járműtest között. Ez a megoldás jelentős mértékben növeli a túlélés esélyeit.

Felszerelésre került egy rács, melynek célja a kumulatív gránátok elleni védelem. Ennek az eszköznek a neve lehet „bar armor”, „slat armor” vagy „cage” azaz ketrec. Az első típus még acélötvözetből készült, de annak tömege mintegy 2,5-3 t volt. Ezt váltotta fel egy alumíniumötvözet kialakítás melynek becsült tömege körülbelül 1,5 t.

A Stryker több modernizáción is átesett, melynek tapasztalatait a GDELS is felhasználta a következő Piranha 3+ páncélozott csapatszállító jármű [26] kifejlesztése során. A jármű megengedett harci tömege az új futóműnek köszönhetően 27 t lehetett.

Nagy hangsúlyt helyeztek a fejlesztéskor a legénység komfortjára és védelmére, illetve a hosszú ideig tartó bevetéseket igyekeztek könnyebben elviselhetőbbé tenni.

A modul rendszerű védelem, már nem opcionális volt, hanem eleve a feladathoz lehet illeszteni az eszköz védelmi szintjét. A gyártó kínál úszóképes kivitelt is, de a szárazföldi alkalmazás vált meghatározóvá. A Piranha III alapú Stryker modellek esetében nem volt szükség úszóképességre az 1,5 m –es gázlómélység elégnek bizonyult az akadályleküzdéshez.

Új fejlesztés a tüzelőanyag takarékos hajtáslánc Fuel Efficient Driveline System (FEDS), melynek köszönhetően a nagy hatótávolság és a nagyon jó terepjáró képesség is egy időben megvalósítható. A hatótávolság valamelyest csökkent ugyan az elődmodellekhez képest, de a megnövekedett harci tömeg tükrében a 700 km is nagyon jó érték.

Az úszóképes verzió már az elődmodellekben bevált alkatrészekkel lett felszerelve, melyek tengeri körülmények között több államhadseregének alkalmazásában is bizonyítottak, a legkülönfélébb körülmények között.

PIRANHA IV – PIRANHA V

7. ábra. Piranha IV[14] és Piranha V

A Piranha IV típus *(6.ábra első kép)* soha nem lett rendszerbe állítva [27] de kitűnő alapként szolgált a Piranha V [28] járműhöz *(6. ábra második kép)*, mely 2010-ben gördült le először a gyártósorról. A technikai adatokon kívül sok információ még nem gyűlt össze az Piranha V járműről, de a modul rendszerű védelem, a fedélzeti kamerák, a függesztett ülések és a 40 éven keresztül fejlesztett hajtáslánc illetve futómű olyan műszaki színvonalat jelent, amelyre az alkalmazó haderők biztosan támaszkodhatnak. Az eszköz hajtásláncában már a hibrid technológia is szerepet kap, amely még 100 kW teljesítményt jelent a 430 kW teljesítmény leadására képes MTU dízelmotor mellé. Igény esetén a 13 t terhelhetőség még 3 t-val növelhető. A belső 14,3 m^3 térfogatú teret osztott klímaberendezéssel lehet hűteni. [39]

1. táblázat, Harcászati műszaki adatok (források:[9][12][30][31])

adatok/Piranha generációk	Piranha I 8x8	Piranha II	Piranha III	Piranha 3+	Piranha IV	Piranha V
hosszúság (mm)	6365	6980	6930	7770	7300	8000
szélesség (mm)	2500	2630	2660	2800	2800	2990
felépítmény magasság (mm)	2200	1850	2170	2310	2250	2340
has magasság (mm)	500	500	595	430	na.	na.
saját tömeg (t)	8,8	10	10,5	17	15	17
harci tömeg (t)	12,4	14	16,5	27	25	30/33*
terhelhetőség (t)	3,6	4	6	10	10	13
teljesítmény (kW)	220-257	202	294	na.	400	430/530**
fajlagos teljesítmény (kW/t)	17,7	14,4	17,8	15,3		14,3
maximális sebesség (km/h)	100	100	100	100	100	100
személyzet (fő)	2-3	na.	2-3	na.	3	3
deszant (fő)	12-13	na.	13-14	na.	6-7	8-10
szállítható személyek (fő)	15	16	16	13	9-10	13
lépcsőmászó képesség (mm)	500	600	650	750	700	750
árokáthidaló képesség (mm)	2000	na.	2000	2000	2000	2000
gázlómélység (mm)	na.	1,4	na.	1500	1500	1500
fordulókör átmérője (m)	15,4	16,5	16	18		15

[14] Forrás: http://www.military-today.com/apc/mowag_piranha_iv.jpg (letöltve:2016.01.13.)

kerékméret	11.00R16	na.	12.00R20	14.00R20		16.00R20
legnagyobb hatótávolság (km)	780	780	800		750	550
sebességváltó működési elve	aut.	aut.	aut.	aut.	aut.	aut.
sebességváltó fokozatok száma	5+1	5+1	6+1	7+2		7+1
központ abroncsnyomás állítás	nincs	opció	van	van	van	van
leküzdhető emelkedő (%)	60	70	60	60		60
megengedett oldal lejtő (%)	30	40	30	30		40

*igény esetén; **hibrid hajtás esetén elérhető teljesítmény; na. - nincs elérhető adat

ÖSSZEGZÉS

Több mint négy évtized folyamatos fejlesztését nehéz részletesen összefoglalni, de az adatok tanulmányozásával megállapítható, hogy:

- a járművek befoglaló méretei nőttek;
- saját tömegük közel megduplázódott;
- a terhelhetőségük majdnem háromszorosára nőtt;
- az akadályleküzdő képesség az adatok alapján nem változott jelentősen.

A fejlődés a védelmi képességekben viszont egyértelműen látszik. A kezdeti, nem bővíthető homogén acél páncél vastagságát növelik, és kiegészítő védőelemek fogadására előkészítik. Az eredmény Stanag 4569 Level 3 szintű védelem, amely tovább fokozható más kiegészítő elemekkel. A kiegészítő védőelemek tömegét csak jóval erősebb futómű és hajtáslánc képes kezelni. A műveleti tapasztalatok összességében igazolják az eszközök alkalmasságát a mai körülmények között, még az első generáció esetében is. A Stryker modelleket ért kritikák abban is tetten érhetőek, hogy a „betegágy” gúnynevet is megkapta[15], de a DVH rendszerrel felszerelt eszközök védelme jelentős előrelépés volt.
Érdemes viszont megkérdőjelezni, mennyire is vannak tisztában a hadseregek a saját igényeikkel rövid és hosszútávon. A negyedik Piranha generáció fejlesztését az angol FCLV (British Army’s Future Command and Liaisson Vehicle) programnak megfelelően kezdték meg, de az angolok más járművet választottak végül. Jól mutatja a mai igények reális felmérésének problémáját, hogy ez nem az első eset az elmúlt évtizedekben, amikor egy ilyen nagy haderő többször is kiszáll egy- egy projektből. A múltban ilyen volt az Artec fejlesztési projekt, melynek a végeredménye lett a Bundeswehr-ben rendszeresített BOXER MRAV legyártása. Ebben az esetben az eszközök mérete és szállíthatósága játszhatta a legnagyobb szerepet, mivel a példaként megemlített eszköz is közel 3 m magas és a 30 t-át a harci tömege meghaladja.

Felhasznált irodalom

[1] Nagy Éva, Helfrih Viktor: A modern haditechnika enciklopédiája (1945-től napjainkig), Guliver kiadó, 2001 ISBN 9639232173, p. 87

[2] Nagy Éva, Helfrih Viktor: A modern haditechnika enciklopédiája (1945-től napjainkig), Guliver kiadó, 2001 ISBN 9639232173, p. 76

[15] http://www.combatreform.org/strykerhorrors.htm

[3] Gyarmati József, Felházi Sándor, Kende György Choosing the Optimal Mortar for an Infantry Battalion's Mortar Battery with Analytic Hierarchy Process using Multivariate Statistics Decision Support Methodologies for Acquisition of Military Equipment. 176 p. Konferencia helye, ideje: Brussels, Belgium, 2009.10.22-2009.10.23. Brussels: NATO RTO, 2009. pp. 1-12. (ISBN:978-92-837-0101-9)

[4] Gyarmati József A nehézpuskát jellemző szempontok fontosságát kifejező súlyszámok számítása és statisztikai vizsgálata HADITECHNIKA 2006:(2) pp. 11-16. (2006)

[5] Dr. Bombay László, Gyarmati József, Dr. Turcsányi Károly: Harckocsik 1916-tól napjainkig, Zrínyi kiadó, Budapest, ISBN 9633273323, p.14

[6] Gávay György: Az IED eszközök által jelentett veszély a járművekre és az ellenük való védekezés lehetőségei, MŰSZAKI KATONAI KÖZLÖNY XXIV. évfolyam, 1. szám ISSN 2063-4986, p.63

[7] Chirstopher F. Foss: Jane's Armour and Artillery 1997-98, Coulsdon 1997, ISBN 0 7106 1542 6, pp. 501-502

[8] Vég Róbert: Defekttűrő és defektmentes gumiabroncsok, Bolyai szemle 2012. II. szám ISSN 1416-1443, p.179

[9] Chirstopher F. Foss: Jane's Armour and Artillery 92-93, Jane's Data division, Coulsdon 1992, ISBN 0710609973 p. 441-443.

[10] Chirstopher F. Foss: Jane's Armour and Artillery 2000-2001, ISBN 0716 20136 Coulsdon 2000, p. 397

[11] Chritopher F. Foss: First Piranha IIs for Oman completed on schedule, Jane's Defence Weekly 2001.09.26. p13

[12] Chritopher F. Foss: Jane's Armour and Artillery 2000-2001, Coulsdon 2000, ISBN 0716 20136, p.504

[13] Chirstopher F. Foss: Jane's Armour and Artillery 1997-98, Coulsdon 1997, ISBN 0 7106 1542 6, pp. 499-501.

[14] Chritopher F. Foss: Jane's Armour and Artillery 2000-2001, Coulsdon 2000, ISBN 0716 20136, p.409.

[15] Forrás: http://www.military-today.com/apc/stryker.htm (letöltve: 2015.12.13.)

[16] Forrás: http://prabook.org/web/person-view.html?profileId=518443 (letöltve: 2016.01.13)

[17] Letters – cím nélkül, Defence News 2001.01.05, (Proquest Military adatbázisából)

[18] Forrás: http://www.ruukki.hu/Acel/Melegen-hengerelt-aceltermekek/Ramor/Ramor- q pancellemez (Letöltve: 2015.11.10)

[19] Frank Tiboni: U.S. Army: Armored Vehicle Too Vulnerble to, Defense News 2 002.04.01. (Proquest Military adatbázisából)

[20] Frank Tiboni: New IAV Armor boosts protection for soliders, Defence News 2002.04.08 (Proquest Military adatbázisából)

[21] Eric Miller: Stryker Problems Highlight Testing Shortfalls, Defense News 2004.11.01. (Proquest Military adatbázisából)

[22] Forrás: http://www.defenseindustrydaily.com/us-army-moves-ahead-with-stryker-hull- modification-06308/ (letöltve: 2015.11.10.)

[23] Forrás: http://www.army-technology.com/projects/stryker/ (letöltve: 2015.12.15.)

[24] Forrás: http://leanermoreagileabct.com/pdfs/Stryker_brochure.pdf (letöltve: 2015.12.15.)

[25] 15 Peter Diekmeyer: Defending the true north, Jane's Defense Weekly, 2013.05.15. volume 50 issue 20 p.24-27 ISSN szám nélküli

[26] Forrás: https://www.gdels.com/brochures/wheeled_piranha8.pdf (letöltve:2015.11.15.)

[27] Forrás: http://www.military-today.com/apc/mowag_piranha_iv.htm (letöltve: 2015.11.17)

[28] Forrás: https://www.gdels.com/products/wheeled_2.asp?id=4 (letöltve:2016.01.17.)

[29] Chritopher F. Foss: Jane's Land Warfare platforms Aroured Fighting Vehicles, IHS, ISBN 09780710630100 2012 p.712

[30] Forrás: http://www.military-today.com/apc/bison.htm (letöltve:2016.01.17.)

[31] Forrás: http://www.military-today.com/apc/lav_25.htm (letöltve:2016.01.17.)

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Vég Róbert László
Vegh.Robert@uni-nke.hu

A MŰSZAKI DIAGNOSZTIKA SZEREPE A TECHNIKAI KISZOLGÁLÁSI ÉS JÁRMŰJAVÍTÁSI TEVÉKENYSÉGBEN

Absztrakt

Jelen korunkra jellemző a technika és a műszaki tudományok rohamos fejlődése. A járművek szerkezetileg és működés módjukat tekintve is lényegesen bonyolultabbakká váltak. A járművek műszaki állapotára csak a megfelelő diagnosztikai vizsgálatok alapján lehet következtetni, már nem elegendő a szerelő érzékszerveire hagyatkozni. A mai korszerű gépjárművek technikai kiszolgálása és javítása nem nélkülözi a korszerű diagnosztikai eljárások alkalmazását. A Magyar Honvédség páncélos- és gépjármű technikai eszközeinek fenntartása egy hatfokozatú tervszerű fenntartási rendszeren keresztül valósul meg. A cikk elhelyezi és értékeli a műszaki diagnosztika feladatát és szerepét a járművek technikai kiszolgálási és javítási folyamatában, és a Magyar Honvédség fenntartási rendszerében.

Our world today is strongly characterized by the rapid development of technology and engineering sciences. The complexity of the vehicle structures and vehicle systems is continuously increasing. Thus the observations and cognitions of the mechanics' organs are no more sufficient for measuring the technical condition of a vehicle. Nowadays we need adequate and exact diagnostically examinations, and these modern diagnostically procedures are indispensable for the repairment and maintenance of the vehicles. In the maintenance processes of the motor-vehicles and armoured technical assets, the Hungarian Defence Force employs a 6-point grading system. This article presents and evaluates the tasks and roles of the diagnostically procedures in the technical service and maintenance system of the Hungarian Defence Force.

Kulcsszavak: *gépjármű, műszaki, diagnosztika, járművizsgálat, karbantartás ~ vehicle, technical, diagnostics, vehicle inspection, maintenance*

HAGYOMÁNYOS KARBANTARTÁSI RENDSZEREK

Az alkalmazott karbantartási stratégiát a szükségletek és a lehetőségek határozzák meg. *A karbantartási stratégiákat meghatározó fontos feltételek:*

- az adott kor technikai szintje,
- a technikai eszköz konstrukciós sajátossága,
- a vezető és kezelő állomány felkészültsége és igényszintje,
- a járműpark nagysága,
- az érvényben levő hazai és nemzetközi előírások,
- az adott szervezeti keret rugalmassága (amelyben az üzemeltetés történik). [1]

A szakirodalom hagyományos karbantartási rendszereknek nevezi, a hibáig üzemelés rendszerét, a merev cikluson alapuló karbantartást, a megbízhatósági szint szerinti karbantartást és a diagnosztikai vizsgálatokon alapuló karbantartást.

Hibáig üzemelés rendszere

A rendszer azt jelentette, hogy az üzemeltetés tárgyát annak meghibásodásáig üzemeltettük, és ha a berendezés meghibásodott, akkor a rajta, vagy vele dolgozó személy azt megjavította. Ezen rendszer legfőbb hátránya, hogy a hibák teljesen váratlanul következnek be, ezáltal súlyos problémákat okozhatnak. A valóságban azonban a hibák ritkán következnek váratlanul, mert működik a felelősségteljes emberre építő „érzékszervi diagnosztika", ugyanis a gép mellett hosszú ideig dolgozó személy felismeri a berendezés megváltozott belső működésének jeleit. A hibáig üzemelés rendszere csak olyan helyeken működhet, ahol a dolgozó rendszeresen figyel a berendezés működésére. Ezen úgynevezett „érzékszervi diagnosztikán" alapuló karbantartás rendszerének hátránya a mérhetőség illetve regisztrálás hiánya. Ezt a karbantartási stratégiát olyan eszközöknél lehet alkalmazni, amelyek meghibásodása következménymentes. [2]

Merev cikluson alapuló karbantartás

A merev cikluson alapuló karbantartást Tervszerű Megelőző Karbantartásnak (TMK) nevezik, ami abból áll, hogy a berendezéseket (járműveket) egy meghatározott üzemidő vagy futásteljesítmény után ciklikusan ellenőrzésnek és karbantartásnak vetik alá. Az ellenőrzések közötti időtartamot úgy választják meg, hogy a műszaki állapotra jellemző paraméter értéke ne tudjon a megengedett és a meghibásodásra jellemző értékek közötti különbséggel változni. A 60-as években Magyarországon általánossá vált TMK rendszer célja a megbízhatóság és a tervezhetőség növelése volt, miközben az alkatrészek kihasználtsága romlott. A merev cikluson alapuló karbantartás rendszere a kádgörbén és a hozzá kapcsolódó elveken alapul.
A TKM rendszer alapelve:

- a hiba gyakorisága korfüggő,
- létezik egy jól definiálható határ a hasznos élettartam és a kijáródás között,
- képesek vagyunk ezt a kijáródási határt definiálni,
- a karbantartási egységciklust a berendezések elemeinek a leggyengébb láncszeme adja,
- az üzembiztonság nagyjavítással növelhető,
- a nagyjavítási ciklust a fenti műszaki megfontolások alapján állapítják meg.

A TMK rendszer esetén a legkényelmesebb a karbantartó feladata, mert a rendszer előírásai meghatározzák neki, hogy mikor mit kell tennie, és ezáltal mentesül az önálló döntések meghozatalával járó kockázatoktól. [3]

Megbízhatósági szint szerinti karbantartás

Ha a meghibásodások gyakorisága egy előre megadott szint alatt van, akkor a vizsgált berendezés rendszeres karbantartás és javítás nélkül tovább üzemeltethető. Ha a meghibásodások gyakorisága eléri a meghatározott felső határt, akkor külön ellenőrzésre vagy idő szerinti üzemeltetésre történő áttérést kell elrendelni. Ez a megbízhatósági szint szerinti karbantartási rendszer csak akkor alkalmazható, ha a műszaki üzembentartási rendszer lehetővé teszi a meghibásodások pontos rögzítését, gyűjtését és folyamatos kiértékelését. A műszaki vezetőnek folyamatosan figyelemmel kell kísérnie a technikai eszközpark állapotát, és a pillanatnyi üzemeltetési stratégiát is. Az irányítók munkája és felelőssége megnő, de egyben közelebb is kerülnek az üzemeltetés folyamatához. [4] [5]

A karbantartások elvégzésének megállapítása és azok szintjének kiválasztása ennek megfelelően egyfajta döntési folyamat, amely katonai műszaki alkalmazását írja le a [6] [7] irodalom.

Diagnosztikai vizsgálatokon alapuló karbantartás

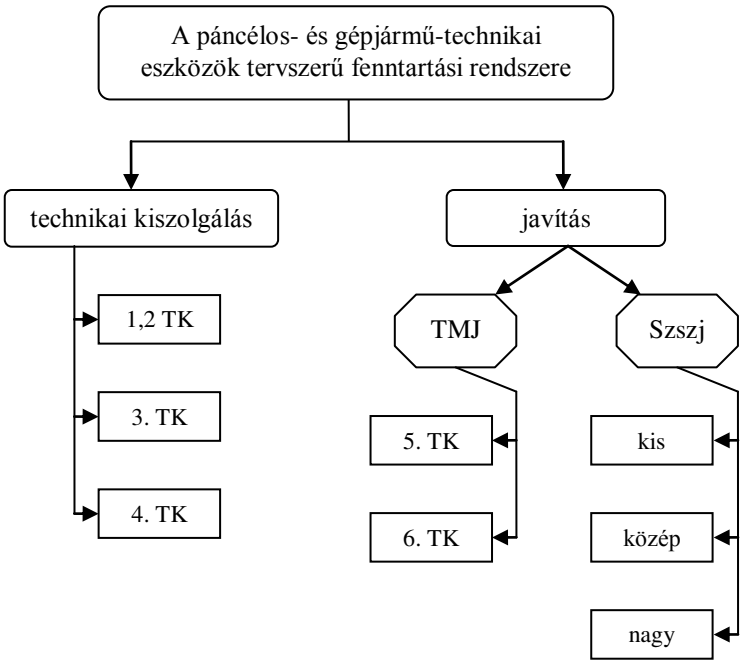
A diagnosztikai vizsgálatokon alapuló karbantartási rendszer esetén a gépen időszakosan, vagy folyamatosan műszeres műszaki állapotvizsgálatot végeznek, amely információkat felhasználnak a karbantartási és javítási munkákhoz. Az üzemeltetett gép állapotát a diagnosztikai vizsgálattal és a mért adatok kiértékelésével határozzák meg. Minden géphez hozzárendelhető egy vagy több, az adott gépre jellemző érték, amelynek mérése révén következtetéseket lehet levonni arra vonatkozóan, hogy mi játszódik le a gép belsejében. *Fontosabb mérhető jellemzők:*

- rezgés,
- ütésimpulzus,
- csapágyhőmérséklet,
- kenőolaj hőmérséklet,
- szivattyúk szívó- és nyomócsonkján mért nyomás,
- gumiabroncs nyomása üzem közben (pl. gumiabroncs nyomásvesztésére figyelmeztető rendszerek). [8]

Az időszakos diagnosztikai vizsgálaton alapuló karbantartás esetén a felülvizsgálatok időpontjait a gépek elhasználódási sajátosságainak figyelembevételével előre megállapítják és éves vizsgálati tervben rögzítik. Folyamatos állapotfigyelésnél a jelzőrendszer a gép kritikus pontjait folyamatos méréssel ellenőrzi. Ha az alsó riasztási értéknél nincs beavatkozás és a gép állapota tovább romlik, akkor a felső érték elérésekor a riasztási jelzőrendszer jelez és a rendszer le is állíthatja a gépet. A figyelő rendszer egy számítógéppel vezérelt ellenőrző rendszer, amely feldolgozza és tárolja a mérési eredményeket. A műszaki diagnosztika a diagnosztikai vizsgálaton alapuló karbantartás esetén, az állapotjelző paraméterek felhasználásával lehetővé teszi a gépek belső szerkezetének vizsgálatát, azok leállítása és szerelése nélkül. [9]

A MAGYAR HONVÉDSÉG PÁNCÉLOS- ÉS GÉPJÁRMŰ-TECHNIKAI ESZKÖZEINEK FENNTARTÁSI RENDSZERE

A páncélos- és gépjármű-technikai eszközök technikai kiszolgálása és javítása tervszerű fenntartási rendszer (TFR) keretei között kerül végrehajtása (1. sz. ábra). A TFR rendszer meghatározott rendszerben és mélységben, tervszerű megelőző jelleggel vagy szükség szerint végzendő technikai kiszolgálási és javítási feladatok összessége. A TFR rendszer biztosítja a páncélos- és gépjármű-technikai eszközök folyamatos, megbízható üzemkészségét, készletteljességét, előírt technikai állapotát és üzemeltetési tartalékát.



TJM – tervszerű megelőző javítás, Szszj – szükség szerinti javítás, TK – technikai kiszolgálás

1. ábra. A Magyar Honvédség tervszerű fenntartási rendszerének felépítése.[1]

A páncélos- és gépjármű-technikai eszközök tervszerű fenntartási rendszere hat fokozatból áll, amelynek első négy fokozata a végrehajtás szintje és a műveletek mélysége szerint tagolt technikai kiszolgálásokból, az 5. és 6. fokozat pedig a tervszerű megelőző javításokból áll. Minden technikai kiszolgálási fokozat technologizált műveletek összességéből áll. A technikai kiszolgálási fokozatok esedékességét naptári időnorma2, teljesítménynorma3 vagy végrehajtandó feladat4 határozza meg. A technikai kiszolgálási rendszer 1. TK és 2. TK fokozatát az üzemeltető alegység kezelő állományának, a 3. TK és 4. TK fokozatát pedig a kezelők bevonásával a szakjavító állománynak kell végrehajtani.

A szükség szerinti javítás a technikai kiszolgálások alatt felfedett, vagy a használat közben keletkezett meghibásodások, és azok előidéző okainak megszüntetését szolgálja. A páncélos-

[1] Saját készítésű ábra a Gépjármű igénybevételi szabályzat 5.1 – 5.2 alfejezetei alapján.
[2] Két technikai kiszolgálás között maximálisan megengedhető időtartam.
[3] Két technikai kiszolgálás között teljesíthető, az eszköz használatára jellemző paraméter mennyiség (üzemóra, lövésszám, kilométer).
[4] A technikai kiszolgálás valamelyik fokozatát meghatározott technikai állapot elérése érdekében feladat előtt vagy után kell elvégezni.

és gépjárműtechnikai eszközök szükség szerinti javítása a végrehajtandó műveletek mélysége szerint lehet kis-, közép- és nagyjavítás. A kisjavítás az eszköz jelentős megbontása nélküli, egyszerű alkatrészcserével végrehajtható javítás. A középjavítás az eszköz jelentős részének megbontásával járó, részegység vagy fődarab cserével végrehajtható javítás. A nagyjavítás az eszköz egészére kiterjedő, bonyolult szerelési és beszabályozási műveleteket igénylő, részegység és fődarabcserékkel végrehajtható javítás.

A tervszerű megelőző javítás (TMJ) célja az eszköz üzemképességének, műszaki paramétereinek és üzemeltetési tartalékának helyreállítása. A tervszerű megelőző javítások a fenntartási rendszer 5. TK és 6. TK fokozatát képezik. Az 5. TK az eszköz részleges felújítását, részegységekre bontását, az alkatrészek és részegységek javítását, beszabályozását jelenti, annak érdekében, hogy az eszköz elegendő üzemeltetési tartalékkal rendelkezzen a 6. TK végrehajtásáig. A 6. TK az eszköz teljes felújítását, ellenőrzését, az alkatrészek cseréjét, beszabályozások, hitelesítések elvégzését jelenti, annak érdekében, hogy az eszköz állapota a gyári újat megközelítő állapotot érjen el. [10]

A Magyar Honvédség állományába az utóbbi években, a missziós feladatok végrehajtása érdekében több5, más hadsereg által használt eszköz került. Ezen eszközök technikai kiszolgálása az Egyesült Államok Hadereje által használt preventív, ciklusrend alapján történő karbantartási rendszerrel (Preventive Maintenance Checks and Services – Megelőző Karbantartási Ellenőrzések és Javítások) valósul meg. A járművek karbantartási leírását technikai utasítások (Technical Manual) tartalmazzák. [11]

A MŰSZAKI DIAGNOSZTIKA FELADATA, SZEREPE

Az eszközöket diagnosztikai vizsgálat alá vetik többnyire a karbantartás és javítás során, vagy pedig a hatósági műszaki ellenőrzések alatt. Diagnosztikai vizsgálatoknak nevezzük a karbantartás, javítás során szemrevételezéssel és mérőeszközökkel végzett vizsgálatokat, amelyek az ellenőrzést, hibafeltárást és beszabályozást szolgálják. A hatósági ellenőrző vizsgálatok a közlekedésbiztonság és a környezetvédelem érdekeit szolgálják. A rendszeres diagnosztikai vizsgálatokkal több hiba is kimutatható, megelőzhető a váratlan üzemképtelenség, növelhető a gazdaságosság és a megbízhatóság. A műszerek objektív mérési eredményei a hosszas hibakeresést kizárják. A diagnosztikai vizsgálatok az eszközök fődarabjaira és részegységeire irányulnak.

A műszaki diagnosztika a gépészeti és mechatronikai rendszerek állapotminősítéséhez szükséges mérések és mérésadat-értékelés összefoglaló megnevezése. Az állapotminősítéshez szükséges információk megszerzése történhet állapotfelügyelettel (folyamatos), vagy állapotvizsgálattal (eseti). [12] [13]

A GÉPJÁRMŰ DIAGNOSZTIKA FELADATA, SZEREPE.

A gépjármű diagnosztika a műszaki diagnosztika alkalmazása. *A gépjármű diagnosztika két főcsoportra osztható:*

- nem fedélzeti diagnosztika (off-board diagnosztika),
- fedélzeti diagnosztika (on-board diagnosztika).

A nem fedélzeti diagnosztikai állapotvizsgálathoz szükséges elemek nem integrál elemei a gépjárműnek, ezen elemeket (mérőeszközöket) a rendszerhez csatlakoztatni kell. A járműbe épített fedélzeti diagnosztikai (emisszió felügyelő) rendszer az irányítóegység hibatárolójába eltárolt hibák segítségével jelzi ki a hibás működést, és annak valószínű okát. A diagnosztikai

[5] pl. Cougar, HMMWV

állapotvizsgálathoz szükséges elemek a gépjárműnek integrált elemei. A diagnosztikai rendszerben a mérések folyamatosan vagy periodikusan történnek, a mérés adatainak feldolgozására időközönként kerül sor. A felismert hiba azonosítója6 a vezérlőegység hibatárolójában, a későbbi kiolvasás céljából megőrződik. A gépjármű vezérlőegységét a diagnosztikai műszer egy közös diagnosztikai csatlakozón (OBD) keresztül éri el. [14]

Az irányított rendszerek vizsgálatát feloszthatjuk:

- irányítóegység-kapcsolatú rendszerdiagnosztikára, amely lehet,
  - soros diagnosztika (fedélzeti on-board soros diagnosztika),
  - párhuzamos diagnosztika,
- periféria diagnosztikára.

A rendszer irányítóegysége az egységek és a funkciók ellenőrzését végzi el folyamatosan, illetve gyakori mintavételezéssel, pl. az indirekt TPMS7 rendszerek. [15]

Az állapotfelügyelet a rendszerállapotban bekövetkező rendellenességekről a javítás számára diagnosztikai információt ad, amely információk a soros diagnosztika keretében olvashatóak ki a rendszerteszter8 műszerrel.

A rendszerfelügyelet diagnosztikai funkciói:

- a hibák felismerése,
- állapotjavító intézkedések bevezetése,
- a vezető informálása a műszaki állapotban bekövetkezett romlásról, a hibás és a korlátozott üzemről,
- a hibaazonosító kód tárolása.

Párhuzamos diagnosztika esetén a vizsgálat a működéssel egy időben történik, ahol a működő rendszer hálózatán, a hálózati elemekre csatlakozva lehet nyomon követni a működést.

Periféria diagnosztikáról akkor beszélünk, ha az érzékelő, beavatkozó elemek vizsgálatát az irányítóegységről leválasztott vezetékhálózat esetén végezzük el. A mérés végrehajtásához szükséges a mérést végrehajtó személy részletes rendszerismerete, a gyári számozással, vezetékszínekkel megadott kapcsolási rajz. A diagnosztika módszere a szakaszmérésekkel történő kizárásos hibahely behatárolás. [16]

DIAGNOSZTIKAI VIZSGÁLATOK A PÁNCÉLOS- ÉS GÉPJÁRMŰTECHNIKAI ESZKÖZÖK TECHNIKAI KISZOLGÁLÁSI MŰVELETEIBEN

A páncélos- és gépjárműtechnikai eszközök technikai kiszolgálási műveletei meghatározásra kerültek a különböző anyagismereti és igénybevételi, és egyéb utasításokban. Elő lett írva, hogy melyik technikai kiszolgálás során kinek, milyen feladatot kell végrehajtania, és a járműnek milyen műszaki követelményt kell kielégítenie. Az 1. sz. táblázat bemutatja különböző járművek 1-4 TK műveleteinek megoszlását aszerint, hogy szemrevételezésen vagy pedig műszeres diagnosztikán alapul-e. A táblázatban szereplő járművek közül az UAZ-469B terepjáró személygépkocsi nincs ellátva fedélzeti vezérlőegységgel, a MB G-270 CDI terepjáró személygépkocsi viszont igen, így ez a jármű öndiagnosztikára alkalmas.

[6] A hibakód és a paraméter környezete.
[7] TPMS: Tire Pressure Monitoring System, azaz gumiabroncs nyomásellenőrző rendszer.
[8] Diagnosztika műszer, amely a szabványos protokoll szerint működő szoftvert tartalmazza.

1. táblázat. A TK műveletek megoszlása különböző járművek esetében

UAZ-469B [17]				
	1.TK	**2.TK**	**3.TK**	**4.TK**
Előírt műveletek száma (db)	25	25	66	20
Szemrevételezéssel[9] végrehajtott műveletek száma (db)	25	24	57	16
Műszaki diagnosztikával végrehajtott műveletek száma (db)	0	1	9	4
MB G-270 CDI [18]				
	1.TK	**2.TK**	**3.TK**	**4.TK**
Előírt műveletek száma (db)	26	31	17	16
Szemrevételezéssel végrehajtott műveletek száma (db)	25	30	14	14
Műszaki diagnosztikával végrehajtott műveletek száma (db)	1	1	3	2

Az UAZ-469B terepjáró személygépkocsi 1.TK és 2.TK végrehajtása során a mérőeszközökkel végrehajtott vizsgálatok száma elenyésző, mindössze az akkumulátor töltöttségére korlátozódik, de ez természetesnek is tekinthető, mivel ezeket a feladatokat a gépjárművezető hajtja végre, és ő nem rendelkezik bonyolult szerszámokkal és műszerekkel. A 3.TK műveletei között már megjelennek konkrét diagnosztikai feladatok is, mint a szelephézag és a gyújtógyertya elektródahézag vagy a megszakító hézag állítása, de ezek viszonylag egyszerű vizsgálatok és nagy műszer igényük nincs. A kipufogógáz összetétel vizsgálata, a kerékösszetartás ellenőrzése, a fékberendezés működésének ellenőrzése és a fényszóró beállítás ellenőrzése viszont konkrét diagnosztikának tekinthető. A 4.TK műveleteinél megjelenik a sűrítési végnyomás mérése, a tüzelőanyag-fogyasztás műszeres mérése, a gyújtás vizsgálata és a lengéscsillapítók működésének vizsgálata.

A MB G-270 CDI terepjáró személygépkocsi technikai kiszolgálási műveletei nem térnek el lényegesen az UAZ-469B típusétól. Az 1.TK és a 2.TK műveletei között csak a gumiabroncsok nyomásellenőrzése és a profilmélység ellenőrzése szerepel. A 3.TK műveletei között megjelenik a fékrendszer próbapadi ellenőrzése mellett a motor működésének ellenőrzése diagnosztikai készülékkel is, ahol lehetőség van a tárolt hibák kiolvasására. A 4.TK műveletei között is igen kevés diagnosztikai vizsgálat található, mindössze a fényszórók beállításának ellenőrzése és a kormánygeometria ellenőrzése jelenik meg.

ÖSSZEFOGLALÁS

A különböző szakirodalmakban kiemelkedő helyet foglal el a műszaki diagnosztika, mint a javítási és karbantartási tevékenység egy fontos és meghatározó eleme. A műszaki diagnosztika kizárja az érzékszervi diagnosztika pontatlanságát és szubjektív jellegét, alkalmazásával növelhető a gazdaságosság és a megbízhatóság. A valóságban viszont az látható, hogy a technikai kiszolgálási műveleteknek csak egy csekély részét foglalja le a műszaki diagnosztika, a feladatok nagy része az érzékszervi diagnosztikán alapul. A két járműtípus összehasonlításából az is látható, hogy hiába a hatalmas technikai szintkülönbség a két jármű között, mégsem alkalmazzák szélesebb körben a diagnosztikai vizsgálatokat.

[9] Szemrevételezéssel, manuálisan kéziszerszámokkal, műszeres diagnosztika nélkül végrehajtott.

Felhasznált irodalom

[1] Dr. Pokorádi László: Karbantartás elmélet. Debrecen, Elektronikus tansegédlet, 2002. 5. p.

[2] Vég Róbert: Technikai kiszolgálási műveletek összehasonlító vizsgálata a GAZ-66 és U-4000 terepjáró tehergépkocsiknál. Bolyai Szemle különszám (HADITECHNIKA 2004-szimpózium). Budapest: ZMNE nyomda, 2004. 1. p. ISSN: 1416-1443.

[3] Péczeli György: A karbantartás korszerű irányzatai (A.A.Stádium Kft IX. évf. 2002.). 2.4.2. alfejezet.

[4] Békési Bertold: A katonai repülőgépek üzemeltetésének, a kiszolgálás korszerűsítésének kérdései. Budapest, Doktori (PhD) értekezés, 2006.). 23. p.

[5] Dr. Pokorádi László: Karbantartás elmélet. Debrecen, Elektronikus tansegédlet, 2002. 6. p.

[6] Gyarmati József, Kende György, Turcsányi Károly Haditechnikai eszközök összehasonlításának korszerű módszerei és ezek alkalmazása HM 2002. évi kutatási terv 6.1. program 1. alprogram (2002)

[7] Gyarmati József, Felházi Sándor, Kende György Choosing the Optimal Mortar for an Infantry Battalion's Mortar Battery with Analytic Hierarchy Process using Multivariate Statistics In: Gyarmati József, Kende György, Felházi Sándor Decision Support Methodologies for Acquisition of Military Equipment. 176 p. Konferencia helye, ideje: Brussels, Belgium, 2009.10.22-2009.10.23. Brussels: NATO RTO, 2009. pp. 1-12. ISBN: 978 92 837 0101 9

[8] Vég Róbert: Defekttűrő és defektmentes gumiabroncsok. Bolyai Szemle 2012. XXI. évf. 2. szám. Budapest: NKE kiadványa. 6. p. ISSN: 1416-1443.

[9] Szabó József Zoltán: Rezgésdiagnosztikai vizsgálatok és haditechnikai alkalmazhatóságuk kutatása. Budapest, Doktori (PhD) értekezés, 2010.). 22-23. p.

[10] Gépjármű igénybevételi szabályzat. A Magyar Honvédség kiadványa, 2015. 5.1 – 5.2 alfejezetek.

[11] Gávay György: A Tervszerű Fenntartási Rendszer és az amerikai forrásból származó páncélos- és gépjármű-technikai eszközök karbantartási rendszere – Honvédségi szemle, 143. ÉVFOLYAM 2015/4. 85-92 p.

[12] Dr. Lakatos István – Nagyszokolyai Iván: Gépjármű diagnosztika. Képzőművészeti Kiadó Kft., 2006. 9-14. p. ISBN: 963 336 960 6.

[13] Kovács László: Gépjárművizsgálat, -javítás. Műszaki Könyvkiadó, Budapest, 1993. 9-5. p. ISBN: 963 16 0045 9.

[14] Tölgyesi Zoltán: Fedélzeti diagnosztika. Maróti Könyvkereskedés és Könyvkiadó Kft., Budapest, 2005. 9-15. p. ISBN: 963 9005 70 3.

[15] Vég Róbert László – Palkovics András: Gumiabroncs nyomásellenőrzése. Bolyai Szemle 2013. XXII. évf. 1. szám. Budapest: NKE kiadvány, 2013. 27-28. p. ISSN: 1416-1443.

[16] Dr. Lakatos István – Nagyszokolyai Iván: Gépjármű diagnosztika. Képzőművészeti Kiadó Kft., 2006. 67-71., 83. p. ISBN: 963 336 960 6.

[17] Gjmű/126. Az UAZ-469B típusú terepjáró személygépkocsi anyagismereti és igénybevételi utasítása. A Honvédelmi Minisztérium kiadása, 1976. 341-357. p.

[18] Utasítás a MB G-270 CDI BA 4, BA6/PK, BA10/F típusú terepjáró személygépkocsik karbantartásához és technikai kiszolgálásához. A Magyar Honvédség Szárazföldi Parancsnokság Logisztikai Főnökség. 3-8. p.

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Csősz László
csoszlaszlo@uni-nke.hu

VESZÉLYES IPARI TEVÉKENYSÉGEK, MINT POTENCIÁLIS VÍZSZENNYEZŐK A SZIGORODÓ SZABÁLYOZÁS TÜKRÉBEN

Absztrakt

A vízminőségvédelemmel kapcsolatos feladatok összetett és fejlődő problémakört alkotnak, amely a szakemberek részéről komoly szakértelmet és felkészültséget kíván. Emberi, illetve műszaki hibákból adódóan rendszeresen előfordul, hogy a vízkészletek elszennyeződnek valamilyen formában. A balesetek okai között a legtöbb esetben megtalálható az emberi tényező, ha a műszaki okokat tekintjük, szintén nyomon követhető az emberi mulasztás. Mivel a felszíni vizek gyakran szolgálnak vízkivételi forrásként, rendkívül fontos, hogy a mindennapi veszélyes ipari tevékenységek mellett is megőrizzék a minőségüket. Ehhez jogi szabályozások, az ezekre alapozó következetes hatósági tevékenység és a vízügyi szervek felkészült munkája, illetve az elsődlegesen beavatkozók szakszerű és hatékony tevékenysége szükséges. Jelen cikk célja, hogy röviden bemutassa az ipari tevékenységeket szabályozó irányelvek kialakulásának előzményeit, az irányelvek fejlődését, illetve konkrét eseteken szemléltesse az ipari eredetű vízszennyezések legfőbb okát.

The tasks related to water quality protection consitute a complex and developing set of problems, wich require serious skills and preparedness of the experts. Resulting from human and technical defects it regularly occurs that water stocks in any form contaminate. Among the reasons of accidents the human factor can be found in most of the cases, if considering technical reasons, human faliure is also traceable. Because the surface waters often serve as water intake sources, it is extremely important to retain their quality even beside the daily dangerous industrial activities. It requires legal regulations, consequent authority actions and the prepared work of damagest he workmanlike and efficient activity of the primary interveners. The purpose of this article is to briefly represent the antecedents of the development of guidelines regulating indusrtial activities and the development of guidelines and to demonstrate the main reason of water contaminations of industrial origin on particular cases.

Kulcsszavak: *civilizációs veszélyforrások, veszélyes üzemek, Seveso irányelvek, vízszennyezések, ~ civilizational threat, hazardus plants, Seveso directives, water pollution*

BEVEZETÉS

Földünk népessége már a kezdetektől ki volt téve a különböző veszélyforrásoknak, leginkább a természeti eredetű katasztrófáknak. Az emberiségnek több évszázadon keresztül csak természeti eredetű veszélyekkel kellett szembenéznie. Az egyes társadalmi berendezkedések kialakulási folyamatai háborúkat, valamint különböző járványokat hoztak magukkal. A technológia, a tudomány és a gazdaság fejlődését követően, amelyek elhozták az ipari forradalmat, új veszélyforrások jelentek meg. Ezek az új veszélyforrások a különböző civilizációs, emberi eredetű veszélyek, katasztrófák voltak.

Az ipari forradalmat követően megsokszorozódott, ugrásszerűen megnőtt ezen balesetek, szerencsétlenségek száma. Az újonnan megjelenő katasztrófatípusoknál túlnyomó részben meghatározó szerepet játszik az emberi tevékenység, a helytelen emberi beavatkozás, mulasztás, figyelmetlenség, illetve a műszaki vagy konstrukciós hibák, amelyek szintén emberi tényezőre vezethetőek vissza. Több tanulmány is készült az emberi tényező szerepéről, legteljesebben Rachel P.E. Gordon a The contribution of human factors to accidents in the offshore oil industry című tanulmányában részletezte, hogy az ember milyen súlyos szerepet tölt be az egyes üzemi balesetek, katasztrófák esetében.[1] Najmedin Meshkati Human factors in large-scale technological systems accidents: Three Mile Island, Bhopal, Chernobly című tanulmányában a három megnevezett szerencsétlenség részletezésével mutatta be szintén az emberi tényező szerepét.[2] A történelem folyamán számtalanszor előfordult, hogy az ipari tevékenységek során a vízkészletek valamilyen formában elszennyeződtek.

Az ipar fejlődését tekintve prognosztizálható, hogy a későbbiekben is előfordulnak majd hasonló ipari eredetű szennyezések. Éppen ezért úgy gondolom, hogy az ipari eredetű vízszennyezések aktuális téma és a későbbiekben sem fog veszíteni aktualitásából, mivel egy fejlődő problémakört alkot.

AZ IPAR, MINT VESZÉLYFORRÁS

A növekvő iparosítással párhuzamosan növekedett a veszélyes anyagokkal kapcsolatos súlyos balesetek száma is. Az ipari balesetek elhárítására kidolgozott irányelvek az európai történelem egyik legsúlyosabb vegyi katasztrófája után születtek.

1976. július 10-én egy észak-olaszországi kisvárosban, Sevesoban működő gyógyszer- és kozmetikum alapanyagokat előállító vegyi üzemben robbanás történt, melynek következtében körülbelül 3000 kilogramm különböző veszélyes anyag került ki gőz formájában az üzemből, amely hat kilométer hosszú és egy kilométer széles sávban borította be a vegyi üzem környezetét.[3] A vegyületek között fellelhető volt például a dioxin is, amely néhány mikrogrammnyi mennyiségben is halálos mérgezést okoz. A balesetet 10 napig titokban tartották, amíg furcsa dolgokat nem kezdtek észlelni a vegyi üzem környezetében élő emberek. A fák idejekorán hullatni kezdték leveleiket, a háziállatok váratlanul elpusztultak. Továbbá a lakosságon bőrelváltozások jelentkeztek, főleg a gyerekeken. A katasztrófa 37 ezer embert érintett. Közel 200 ember szenvedett súlyos sérüléseket. 11 ezer embert kellett kitelepíteni a vegyi üzem közvetlen közeléből.[3] A hatóságok továbbá 80 ezres nagyságú állatállományt semmisítettek meg, hogy megakadályozzák a mérgező dioxin táplálkozással való emberi szervezetbe jutását. A helyben termesztett élelmiszerek fogyasztását hosszú időre megtiltották. A szennyezés hatása azonban ennél is súlyosabb volt, ugyanis az újszülöttek körében jelentősen nőtt a születési rendellenességek aránya, valamint nőtt a koraszülések, illetve a vetélések száma is. Az Európai Parlament küldöttsége a katasztrófát követően a helyszínre látogatott, hogy felmérje a helyzetet és hat évvel később megszületett a SEVESO I. irányelv, amely megszigorította a vegyi anyag gyártás ellenőrzését.

Az egyetlen megoldás, hogy a közeljövőben ne következzenek be hasonló szerencsétlenségek, a gondos felügyelet, ugyanis a vegyi üzemeket nem lehet bezárni. A vegyipar igen jelentős szerepet tölt be mindennapi éltünkbe. A modern társadalmakban ez élet szinte elképzelhetetlen a vegyipar termékei nélkül. Ezek hiányában például leállna a közlekedés jelentős része, minden benzinnel vagy olajjal hajtott jármű, megbénulna az áruszállítás, leállna több iparág is, mint például a gépipar, a textilipar, továbbá megszűnne a gyógyszerellátás, eltűnnének a festékek, mosóporok, tisztítószerek és még hosszasan lehetne sorolni. mindezeken kívül a különböző vegyi anyagoknak a gyártása több milliárd eurós exportágazata az Európai Unió vállalatainak, minden veszély ellenére. Az egyik fő probléma többek között leginkább az, hogy a vállalatok sokszor nem akarják tájékoztatni az embereket arról, hogy mit tegyenek vegyi baleset esetén. A gyárak egyik fő célja ugyanis a profit termelés és mivel a biztonsági intézkedéseknek súlyos anyagi vonzatai vannak, ez a folyamat a sevesoi katasztrófa tanulságai ellenére van, hogy a mai napig háttérbe szorul.

Seveso I. irányelv szabályozása

Az Európai Unió Tanácsának 1982. június 24-i (82/501 EGK számú) SEVESO I. irányelve foglalkozott először átfogóan az egyes ipari tevékenységgel járó súlyos baleseti kockázatokkal. [4] Az Európai Unió meghatározta tagállamai számára, hogy legkésőbb 1986. január 8-ig tegyék meg azon belső jogi intézkedéseket, amelyek szükségesek a SVESO I. irányelv előírásainak megvalósításához. A SEVESO I. már nem hatályos, azonban a jelenlegi európai ipari baleseti megelőző és elhárító rendszerek ezen irányelv alapján jöttek létre.
A SEVESO I. irányelv kiemelte [4]:

- a lakosság, a környezet védelme, illetve a munkahely biztonsága továbbá az egészségvédelem megköveteli, hogy különös figyelmet fordítsanak az ipari tevékenységekre, amelyek nagyobb balesetek okozói is lehetnek;
- minden olyan ipari tevékenységnél, ahol valamilyen veszélyes anyagot alkalmaznak vagy alkalmazhatnak, és így nagyobb baleset esetén sokkal súlyosabb hatásokkal kell számolni az emberre és a környezetre nézve, szükséges, hogy a gyártó minden rendelkezésre álló eszközzel elejét vegye a balesetek bekövetkezésének, illetve mérsékelje azok következményeit;
- azon ipari tevékenységeket, amelyek különösen veszélyes anyagokat alkalmaznak vagy alkalmazhatnak bizonyos mennyiségben, fontos, hogy a gyártó közölje az illetékes hatósággal a szóban forgó anyagokra vonatkozó adatokat, információkat.

A SEVESO I. irányelv egyik hangsúlyos része volt a súlyos ipari balesetek megelőzését és elhárítását szolgáló egységes irányítási rendszer nemzeti jogszabályok alapján történő kialakítása. Az Uniós tagállamoknak biztosítaniuk kellett, hogy a súlyos balesetekre a különböző biztonsági intézkedéseket az üzemeltetők elemezték, illetve gondoskodtak a kidolgozásukról. A SEVESO I. irányelv szerint a tagállamoknak továbbá ki kellett alakítaniuk azokat az illetékes hatóságokat, amelyek megszervezték a veszélyes létesítmények felügyeletét, ellenőrző tevékenységet láttak el, valamint gondoskodtak arról, hogy a veszélyes létesítményen kívüli mentési tervek szintén kidolgozásra kerüljenek. A veszélyes ipari létesítmények üzemeltetőinek az illetékes hatósághoz nyilatkozatot kellett eljuttatniuk, amely nyilatkozat tartalmazta a veszélyes létesítmény vagy veszélyes üzem pontos nevét és címét, a felelős igazgató nevét, a gyártás vagy tárolás típusát, valamint az alkalmazott vagy tárolt anyagokat. [4] A tagállamoknak arról is gondoskodniuk kellett, hogy a veszélyes létesítmények üzemeltetői 1989. június 8-ig elkészítsék és eljuttassák az illetékes hatósághoz azokat a kiegészítő információkat, amelyeket a súlyos balesetek megelőzése érdekében, valamint következményeiknek csökkentése érdekében hoztak. A SEVESO I. irányelv előírásai szerint a nyilvánosságot, a lakosságot tájékoztatni volt köteles a veszélyes üzem, létesítmény tulajdonosa a meghatározott ipari tevékenységről, illetve a lehetséges balesetek

káros következményeiről. Ezeket a tájékoztatókat rendszeresen meg kellett ismételni, azonban az irányelv nem szabott erre vonatkozóan határozott időnormákat.

Az Európai Unió tagállamainak képviselőiből megalakítottak egy bizottságot, amelynek feladata egyrészt az irányelv időszakonkénti felülvizsgálata és összehangolása volt a műszaki haladással, másrészt információcserére szolgált a súlyos balesetek megelőzése és következményeiknek csökkentése területén szerzett gyakorlati tapasztalatokról. Ennek érdekében a tagállamok közölték a Bizottsággal, hogy mely intézménynél található az illetékes hatóságuk, és tájékoztatót adtak a területükön bekövetkezett súlyos balesetekről. A Bizottság gyűjtötte és elemezte a rendelkezésre álló adatokat, és a következtetéseket a tagállamok számára rendelkezésre bocsátotta.

Jelentős és fontos lépés volt a SEVESO I. direktíva megalkotása. A sevesoi katasztrófa után felismerték, hogy elejét kell venni az egyre több áldozatot követelő súlyos ipari balesetek bekövetkezésének, amely csak szigorú szabályozással valósítható meg. Már ezen direktíva megalkotásakor is tisztán körvonalazódott, hogy meg kell határozni egyes feladatokat, tevékenységeket, hogy minimalizálják az ember által okozott balesetek bekövetkezését. A SEVESO I. szilárd alapot képezett, amely lehetővé tette az irányelv későbbi továbbfejlődését. Ennek köszönhetően egy szigorú ám még kiegészítésekre szoruló szabályzóra épülhetett a SEVESO II. irányelv.

Seveso II. irányelv

A történelem addigi legtöbb halálos áldozatot követelő vegyi katasztrófája 1984. december 3-ára virradó éjszakára következett be, amikor mérgező gázok szabadultak ki az amerikai tulajdonú Union Carbide vegyipari cég növényszereket gyártó indiai telephelyű üzemében, Bhopalban. [5] Órák alatt közel 8 ezer ember fulladt meg a várost beborító, fojtogató metil-izocianát gázfelhőben. A katasztrófát követően megnőtt a születési rendellenességek és a torz születések száma, valamint 120 ezerre tehető a krónikus megbetegedéssel élők száma. A vegyi üzemet azonnal bezárták. A lefolytatott vizsgálat kiderítette, hogy az üzemben óvintézkedések alig történtek, a biztonsági rendszert takarékossági okokból pedig ki sem építették.

A bhopali tragédia jól mutatta, hogy a SEVESO I. irányelv szigorúbb szabályozása sem tudta kiküszöbölni a civilizációs katasztrófák létrejöttének egyik legjellemzőbb tényezőjét, magát az embert, vagyis az emberi hanyagságot és felelőtlenséget. Az irányelvet módosítani kellett további kiegészítésekkel. Létrejött „Az ipari balestek országhatáron túli hatásairól és kezeléséről szóló (Helsinki) egyezmény" az ENSZ égisze alatt, illetve a SEVESO II. irányelv, amelyek a fentiekhez hasonló balesetek elkerülését, a veszély csökkentését, a biztonság növelését tűzték ki célul. [5] Az ipari balesetek országhatáron túli hatásairól szóló egyezményt vagyis a Helsinki Egyezményt 1992. március 17-én írták alá a tagállamok és 2000. április 19-én lépett hatályba. Az egyezmény létrejöttére időben a két irányelv, a SEVESO I. és a SEVESO II. irányelv megszületése között került sor. A Helsinki Egyezmény előkészítő munkái folyamán figyelembe vették a SEVESO I. addigi gyakorlati tapasztalatait és a SEVESO II. előkészítő tanulmányait is. Az Egyezmény célja a nemzetközi együttműködés elősegítése az érintett államok között, ezen belül a súlyos balesetek országhatáron túl terjedő hatásainak megelőzése, a felkészülés, a kölcsönös segítségnyújtás, illetve a gyors tájékoztatás és információ csere a tagállamok között. Nemzetközi szinten az információk cseréjével, konzultációkkal és egyéb együttműködési lehetőségekkel, összehangolt stratégia kidolgozásával teremtik meg a balesetek, katasztrófák kockázatának csökkentését. Az Egyezmény 3. Cikkelyében kerül megfogalmazásra, hogy az üzemeltetőnek minden szükséges intézkedést meg kell tennie a súlyos balesetek veszélyének mérséklése érdekében. A 6. Cikkely részletezi a megelőzéssel. A súlyos ipari balesetek megelőzésének, illetve azok káros hatásai minimalizálásának alapjában két fontos eleme, illetve előfeltétele van: az egyik, hogy mindenki, aki veszélyes üzem, létesítmény környezetében él megfelelő

információval rendelkezzen az üzem tevékenységéről, az anyagokról, a veszélyforrásokról, a kockázati tényezőkről, a másik az, hogy egy megfelelő gyakorlati intézkedési programcsomag álljon rendelkezésre, amely a részleteket is figyelembe véve osztja ki a feladatokat, hatásköröket, valamint a felelősséget. Az Egyezményt aláíró felek intézkedéseket hoznak az ipari baleseti kockázatok megelőzésének csökkentéséére és egyúttal megkövetelik az üzemeltetőtől a veszélyes tevékenység biztonságos működtetésének bizonyítását, megfelelő információk rendelkezésre bocsátásával. Az egyezmény főbb pontjai [6]: potenciális veszélyek és veszélyeztetett terültek felmérése; helyi körülmények feltérképezése; riasztási eljárások és következtetések; felkészülési tervek kialakítása.

Az ipari balesetek országhatáron túli hatásairól szóló egyezmény fő vonalait tekintve hasonlóságot mutat a SEVESO II. irányelvben meghatározott elvekhez. [6] Az Egyezmény a veszélyes tevékenységek elemzésére és értékelésére megfelelő mennyiségű útmutatást ad, amely alkalmazható a SEVESO II. irányelvben megfogalmazott elemzések elvégzéséhez is. Ezen elemzéseket az üzemeltetők, az illetékes hatóság, illetve a helyi hatóságok csak együttesen, egymás folyamatos informálásával, tulajdonképpen a megosztott felelősség elvének gyakorlati alkalmazása alapján tudják összeállítani. A veszélyhelyzetekre való felkészülés és az ipari balesetek országhatáron átterjedő káros hatásainak a minimalizálására felkészülési terveket kell létrehozni, amely az üzemeltető kötelesége.

A veszélyes anyagokkal kapcsolatos súlyos ipari balesetek megelőzése, a környezetre, illetve az egészségre ártalmas következmények csökkentése, az ember és a környezet magas fokú védelemének biztosítása érdekében az Európai Közösség országaiban 1997. február 3-án hatályba léptették a 96/82/EK számú Seveso II. Tanácsi Irányelvet.[7] Az Európai Unió tagállamainak saját törvényhozásukban 24 hónapon belül volt szükséges elvégezni a jogharmonizációt, majd 1999. február 3-tól alkalmazni az újonnan meghatározott irányelvet. A SEVESO I. irányelvet követően a SEVESO II. irányelv jelentette az Európai Unió tagállamaiban az ipari katasztrófák megelőzésével és az ipari katasztrófák elhárításával kapcsolatos szabályozás alapjait.

A SEVESO II. irányelv bevezető szakaszában általános alapelveket fogalmaztak meg hangsúlyozva, hogy szükséges:

- a SEVESO I. irányelv hatékonyabb megvalósításának részeként hatásosabb rendszerek bevezetésének a megteremtése;
- az új ipari létesítményekre vonatkozó szigorúbb felügyelet és ellenőrzés;
- az ipari létesítmények vezetési rendszereiben olyan alapelvek meghatározása, amelyek minimalizálják a súlyos balesetek bekövetkezésének a lehetőségeit;
- a Helsinki Egyezménnyel való harmonizációjának a megteremtése;
- a nyilvánosság tájékoztatása, a környezetvédelmi információkhoz való szélesebb körű hozzáférhetőség biztosítása;
- a súlyos ipari balesetek megelőzése érdekében az eddigi tapasztalatok összegyűjtése és ezen információk hatékony feldolgozása, elemzése, valamint az egész Közösséget átfogó információs rendszer működtetése.

A SEVESO II. irányelvben számos hangsúlyos újítást fogalmaztak meg [8]:

- egyrészt hatályát kiszélesítették, másrészt egyszerűsítették, azaz nem kellett alkalmazni többet az ipari üzemek és létesítményeknek tételes felsorolását, a különböző nevesített veszélyes anyagoknak rövidebb listáját kellett meghatározni, ugyanakkor növelni kellett a veszélyes anyagok osztályainak számát és meg kellett fogamzani és határozni az egyes osztályok kritériumait;
- az ipari létesítményekben a súlyos balesetek megelőzése érdekében biztonsági vezetési rendszert kellett kialakítani, amelynek szervesen kellett kapcsolódnia az általános vezetési rendszerhez és magába kellett, hogy foglalja a szervezési módszereket is;

- fontos eleme volt az irányelvnek, hogy a belső és külső veszélyhelyzeti tervek használhatóságát és alkalmazhatóságát a továbbiakban a gyakorlatban is ki kellett próbálni, monitoring rendszert kellett létrehozni a megelőzési tervek folyamatos értékelésére;
- a területhasználati tervekben az új létesítmények helyének kiválasztásakor, illetve a meglévő módosításakor vagy fejlesztésekor a hosszútávú igényeket is szem előtt tartva biztonságos távolságot kellett meghatározni a létesítmény és a lakott területek, vagy egyéb szempontból fontos építmények, objektum között;
- az irányelv ellenőrzése, valamint betartására felügyeleti rendszert kellett létrehozni.

Alapvető célkitűzésként fogalmazódott meg a SEVESO II. irányelv megalkotásakor, a különböző veszélyes anyagok alkalmazásával, előállításával és tárolásával kapcsolatos súlyos balesetek megakadályozása, illetve ezen baleseteknek a környező lakosságra, valamint a természetre gyakorolt káros hatásainak a csökkentése. Az újragondolt irányelv hatálya minden olyan létesítményre érvényes volt, ahol különböző veszélyes anyagok előfordulhatnak, illetve valamilyen kémiai folyamat ellenőrizhetetlenné válása következtében veszélyes anyagok keletkezhetnek. A SEVESO II. direktíva jelentős mértékben szigorodott és kibővült elődjéhez képest, azonban az ipari eredetű balesetek továbbra sem szűntek meg, az emberi tényező még mindig hangsúlyos szerepet játszott ezen baleseteknél, így nem volt elegendő csak kiegészítésekkel kipótolni ezen irányelveket.

Seveso III. Irányelv

A SEVESO irányelvek alklamazásának nemzetközi tapasztalatait vizsgálva elmondható, hogy a szigorításoknak köszönhetően az irányelv megfelelően működik, annak ellenére, hogy a veszélyes üzeme száma az EU-ban jelentősen megnőtt, a súlyos balesetek száma állandó maradt, nem emelkedett.[9] Évente átlagosan 27 súlyos baleset történik. Az elmúlt tíz évben jelentősen csökkent a bejelentett halálos, illetve sérülésekkel járó balesetek száma.

A SEVESO direktívát annak érdekében, hogy a súlyos balesetek száma ne csak stagnáljon, hanem csökkenjen ki kellett egészíteni. [10] Az új CLP rendszer bevezetésekor, amely az anyagok és keverékek osztályozásával, címkézésével és csomagolásával kapcsolatos határozat, már nem volt elegendő az akkor hatályos irányelv kiegészítése, új irányelvet kellett alkotni. Létrejött a SEVESO III. irányelv, amelynek az egyik legfőbb eleme a veszélyes anyagok listájának, valamint a veszélyességi kategóriáknak a szinkronizálása a CLP rendszerrel, mert ez változásokat okozhat az ipari üzemek besorolásban. Az új irányelvben bővült a nevesített anyagok listája, a korábbi 11 veszélyes anyag kategória pedig 21 kategóriára bővült, melyeken belül megkülönböztetésre került az egészségi, a fizikai, a környezeti és az egyéb veszélyek külön betűjellel. [11] A SEVESO II. irányelv módosítását követően ismét bekövetkezett néhány olyan súlyos ipari baleset, mint például a 2005. december 11-i buncefieldi üzemanyag tároló robbanása vagy éppen a 2010. október 04-i ajkai vörösiszap-katasztrófa. Ezek a módosítást követően bekövetkezett katasztrófák rávilágítanak a SEVESO II. irányelv felülvizsgálatának szükségességére. Ennek során megállapításra került, hogy bár az irányelv Unió szerte a védelmi szint növekedését eredményezte a védelem további megerősítése érdekében, különös tekintettel a súlyos balesetek megelőzése vonatkozásában további módosításokra van szükség.

Az újonnan létrehozott direktíva egyik jelentős változását a nyilvánosság tájékoztatására vonatkozó határozatának az ENSZ EGB Aarhusi egyezményében foglaltakhoz igazítása jelenti. [9] Ennek megfelelően szükséges a nyilvánosság kellő mértékű információval való ellátása, a döntéshozatalban való bekapcsolódása, nyilvános konzultációk és fórumok biztosítása, valamint az igazságszolgáltatáshoz való jog feltétel nélküli biztosítása. Az direktíva hangsúlyozza azonban, hogy a felesleges adminisztratív terhek kiszűrése érdekében a benne megfogalmazott tájékoztatási kötelezettséget bizonyos esetekben egyéb uniós

szabályozóban foglalt kötelezettséggel integrálva lehetséges végrehajtani. A direktíva hatálya kibővül és újonnan tartalmazza a szárazföldi földalatti, természetes rétegekben, víztartó rétegekben, sóüregekben és használaton kívüli bányákban végzett gáztárolás. Az irányelv hatálya alá nem tartozó „kivételek" listája kibővül a földalatti hulladéktárolókkal, továbbá a gáz földalatti nyílt tengeri helyszíneken történő tárolásával, azonban a veszélyes anyagok szállításához kapcsoló tárolás meghatározása sokkal szabályozottabbá és szigorúbbá válik és csak egyes a szállításhoz közvetlenül kapcsolódó tárolás jelent kivételt az direktíva hatálya alól. Mindezeken kívül pontosítások és finomhangolások történtek a fogalom meghatározások területén is, megjelentek a különböző eljárási folyamatoknak megfelelő új elemek (például: új üzem, meglévő üzem, egyéb üzem). Míg a SEVESO II. Irányelv egyes részeit csak a felső küszöbértékű üzemekre volt szükséges alkalmazni, az új direktíva hatálya most már kiterjed a biztonság megerősítése érdekében az alsó küszöbértékű ipari üzemekre is, azzal a kiegészítéssel, hogy míg minden üzemeltetőnek el kell készítenie egy úgynevezett MAPP-ot (major accident prevention policy - súlyos belesetek megelőzésére vonatkozó terv), addig biztonsági jelentést és belső védelmi tervet csak a felső küszöbértékű üzemeknek az üzemeltetőinek szükséges csak kidolgozniuk. [12] A Biztonsági Jelentés tartalmi követelményei pedig kiegészülnek azzal, hogy figyelembe kell venni azokat a nem a direktíva hatálya alá eső ipari üzemeket, illetve területeket is, melyek fokozhatják egy súlyos baleset káros hatásainak a következményeit, illetve megnövelhetik a dominóhatás kockázatát.

A SEVESO II. direktíva Biztonsági Jelentéssel kapcsolatos meghatározásai közül kikerült az a tétel, hogy amennyiben az üzemeltető igazolja, hogy valamely veszélyes anyag az üzemben olyan állapotban van jelen, hogy az kizárja a súlyos baleset bekövetkezését, akkor az adott hatóság engedélyével az erre a bizonyos anyagra vagy vegyületre vonatkozó információkat nem szükséges belefoglalni a Biztonsági Jelentésbe. A SEVESO III. irányelvben sokkal részletesebben meghatározásra kerültek a hatóság ellenőrzésekkel, üzemek felügyeletével kapcsolatos feladatai kitérve az ellenőrzések tervszerűségére, az üzemek veszélyeinek az értékelésére és az ellenőrzés eredményének függvényében elvégzendő tevékenységekre, kiemelve továbbá a településrendezési tervezés alkalmával a megfelelő biztonsági távolságok betartását. [13] A SEVESO III. irányelv 2012. augusztus 13-án lépett hatályba, az egyes tagállamoknak az új szabályozást 2015. május 31-ig kellett bevezetniük és összehangolni saját szabályozásukkal. [14] [15]

2002-BEN A BRÜSSZELI KIKÖTŐBEN BEKÖVETKEZETT KŐOLAJSZENNYEZÉS VIZSGÁLATA

Olajszivárgás történt Brüsszel egyik kikötőjében, Belgiumban 2002. augusztus 22-én. [16] Működési engedélye szerint az érintett üzem egy kőolaj tárolására és kereskedelmére szakosodott cég tulajdonában állt. Alaphelyzetben a tanker hajó beérkezik az üzem kikötőjébe, a szállított kőolajat átfejtik tartálykocsiba és elszállítják az üzem területéről vagy tárolótartályokba fejtik át őket és raktározzak az üzem területén. A helyi lakosság riasztotta a hatóságokat és a médiát, hogy valami nincs rendben az üzemben, miután észlelték a csatorna elszennyeződését. Az üzem fenntartójától semmiféle jelzés nem érkezett a hatóságok felé. A környezetvédelmi hatóság szakemberei a helyszínre érkezést követően riasztották a tűzoltóságot mi szerint kőolaj szivárog az egyik tanker hajóból. Eközben két közelben lévő hajó kapitánya is észlelte a szivárgást és megpróbáltak közel húzódni a sérült hajóhoz, hogy gátat szabjanak az olajfolt szétáramlásának. A tűzoltó egységek két úszó gátat alkalmaztak, hogy megakadályozzák a szennyezés további terjedését. Mivel a tűzoltó egységeknek nem rendelkeztek szivattyúval a kőolaj kiemeléséhez a vízből, a helyszínre riasztották a Polgári Védelmet. A környezetvédelmi hatóság közben leállította a forgalmat a csatornán és bevetett még két merülőgátat a szennyeződés szétterjedésének megakadályozására. Az erős szél

jelentősen megnehezítette a kárelhárítást. A Polgári Védelem a helyszínen megkísérelte kiszivattyúzni az olajat a vízből, de azonban csak egy részét sikerült eltávolítani a csatornából. A baleset következtében 2 m^3 olaj szennyezte el a vizet.

Egy újabb baleset következett be 2002. december 13-án, néhány hónappal az első esetet követően az üzem egy másik részén 1,5 km-re az előző helyszíntől. Ez a baleset akkor történt, amikor a beérkező tankerhajóból fejtették át a tároló tartályokba a kőolajat. Amikor az első tartály majdnem megtelik, egy jelzőrendszer figyelmezteti a kezelőt, hogy fel kell készülni a második tartályba történő átfejtésre. Az első tartály a rendnek megfelelően meg is telt, azonban a kezelő figyelmen kívül hagyta a jelzőrendszer riasztását, ezért az első tartály túlcsordult. Az üzemben úgy gondolták, hogy a szennyezés nem fog problémát okozni és nem fog kikerülni az üzem területéről, de értesítették a hatóságokat az esetről. Ismét a helyszínre érkeztek a tűzoltó egységek és a környezetvédelmi hatóság emberei, akik a fennforgó eseten kívül egyéb problémákat is feltártak, például, hogy a tartályok nagyon közel voltak egymáshoz, szinte összeértek. További probléma volt, hogy a tartályok többsége túl voltak csordulva, a tartályok tetején szivárgott ki a kőolaj. A hatóságok felmérése alapján 3 m^3 olaj került ki a környezetbe az üzem falain belül és 2 m^3 olaj szivárgott ki az üzem falain kívülre.

1. ábra: A tárolótartályok és a kiömlő kőolaj [17]

A lefolytatott vizsgálat megállapította, hogy nem tartották be a kötelező előírásokat, vagyis emberi mulasztás, figyelmetlenség és hanyagság okozta a baleseteket. Számos hiányosságot tárt fel a vizsgálat az eseteket követően. A bíróság pénzbüntetést szabott ki az üzemre és kötelezte bizonyos biztonsági eszközök pótlásásra, illetve beszerzésére. Az eszközök között voltak például merülőgátak, amelyek az üzembe érkező legnagyobb hajót és körül tudják zárni szivárgás esetén, többnyelvű biztonsági tájékoztatók, valamint radar, amely kimutatja a tartályok töltöttségi szintjét átfejtés közben, hogy megelőzhető legyen azok túlcsordulása. Az érintett cég eleget tett a bíróság előírásainak és pótolta a hiányosságokat. Az üzemben azóta külön megelőzési tanácsadó foglalkozik a hasonló balesetek megelőzésével és az üzem tartja magát a hatályos SEVESO irányelv előírásaihoz.

2. ábra: Az ipari balesetek Európai skáláján ábrázolva az eset mértéke [17]

A SILLAMAE-I PALAOLAJ SZENNYEZÉS HATÁSAINAK ELEMZÉSE

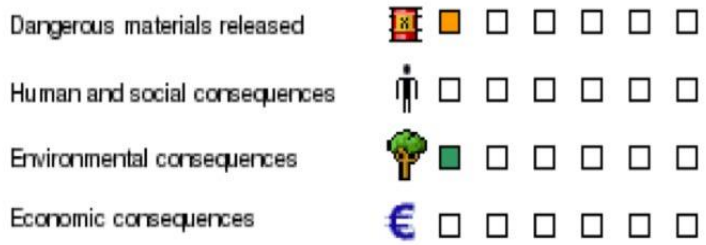
Az észtországi Sillamae város kikötőjében egy palaolaj tárolásra és átfejtésére szakosodott cég telephelye található. A palaolaj, olyan nem-konvencionális nyersolaj fajta, amelyet magas szervesanyag tartalmú üledékes kőzetekből állítanak elő. A kitermelt olajpalából különféle módszerekkel, például hidrogénezéssel lehet az olajat kinyerni. Ezen folyamat során az olajpalában található szerves anyagok szintetikus kőolajjá alakulnak át. A művelet eredményeként kinyert olajat fel lehet használni például fűtőanyagként. Az üzembe vasúton és tankerhajón egyaránt érkezik palaolaj szállítmány. Az üzem területén 12 tározó található, amelyek 172 500 m^3 olaj tárolására alkalmasak. A tározók 3 vasbetontöltésen helyezkednek el, amelynek a célja, hogy megvédje a talajt és a felszíni vizeket az esetleges elszennyeződésektől. Az esővizet esővízelvezető-csatornákkal gyűjtik össze tárolókba és csak olajfogón keresztül juthatnak bele a tengerbe.

2008. szeptember 12-én a Balti-tenger azon szakaszának partvonala mentén, amely az Észt Környezetvédelmi Felügyelőség területén található, sötét szennyező anyag jelent megkb. 150 méterre benyúlva a tengerbe. [18] A felügyelőség szakemberei nem tudták pontosan megállapítani honnét származik a szennyező anyag, ezért ellenőrizték az összes közelben lévő üzemet és telephelyet. A hatóságok arra a következtetésre jutottak a fent említett telephely ellenőrzése során, hogy onnét származik a szennyező anyag. Felszólították a céget, hogy szüntesse meg a szennyezést, és tisztítsa meg a partszakaszt, amely ennek eleget is tett. A kikerült palaolajat begyűjtötték és elszállították egy speciális veszélyeshulladék-kezelő létesítménybe, ahol miután szétválasztották a tengervíztől kiderült, hogy 2400 kg olaj került ki az üzem területéről a környezetbe.

3. ábra: Az egyik telítődött vízelvezető-csatorna [19]

A vizsgálat kiderítette, hogy a csapadékvíz-elvezető csatornák és a csapadékvíz-tárolók megteltek, túlcsordultak és a szennyező anyag beszivárgott a tengerbe. Mint kiderült, nagyobb

csatornahálózatra lett volna szükség, nem volt elegendő befogadó képessége az érintett hálózatnak. Ebben az esetben is emberi hanyagságról, figyelmetlenségről beszélhetünk, ennek következtében alakult ki a szennyezés. A bíróság kötelezte a céget, hogy építsen nagyobb befogadású csatornarendszert, és hogy szerelje fel jelző berendezéssel, amely a hasonló esetekben riasztást ad. Továbbá a hatóság is el lett marasztalva, amiért elfogadták és biztonságosnak ítélték az alacsony kapacitású csatornarendszert.



4. ábra: Az ipari balesetek Európai skáláján ábrázolva az eset mértéke [19]

ÖSSZEFOGLALÁS

A XX. században növekvő tendenciát mutat a bekövetkezett ipari eredetű balesetek száma. Világunk folyamatosan fejlődik, egyrészt a népesség számának növekedésével párhuzamosan fokozódik az ipari teljesítmény, másrészt a fejlődésnek köszönhetően újabb és újabb ipari eljárások, technikák születnek. Mindezek mellett a lefektetett szabályozók, rendelkezések és előírások egyre szigorodó feltételeket szabnak a veszélyes anyagokkal kapcsolatos tevékenységekre, úgymint a szállításra, raktározásra, felhasználásra és a gyártásra egyaránt. Fontos, hogy az ember egészségét, javait és a környezetet veszélyeztető súlyos balesetek elkerülése érdekében az ipar minden érintett szereplője betartsa a megelőzéssel és a védekezéssel kapcsolatos dokumentációs és gyakorlati teendőket egyaránt.

A kiválasztott káresetek tanulmányozásával feltártam az ipari balesetek egyik legkritikusabb tényezőjét, magát az embert. Az ipari eredetű balesetek legtöbbször a műszaki hibák mellett emberi mulasztás, figyelmetlenség, hanyagság miatt következnek be. A két általam kiválasztott eset, jól mutatja az emberi tényező szerepét. Az első esetnél a teljes hanyagság volt megfigyelhető, semmiféle biztonsági előírást nem tartottak be, illetve nem rendelkeztek a megfelelő biztonsági berendezésekkel, eszközökkel. A második esetben, minden előírást és biztonsági szabályt betartottak, azonban elég volt egy emberi hibából adódó konstrukciós hiba a szennyezés bekövetkezéséhez.

Arra a következtetésre jutottam az irodalmak, tanulmányok és az egyes esetek tanulmányozása során, hogy mind a megnövekedett ipari teljesítmény, mind az új ipari eljárások potenciális veszélyeket jelentenek és magukban hordozzák az ipari balesetek bekövetkezésének lehetőségét. A veszélyes kategóriába sorolható – nukleáris, kémiai, biológiai eredetű – anyagok felhasználása, alkalmazása, tárolása előrevetítheti egy esetleges baleset és abból adódó katasztrófahelyzet kialakulásának esélyeit, ugyanis mindegyik esetben jelen van az emberi tényező, mint potenciális veszélyforrás.

Felhasznált irodalom

[1] Rachel P.E. Gordon: The contribution of human factors to accidents in the offshore oil industry, Aberdeen University, Psychology Department. Kings College. Aberdeen AB24 2UB, Norther Irland, 1998. http://www.nrc.gov/docs/ML0906/ML090650437.pdf (2015.10.02)

[2] Najmedin Meshkati: Human factors in large-scale technological systems accidents Viterbi School of Engineering, University of Southern California, Los Angeles, USA, 2006. http://archiwum.ciop.pl/16249 (2015.10.02.)

[3] Tolna Megyei Katasztrófavédelmi Igazgatóság: *SEVESO*.
http://tolna.katasztrofavedelem.hu/seveso (2015.10.03.)

[4] Bognár B., Damjanovich I.: *A súlyos ipari balesetek megelőzésével és elhárításával kapcsolatos nemzetközi és Európai Uniós szabályzások összefoglalása.* http://inventor.hu/ceco/kock/konyv/ofoglalo.pdf (2015.10.05.)

[5] Tolna Megyei Katasztrófavédelmi Igazgatóság: *BHOPAL.*
http://tolna.katasztrofavedelem.hu/bhopal (2015.10.03.)

[6] Damjanovich I., Karádi T., Varga I.: *Útmutató a veszélyes üzemek környezetében élő lakosság tájékoztatása megszervezéséhez.* Budapest: Közép-és Kelet-Európai Intézet, 2004.

[7] Bonnyai Tünde; Bognár Balázs (szerk.); Görög Katalin; Kátai-Urbán Lajos (szerk.); Vass Gyula. Létfontosságú rendszerek és létesítmények védelme: Kézikönyv a katasztrófavédelmi feladatok ellátására. Budapest: Nemzeti Közszolgálati Egyetem, 2015. *149 p.*ISBN: 978-615-5057-49-6 (2015.10.06.)

[8] *Directive 2012/18/EU of the europen parliament and of the council of 4 July 2012.* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:197:0001:0037:en:PDF (2015.10.11.)

[9] Dr. Vass Gyula: SEVESO III. Irányelv bevezetése, BM OKF, Balatonalmádi, 2015.
http://biztonsagtechnika.mke.org.hu/eloadasok/Vass.pdf (2015.10.10)

[10] Szilágyi E.: *GHS és a Seveso II. Irányelv I. sz. melléklete - EU Hatástanulmány előzetes eredményeinek ismertetése*. Seveso Szakértői Csoport 2009. II. félévi Értekezlete, Göd, 2009. november 20.

[11] Címer Zs., Halász L.: A kémiai biztonsági jogszabályok változása, a CLP és a Seveso II. irányelv kapcsolata. *Hadmérnök*, (1) 2010. 87–98. http://hadmernok.hu/2010_1_cimer_halasz.pdf (2015.10.14.)

[12] Szendi R.: A Seveso III. irányelv Magyarországi adaptálásnak várható hatásai a veszélyes üzemekre és a hatósági feladatira. *Hadtudományi Szemle,* 7 1 (2014), 199–209.
http://epa.oszk.hu/02400/02463/00023/pdf/EPA02463_hadtudomanyi_szemle_2014_02_199-209.pdf (2015.10.13.)

[13] *Health and Safety Executive: Changes from seveso II to seveso III.* http://www.hse.gov.uk/seveso/changes.htm (2015.10.15.)

[14] Dobor J., Szendi R.: Veszélyes üzemek azonosítása és a kapcsolódó hatósági tevékenységek, Hadtudományi szemle, az NKE HHK tudományos folyóirata VIII. Évfolyam, 3. Szám, Magyarország, Budapest 2013. http://hadmernok.hu/133_13_doborj.pdf (2015.10.16.)

[15] Kátai-Urbán Lajos : Veszélyes üzemekkel kapcsolatos iparbiztonsági jog-, intézmény és eszközrendszer fejlesztése Magyarországon, Budapest: Nemzeti Közszolgálati Egyetem, 89 p

[16] *French Ministry of the Enviroment: Leaks of fuel oil and pollution of waterway / Pollution of the site.* http://www.aria.developpement-durable.gouv.fr/wp-content/files_mf/FD_26981_26982_bruxelles_2002_ang.pdf (2015.10.01.)

[17] *ARIA - Lessons learnt from industrial accidents: Leaks of fuel oil and pollution of waterway / Pollution of the site.* http://www.aria.developpement-durable.gouv.fr/accident/26981_en/?lang=en (2015.10.02)

[18] *French Ministry of the Enviroment: Pollution of the port of Sillamäe by hydrocarbons produced from oil shale.* http://www.aria.developpement-durable.gouv.fr/wpcontent/files_mf/FD_35835_sillamae_2008_ang.pdf (2015.10.02.)

[19] *ARIA - Lessons learnt from industrial accidents: Pollution of the port of Sillamäe by hydrocarbons produced from oil shale.* http://www.aria.developpement-durable.gouv.fr/accident/35835_en/?lang=en (2015.10.02.)

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Grósz Zoltán – Kuti Rajmund – Takács Krisztina
grosz.zoltan@uni-nke.hu kuti.rajmund@sze.hu takacskr@nebih.gov.hu

BIOLÓGIAI FERTŐTLENÍTŐ ANYAGOKKAL SZEMBEN TÁMASZTOTT KÖVETELMÉNYEK

Absztrakt

A híradások naponta beszámolnak különféle biológiai veszélyhelyzetekről, járványokról. A megfelelő megelőző intézkedések nélkül, a humán és technikai feltételek hiányában a vírusok gyorsan terjednek, pandémiás veszélyhelyzetek alakulnak ki. A járványveszély kezelése, a fertőzések továbbterjedésének megakadályozása, a megfelelő fertőtlenítőszerekkel történő hatékony fertőtlenítési eljárások alkalmazása nélkül nem valósulhat meg. Kutatásaink során fizikai, kémiai tulajdonságok, továbbá hatásspektrum szerint vizsgáltuk a Magyarországon elérhető fertőtlenítő anyagokat. Eredményeinkkel hozzá szeretnénk járulni a hatékony gyakorlati alkalmazáshoz, valamint segítséget kívánunk nyújtani a beavatkozásokat legtöbb esetben végrehajtó hivatásos szervezetek egységeinek.

The news reports about several biological threat situation and, epidemics every day. Without proper preventive measures, viruses spread rapidly because of the lack of human and technical conditions which develops pandemic emergency. The pandemic risk management and preventing infections from spreading could not be achieved without the implementation of effective disinfection procedures done by the appropriate disinfectants. During our study, available disinfecting substances were examined in Hungary, according to their physical, chemical properties and spectrum of activity. The detected results would contribute the effective practical application and would also help the professional organizations participants in interventions.

Kulcsszavak: *járvány, biológiai veszély, kárfelszámolás, fertőtlenítési eljárás, fertőtlenítő anyag ~ epidemic, biological hazards, remediation, disinfection, disinfection materials.*

BEVEZETÉS

A különféle járványok, fertőzések megelőzésének, kezelésének problémái mindig komoly kihívás elé állították az emberiséget. Kezdetben a betegek elkülönítésével, a városokba történő bezárkózással próbálták elkerülni a fertőzések továbbterjedését. Felismerték, hogy legtöbb esetben a halottak terjesztik a kórt, a tűz megakadályozza a járványok terjedését, ezért az érintett területeken a halottakkal együtt mindent elégettek. Földünkön jelenleg is pusztítanak járványok, a tudomány azonban lehetővé tette, hogy az érintett területek felégetése helyett különféle eljárásokkal, vegyi anyagok alkalmazásával gátolják meg a biológiai kórokozók terjedését.

A globális felmelegedés hatásairól sem lehet megfeledkezni, ugyanis azok a veszélyhelyzetek kialakulásában és a kárfelszámolás hatékonyságában is szerepet játszanak [1]. Napjainkban egyre többször alakulnak ki biológiai veszélyhelyzetek, melyek során különféle kórokozók veszélyeztethetik a kárfelszámolást végzőket, a humán környezetet, ezért a fertőzésveszély kezelése fontos feladat. A biológiai szennyező anyagok közömbösítése, vagy eltávolítása érdekében biológiai mentesítést, más néven fertőtlenítést(dezinfekció) kell végezni. A fertőtlenítés rendkívül költséges, időigényes folyamat, hatékony végrehajtásához hatékony fertőtlenítő anyagok és eljárások alkalmazása szükséges. Cikkünkben a Magyarországon leggyakrabban alkalmazott fertőtlenítő anyagokat mutatjuk be, elősegítve ezek gyakorlati alkalmazását.

FERTŐTLENÍTŐ ANYAGOK

A fertőtlenítő anyagok alkalmazásához elengedhetetlen a feladatokat végző állomány elméleti és gyakorlati oktatása, felkészítése a biológiai veszélyekre [2]. Meg kell ismerniük a fertőtlenítő anyagok fizikai kémiai tulajdonságait, az alkalmazhatóságuk követelményeit, a személyi védőfelszerelések használatának szabályait. Korábbi írásunkban már foglalkoztunk a fertőtlenítési eljárások fajtáival, bemutattuk a feladatok végrehajtásához szükséges személyi és tárgyi feltételeket is.

A fertőző anyagok jelenlétében történő különféle beavatkozások során törekedni kell a folyamatos fertőtlenítés végrehajtására. A hatékony fertőtlenítés feltételeinek és logisztikai hátterének megteremtése alapos és körültekintő tervezést igényel [3]. A folyamat fontos része a megfelelő fertőtlenítési eljárás és fertőtlenítő anyag megválasztása. Ismert eljárások a kémiai eljárás, a sugárzó energiával történő fertőtlenítés, valamint a hőenergia alkalmazása.

Terepen, különféle kárhelyszíneken történő fertőtlenítési feladatok során legtöbb esetben a kémiai eljárások kerülnek alkalmazásra, ezért az ezekhez szükséges fertőtlenítő anyagok a következőkben részletesen is bemutatásra kerülnek.

Az alkalmazni kívánt fertőtlenítő anyag kiválasztásánál a kívánt hatás elérése érdekében, fontos a következő követelmények figyelembe vétele.

A kémiai fertőtlenítő anyagokkal szemben támasztott követelmények:

- Széles határspektrum,
- Gyors hatásidő,
- Kiváló fertőtlenítő hatás,
- Jó vízoldékonyság,
- Megbízhatóság,
- Kémiai stabilitás,
- Ne legyen korrozív,

- Ne legyen tűzveszélyes,
- Legyen környezetbarát,
- Alkalmazása gazdaságos legyen [4].

Kémiai eljárások hatását befolyásoló tényezők:

- Koncentráció,
- Kémhatás,
- Szelektivitás,
- Kapilláraktív hatás,
- Mechanikus hatás.

A kémiai fertőtlenítő anyagok fertőtlenítő hatás szempontjából történő csoportosítása:

- Baktériumok szaporodását gátló hatás (bakteriosztatikus),
- Baktériumölő (baktericid),
- Csíraszám csökkentő hatás (szalációs effektus),
- Spóraölő (sporicid),
- Vírus inaktiváló (virucid),
- Gombaelemeket pusztító (fungicid),
- Parazitákat pusztító (paraziticid) [5].

A fenti követelményeknek megfelelő fertőtlenítő anyagok előállítása figyelembe véve a magas kritériumrendszert komoly feladat. Ebből adódóan a komplex hatásmechanizmusú termékek beszerzése költséges, ezért Magyarországon több olyan fertőtlenítőszer is a rendszerben van, amelyek nem minden feltételnek felelnek meg [6].

Következőkben a leggyakrabban alkalmazott kémiai fertőtlenítő anyagokat mutatjuk be. Oxidálva fertőtlenítő anyagok (vízzel való reakciójával erős fertőtlenítő hatású naszcensz oxigén keletkezik)

Klór és vegyületei

- Cl2 + H2O $\Rightarrow$ HOCl + HCl; HOCl $\Rightarrow$ HCl + ’O’ (redukál, a fehérjét oxidálja)
- Nátrium-hipoklorit: NaOCl $\Rightarrow$ NaCl + ’O’ (só, lúgos kémhatású, vizes oldata sárga)
- Kalcium-hipoklorit (klórmész): Ca(OCl)2 (vízben oldódó por, átlátszó folyadék, savak hatására klórgáz fejlődik)
- Klóraminok: (hidrolízise során NaOCl keletkezik. Kevésbé izgatják a bőrt. Ilyen anyag a Flórasept.

Jód és vegyületei

- A jód kristályos, halogén elem. A bőrt és nyálkahártyát is izgatja, szublimál, szilárdból légnemű lesz. Vízben jól oldódik, oxidáló hatású. Fertőtlenítésre a jódtinktúrát használják.
- Jódtinktúra: 82 % alkoholos oldatban 5 % jód és 4 % kálium-jodid, mely a szövetizgató hipo-jodidok keletkezését gátolja.
- Lúgos oldat: a jód 5 % Kálium-jodidos vizes oldata.
- Jodoforok: Az elemi jód felületaktív anyagokkal alkotott komplexei. A komplexekből felszabaduló elemi jódtól függ a fertőtlenítő hatás.

Hidrogén-peroxid (H_2O_2)

- Színtelen, nagy tömegben halványkék. A víznél sűrűbb, folyékony. Kémhatása gyengén savas. Erős oxidálószer, ezért hatékonyan használható fertőtlenítésre.

Kálium-permanganát ($KMnO_4$) (hipermangán):

- Ibolyaszínű, kristályos anyag, vízben jól oldódik, oldata lila színű, naszcensz oxigén felszabadulása közben bomlik. Fertőtlenítő hatása kiváló, mert a test szöveteivel érintkezve naszcensz oxigén hasad le belőle, amely fertőtlenít, szagtalanít.

Redukálva fertőtlenítő anyagok

Aldehidek

- Aldehid származékok: (széles spektrumú fehérje kicsapó hatású fertőtlenítők, melyek a baktériumok citoplazmatikus membránját és az enzimrendszerét károsítják.
- Formalin (HCHO) a formaldehid 40 %-os vizes oldata. Helyiségek és eszközök fertőtlenítésére használják.
- Lysoform: a formaldehid alkoholos oldata
- Káliszappanos oldat 2-3 %, gombaellenes, eszközfertőtlenítő.
- Hexametilén-tetramin: formalin és az ammónia addíciós vegyülete. Tartalmazzák: virusept, klórhexidin.

Fenol származékok

- Fertőtlenítő hatása abban rejlik, hogy a kórokozók sejtmembránjának áteresztőképességét fokozza.
- Krezol: színtelen vagy sárga folyadék, vízben kevésbé oldódik
- Hexaklorofén: fehér por, erős bakterocid, fungicid hatású, dezodoráns, fertőtlenítő szappanokban is alkalmazzák.

Fehérje kicsapódással fertőtlenítő anyagok

- Alkoholok: Leghatékonyabban az 1-2 értékűek alkalmazhatók. Hatásuk: a fehérje koaguláción (fehérje kicsapódás) alapul, csak a vegetatív állapotban lévőket öli meg, a latenst nem. Vízelvonó hatású.
- Etil-alkohol (CH3-CH2-OH) (spiritus concentriecutinius)
- 96 %-os alkohol: spiritus cencentratissimus
- 90 %-os alkohol: spiritus concentratus
- 70 %-os alkohol: spiritus dilitus
- Propanol: 70 %-os oldatát használjuk fertőtlenítésre
- Izopropanol: izopropil-alkohol 60%-os töménységben
- Glikol: 2 értékű alkohol. A bőrre közvetlenül nem használjuk, levegő fertőtlenítésére a gőzei megfelelőek.

Fémek, fémsók:

- Elsősorban a nehézfémsók hajlamosak a fehérjekicsapásra.
- Ezüst és vegyületei: ezüst-nitrát (lápisz), állatorvosok mai napig használják
- Higany-klorid (HgCl2): Fehér, kristályos anyag, vízben jól oldódik, fehérjéket kicsapja, 0,1-0,2 m/m %-os oldatát használjuk fertőtlenítésre

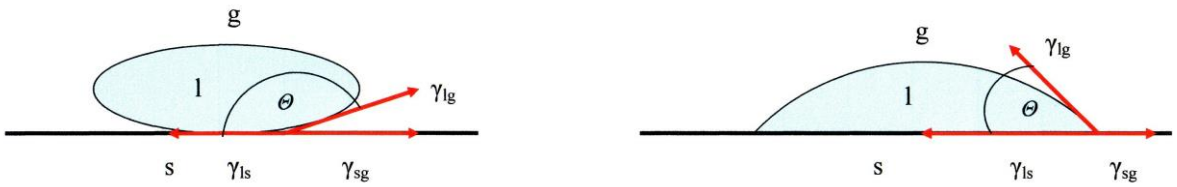
Savak:

- Bórsav
- Szalicilsav
- Benzoesav, sói: nátrium-benzoátok
- Para-oxi-benzol
- Metil észterek: nipagin M
- Etil észterek: nipagin A
- Solotio-conservans nipasol M (nipagin M alkoholos oldata) [7].

FELÜLETAKTÍV ANYAGOK ALKALMAZÁSA FERTŐTLENÍTŐ OLDATOKBAN

A különféle fertőtlenítő anyagok legtöbb esetben vizes oldatban kerülnek felhasználásra. A víz nagy felületi feszültsége alapvetően nem előnyös a fertőtlenítésre történő alkalmazás szempontjából.

Régi és közismert jelenség, hogy a folyadékok gáztérben, vagy velük nem elegyedő folyadékokban gömbalakot – vagyis a legkisebb felületű alakot – igyekeznek felvenni. A felületi feszültség tulajdonképpen az az ellenállás, amelyet a folyadék felszín tanúsít azzal az erővel szemben, amely a felületét meg akarja növelni. A felületi feszültség tehát a felület egységnyi hosszúságában működő, felületet csökkentő erő. Mértékegysége: N/m. A vízcseppet körülvevő anyagok molekulái a vízcseppre különféle erőket fejtenek ki. Ha az erők vízmolekulára kifejtett hatása elhanyagolható (levegő: g) a kohéziós erőhöz képest, akkor a víz felületén lévő részecskék a kohéziós erő hatására a folyadék belseje felé igyekeznek elmozdulni, vagyis a felület tényleg csökken. Ezeknek az erőknek a víz (l) molekuláira kifejtett hatása nem hanyagolható el, ha a vízcsepp egy szilárd (s) felületre került. A vízcsepp jobban, vagy kevésbé terül szét azon – nedvesíti, vagy kevésbé nedvesíti a felületet – a vonzó és taszító erők függvényében. A nedvesítés mértéke a nedvesítési peremszöggel (Θ) jellemezhető. Ha a peremszög nagyobb 90^o –nál, akkor részleges nem nedvesítésről, ha kisebb 90^o –nál, részleges nedvesítésről beszélünk. A vízcsepp nedvesítés hatására történő változását a következő ábra szemlélteti.



1. sz. ábra: Víz felületi feszültségének változása nedvesítés hatására (Forrás: [8])

A közös határfelületen fellépő erőket a határfelületi feszültséggel jellemezzük γ_{ls}, γ_{sg} γ_{lg}. A nedvesítés mértéke a határfelületi feszültségek módosításával is befolyásolható. A felületi feszültséget különféle adalékanyagok, nedvesítő szerek (például tenzidek) hozzáadásával lehet csökkenteni. Az adalékanyag csökkenti a víz felületi feszültségét és olyan hatást fejt ki, hogy a fertőtleníteni kívánt anyag felülete és a vízmolekulák között nagyobb lesz a vonzerő, mint az egyes vízmolekulák között. Így a víz rátapad az anyagok felületére, könnyebben hatol be a porózus felületi részekbe, ezáltal felgyorsul a folyamat [8]. Fertőtlenítési munkálatok során is jelentkezik ez a probléma, ugyanis a különféle berendezésekből kijuttatott oldatok cseppjei a fertőtleníteni kívánt felületet nem nedvesítik kellően, így a kívánt hatás elérése érdekében több oldat kerül felhasználásra.

Felületaktív anyagok

Leggyakrabban alkalmazott felületaktív anyagok a tenzidek, melyek alkalmazásával a vizes oldatok felületi feszültséget csökkentik. Hatásuknál fogva lehetővé teszik az oldatok megtapadását erősen szennyezett felületeken is. Alkalmazásukkal könnyebbé válik a zsírok, egyéb szerves apoláris szennyeződések fellazítása, eltávolítása így a fertőtlenítő anyag hatásának kifejtését növelik, ezzel a fertőtlenítő folyamatot is felgyorsítják.

A felületaktív anyagok lehetnek ionosak és nem ionosak:

Ionos felületaktív anyagok:

Aanionaktív anyagok:

Önmagukban nincs fertőtlenítő hatásuk, de oldják a lipideket, ezzel elősegítve a dezificiensek mikrobaölő hatásának kifejtését. Ilyen anyagok a különféle szappanok, egyszerű mosogatószerek.

Kationaktív anyagok:

Az anion aktív tenzidekhez képes fordított molekula szerkezetűek, bennük a kation a felületaktív, lipideket emulgeáló rész, kémiai szerkezetüktől függően enyhe fertőtlenítő hatást is kifejtenek. Ilyen anyagok az invert szappanok. A kationaktív tenzideket nem szabad keverni anionaktív tenzidekkel, mert azok hatását közömbösítik.

Amfoter tenzidek:

A kationaktív tenzidekhez hasonlóan jó szennylazító és tisztító tulajdonságúak, egyben fertőtlenítő hatást is képesek kifejteni. Kombinált fertőtlenítő szerekben alkalmazzák.

Nem ionos felületaktív anyagok:

Önmagukban nincs fertőtlenítő hatásuk, de kiváló zsíroldó és szennyeltávolító hatásuknál fogva más dezificiensek mikrobaölő hatását elősegítik Ilyenek a mosóaktív szappanok, mosogatószerek.

MAGYARORSZÁGI GYAKORLAT

Magyarországon olyan fertőtlenítési feladatokat, melyek során nagy mennyiségű fertőtlenítő anyag kerül felhasználásra leggyakrabban a hivatásos kárfelszámoló szervezetek – Katasztrófavédelem, Magyar Honvédég – egységei végeznek, elsősorban árvízi védekezés záró fázisaként, vagy biológiai szennyezéssel járó balesetek utómunkálatai során. A fentiekben felsorolt követelményeknek megfelelő fertőtlenítő anyagok beszerzése komoly anyagi ráfordítást igényel, mely források sajnos nem mindig állnak rendelkezésre, ezért a magyar kárfelszámolási szervezetek legtöbb esetben kalcium-hipoklorit $Ca(OCl)_2$ oldatot, nátrium-hipoklorit NaOCl oldatot, és etil-alkoholt CH_3CH_2OH használnak fertőtlenítésre. Ezeknek az anyagoknak az előnye a széles körben történő alkalmazhatóság, ugyanakkor komoly terhelést jelentenek a környezeti elemekre, főleg a kalcium-hipoklorit.

A különféle állati járványokkal, állatbalesetekkel kapcsolatos fertőtlenítési feladatokat az állategészségügy felügyeli. A hatékony fertőtlenítőszerek használata elengedhetetlen az állategészségügyben is, hiszen hazánkban is felbukkannak különféle járványok, melyek sok esetben nem csak az állatokra veszélyesek, hanem zoonózis is kialakulhat. Ilyen esetekben a fertőző betegségek állatról emberre is képesek átterjedni. Az állategészségügyi hatóságok feladata többek között a különböző állatbetegségek, járványok megállapítása, kivizsgálása, továbbá ezek elleni védekezés elrendelése, melyben kiemelt szerephez jut a fertőtlenítés. A fertőző állatbetegségek megelőzéséhez és leküzdéséhez a 41/1997. (V.28.) FM rendelet egy fertőtlenítési útmutatót állított össze, amelyben szabályozzák, hogy a különböző betegségek esetén milyen fertőtlenítőszert, illetve milyen koncentrációban kell alkalmazni.

Az állategészségügyben leggyakrabban alkalmazott fertőtlenítőszerek:

Lúgok

- Mésztej,
- Nátriumhidroxid 2-4%-os oldata ,
- Káliumhidroxid 2-4%-os oldata,
- Nátriumkarbonát 3-6%-os oldata ,
- Nátriummetaszilikát 1%-os oldata.

Karbonsavak

- Citromsav 0,4%-os oldata,
- Tejsav 1-2%-os oldata,
- Hangyasav 1-2%-os oldata.

Klórtartalmú fertőtlenítő szerek

- Hipokloritok- Nátriumhipoklorit, (aktív klórtartalma 9–12%) 3–6%-os oldatban,
- Klóros mész (aktív klórtartalom 25–30%) 2,0%-os oldatban,

Aldehidek

- Formalin, (a formaldehid 36–40%-os oldata) 1–6%-os oldatban. 15 °C hőmérséklet alatt hatása mérsékelt, ezért abban a hőmérsékleti tartományban használata nem javasolt.

Egyéb fertőtlenítő anyagok

- Jodoforok, 1–5%-os oldatban pH: 2,5–4,0,
- Szulfaminsav 0,2 %-os oldata [9].

ÖSSZEGZÉS

A természeti és a humán környezet megóvására egyre nagyobb figyelmet érdemel a jövőben, ezért a kárfelszámolások során fokozottabban törekedni kell a fertőzésveszély kezelésére, továbbá a fertőtlenítés hatékonyságának növelésére. Cikkünkben a Magyarországon leggyakrabban alkalmazott fertőtlenítő anyagokat mutattuk be, ismertetve fizikai, kémiai tulajdonságaikat, alkalmazásuk előnyeit, korlátait. A Magyarországon használt anyagok legtöbbjének előnye a széles körben történő alkalmazhatóság, ugyanakkor komoly terhelést jelentenek a környezeti elemekre, főleg a kalcium-hipoklorit. A nemzetközi folyamatok is ösztönzően hatnak arra a törekvésre, hogy a környezetet károsító fertőtlenítő anyagokat ki kell váltani olyan fertőtlenítésre alkalmas anyagokkal, amelyek mind hatékonyságban, mind alkalmazhatóságban magasabb értékeket képviselnek. Kutatásainkkal fel kívántuk hívni a figyelmet a téma fontosságára, a cikkben bemutatott fertőtlenítő anyagok alkalmazása segítséget nyújthat a fertőtlenítési feladatokat végrehajtó beavatkozó egységek számára.

Felhasznált irodalom

[1] HALÁSZ L., FÖLDI L., PADÁNYI J.: Climate change and CBRN defense. *Hadmérnök*, VII 3 (2012), http://hadmernok.hu/2012_3_halasz_padanyi_foldi.pdf 42 – 49. (downloaded: 13 03 2015)

[2] Grósz Zoltán: Az ABV védelem alapjai, Tankönyv, Zrínyi Egyetemi Kiadó Budapest, 2003.

[3] Kuti Rajmund: Mentesítési feladatok új dimenziói, Bolyai Szemle, XVI. 1. szám 62-67. p. 2007. ISSN 1416-1443, URL cím: http://portal.zmne.hu/download/bjkmk/bsz/bszemle2007/1/05%20Kuti.pdf

[4] Grósz Zoltán: Vegyi- sugár és bakteriológiai szennyezések mentesítésének elméleti és gyakorlati kérdései a katonai alkalmazásban, Tanulmány, ZMNE VKBT Letéti Könyvtár, 1996

[5] Dr. Papp Katalin –Ujváriné Dr. Siket Adrienn: Az egészségügy és az ápolás általános alapelvei, Tankönyv, Debreceni Egyetem Egészségügyi Kar, 2014

[6] Grósz Zoltán: Biológiai Hadviselés, Bolyai Szemle, 1996/2. pp. 30-38.

[7] Halász László – Grósz Zoltán: ABV védelem, Egyetemi jegyzet, ZMNE Budapest, 2000.
[8] Kuti Rajmund: A víz tűzoltói felhasználhatóságának lehetőségei, korlátai, Védelem Online: Tűz-és Katasztrófavédelmi Szakkönyvtár, 536, pp 1-7. 2015, URL cím: http://www.vedelem.hu/letoltes/anyagok/536-a-viz-tuzoltoi-felhasznalhatosaganak-lehetosegei-korlatai.pdf
[9] 41/1997. (V. 28.) FM rendelet az Állat-egészségügyi Szabályzat kiadásáról, Budapest, 1997.

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Kaluzsa Anikó
anikokaluzsa@gmail.com

A HAZAI VÍZGAZDÁLKODÁS RÖVID ÉRTÉKELÉSE

Absztrakt

A vízkészletek jelentős része az országhatáron átnyúlik, ezért megóvásuk csak nemzetközi összefogással valósulhat meg. A vízkészletek minőségét és mennyiségét óvó hazai intézkedések, a vízminőséggel szemben támasztott elvárások, és az ezeket szabályozó kormányrendeletek folyamatos megújítása biztosítja a naprakészséget. A fenntartható szemléletmód a vízfogyasztás terén mind a lakosság, mind az ipari szféra szempontjából elengedhetetlen. A hazai vízkészletek mind mennyiségileg, mind minőségileg folyamatosan csökkennek. A cikk írójának célja, hogy egy rövid áttekintést nyújtson a hazai vízgazdálkodásról. Továbbá bemutatja a vízkészletek során figyelembe vett minőségi kategóriákat, és kitér a vízbiztonság és a fenntartható vízgazdálkodás témakörére, mely részek együttesen segítik elő a vízbázisok védelmét.

The main part of water resources are across borders, so their preservation is only possible with international cooperation. The actuality is insured by the water resources national quality and quantity protective measures, water quality requirements and the ongoing renewal of government regulations. Sustainable approach is essential for both the population and the industrial sector in terms of water consumption. The domestic water resources are both reducing quantitatively and qualitatively. The author of the article is intended to provide a brief overview of the national water management. It also presents the quality categories of water resources and includes water security and sustainable water management issues, which parts collectively promote the protection of water resources.

Kulcsszavak: *vízgazdálkodás, vízellátás, vízminőség, fenntartható vízgazdálkodás ~ water management, water supply, quality of water, sustainable water management.*

BEVEZETÉS

A vízgazdálkodás az emberiség történelme során folyamatos változáson esett át, és ahogy a technológia alakult és modernizálódott, a vízgazdálkodásban is megjelentek azok a modern találmányok és fejlesztések, amelyek az adott korra jellemzőek voltak.

Arról, hogy mi miden tartozik a vízgazdálkodás fogalmába, nagyjából megegyeznek a szakvélemények. Vermes László szerint beletartozik minden olyan emberi tevékenység, mely a víz körforgásában szerepet játszik. [1: 106-107] Ligetvári Ferenc szerint tág értelmezésében egy olyan tevékenységi kör, mely a társadalom szükségleteinek vízigényeit összehangolja a természet vízháztartásával. A vízzel való gazdálkodás kialakulásának szükségessége akkor jelentkezett, mikor a vízkészletek és a vízigények között egy negatív különbség kezdett kialakulni. A vízgazdálkodás tevékenységi köre a történelem során eltérő feladatokat látott el, az adott környezet éghajlati, társadalmi-gazdasági viszonyaitól függött, és ezek a viszonyok jelenleg is döntően meghatározzák, hogy az adott területen mely tevékenységekre van dominánsan szükség. [2] A vízgazdálkodás sok különböző területet ölel fel, mint például a vízrendezés, árvízmentesítés, ipari vízszolgáltatás, vízellátás, csatornázás, öntözés, vízkészlet-gazdálkodás, stb. A jelen tanulmánnyal a vízkészleteket mutatom be a vízellátáson át a szennyvíz elvezetéséig, valamint a védelmi oldalon a vízbiztonsági terv szükségességét, és a fenntarthatóság elveit.

A VÍZKÉSZLETEKRŐL ÁLTALÁNOSSÁGBAN

A vizeink védelme, valamint a vízkészleteink folyamatos rendelkezésre állása kiemelt jelentőségű a vízellátás terén. A környezetünk biztonsága alapvető igényünk, és ennek feltétele a veszélyes tényezők kiszűrése, és előfordulásuknak a lehető legkisebb szintre csökkentése. A vízellátás a környezetbiztonság elvárásait és kihívásait is figyelembe véve hatékonyan csak nemzetközi keretek között tud mozogni, és a vízkészletek állapotának megóvása kizárólag akkor lehetséges, ha egy határokon átívelő együttműködés valósul meg. Szerencsére ilyen jellegű összefogásokra vannak igen jó példák, az egyik a Duna Stratégia Terv. Ez a Duna egész vízgyűjtő területére kiterjed, és célja a környezet védelme oly módon, hogy az energiahatékonyság és a gazdasági, társadalmi fejlődés a fenntarthatóság jegyében valósuljon meg. Erre több különböző lépést dolgoztak ki, például a súlyos bűncselekmények elleni fellépés, jólét megteremtése a régióban, a környezettudatosság beemelése az oktatásba, stb. [3]

A fenntartható életvitel fontosságát bizonyítja a tény, hogy a Földet borító vízfelszín csupán kis töredéke alkalmas ivóvíznek, és ráadásul ennek igen kis hányada áll rendelkezésünkre, melyet fel tudunk használni. A problémát fokozza a vizek egyenlőtlen eloszlása is. A vízkérdést tovább bonyolítja, hogy az elérhető ivóvízkészlet jelentősen csökkeni kezdett a globális felmelegedés, illetve a klímaváltozás következtében, amely jelenséget a rohamos iparosodás és a pazarló életvitel felgyorsított. A hazai ivóvízellátással kapcsolatosan megjegyzendő, hogy Magyarország klimatikus viszonyainak köszönhetően a vízhelyzet jobb, mint a világon általánosságban, mert a Kárpát-medence belsejében párolgási vízhiány uralkodik, valamint a felszín alatti vizek feltöltődése nagyon jó arányt mutat. Ha a csapadék mennyiségét és eloszlását is figyelembe vesszük, akkor a hazánkban lehulló víz mennyisége nem lenne elegendő a mezőgazdasági termelés számára, mely a legmagasabb vízfogyasztói ágazat. [4]

Jelenleg ivóvízzel öblítjük a WC-t, a tűzoltók ivóvízzel oltják a tüzet, locsoláskor és mosáskor is az ivóvízhez nyúlunk elsődlegesen. [5] Sokszor lehet hallani az érvelést, hogy ez a tendencia ahhoz vezethet, hogy a vízkészleteink csökkennek, majd elapadnak. Ha kimerül a

felszín alatti vízforrás, akkor a felszíni vizekből fogjuk az ivóvizet nyerni. Továbbá a szennyvizet a befogadóba engedés előtt fokozatosan és egyre jobban kezelni kell, ami még több kémiai anyag használatát jelenti, és hatalmas terhelés a környezet számára is. Ezek az érvelések nem alaptalanok, azonban eltúlzottak, ami a vízfogyasztást illeti. A cikk további részében ezt a gondolatot részletesebben kifejtem.

2015. év végéig elkészült a Magyarországra vonatkozó Vízgyűjtő-gazdálkodási Terv felülvizsgálata, a második Országos Vízgyűjtő-gazdálkodási Terv, valamint Magyarország Árvízi Kockázat Kezelési Terve. [6] Ezen tervek mindegyikének az a célja, hogy javítsa és védje a vizek állapotát, megakadályozza az állapotromlást, és a fenntarthatóság jegyében hosszú távú terveket tűz ki.

A HAZAI VÍZELLÁTÁS

A hazai víziközmű-szolgáltatás két fő részre oszlik, a vezetékes ivóvízellátásra és a közműves szennyvízelvezetésre. Magyarországon minden településen be van vezetve az ivóvíz, és a polgári lakosság 95%-ának van hozzáférése. Az ország évente nagyjából 440 millió m^3 vizet fogyaszt, és ennek háromnegyede lakossági fogyasztás. Az egy főre jutó napi átlagos vízfogyasztás 90-100 l/fő. A szennyvízelvezetés kiépítettsége 2013-tól nagyjából 75%-os szinten van. Ezek az értékek fix számoknak tekinthetőek a jövőre nézve, azaz a közművesítés elérte a növekedési maximumát. [7]

Jelenleg egy 1,4%-os csökkenési periódusban van a vízfogyasztás a magyar lakosság körében. Ez egy érdekes problémát okoz a közművekre nézve. A vízszolgáltatás kiépítésének a kezdetén magasabb, és egyre növekvő vízfogyasztással terveztek. A tendencia jelenleg ezzel ellentétben csökkenést mutat, ami a víztakarékos háztartási berendezéseknek, valamint a környezettudatos életmódnak és a háztartási spórolásnak tudható be. A kisebb vízfogyasztás pangó vizet eredményez a hálózatban, amit időszakosan ki kell engedni egy-egy végponton. Ennek a célja az, hogy felfrissítse a rendszert, ami környezet-egészségügyi szempontból egy fontos lépés. A másik probléma, hogy a hálózatos rendszerek nagyjából 80%-a fix költség, és akkor is fenn kell tartani a szolgáltatást (rendelkezésre kell állnia), ha azt csak kisebb mértékben veszik igénybe. Gyakorlatilag a hálózat fenntartási költségének nagy része a fogyasztástól független, amit a szolgáltató ráfordít a hálózatra (csőtisztítás, dolgozók bére, karbantartás, számlázási osztály, stb). Ez a tendencia egész Európára jellemző, és az ottani szolgáltatók is hasonló problémával találták szembe magukat. [7] Az iparosodás kezdetén szinte mindenhol nagyobb hálózatot építettek ki, és egy dinamikusan növekedő vízfogyasztással számoltak.

1. táblázat: A közüzemi ivóvízhálózathoz csatlakozott lakosság aránya 2011-ben Magyarországon és a környező országokban. Készítette: Szerző, MAVÍZ adatai alapján [7]

Magyarország	Csehország	Lengyelország	Szlovákia	Horvátország	Románia	Átlag
95%	94%	88%	87%	86%	57%	84,5%

Az alábbi táblázat adatai alapján jól látható, hogy a környező országok statisztikáit figyelembe véve Magyarország kiemelkedő arányt ért el az ivóvízellátás területén.

A hazai közműves vízellátás kezdete a római kor előtti időszakig nyúlik vissza. Az ókori vízszállító tevékenységtől a középkoron át az újkorig folyamatos fejlődést lehet megfigyelni. A modern kori vízellátás alapjai Budapesten 1868-ban kezdődtek, mikor a fővárosi vízellátáshoz a Vízvezetéki Irodát megalapították, majd Vízművek Igazgatósága néven beintegrálták a

Fővárosi Mérnöki Hivatalba, és kiépítették a jelenleg is üzemelő parti szűrésű kútrendszert. A technikai fejlesztések terén a villamosítással, később a számítógépek rendszerével a vízkitermelés a fejlődés egy új útjára lépett országosan. [8]

Hazánkban a teljes vízellátás 98%-a felszín alatti vízkészletre épül, melynek részben a rendelkezésre álló készletek, részben a kialakult hagyomány ad magyarázatot. Mivel a felszín alatti készletek gyakorlatilag az ország minden területén megtalálhatóak és hasznosíthatóak, ezért a közvetlen felszíni vízkivételek ivóvíz céljára csak azokon a területeken jellemzőek, ahol másképp nem lenne megoldható az ivóvízellátás. [4]

A vízminőség meghatározására a tisztasági fokozat szerint az alábbi kategóriákat használják:

- kiváló minőségű,
- jó minőségű,
- tűrhető minőségű,
- szennyezett,
- illetve erősen szennyezett víz. [9]

Az említett kategóriák szerint a kiváló és a jó minőségű víz emberi fogyasztásra alkalmas. A tűrhető minőségű vizeket megfelelő tisztítási eljárással még fel lehet használni újra. A szennyezett, valamint az erősen szennyezett víz a fertőzés és szennyezés veszélye miatt egyrészt nem fogyasztható, valamint az ilyen típusú vizek közvetlenül és közvetetten sem érintkezhetnek az emberrel, például úszás, fürdés során, vagy emberi fogyasztásra szánt növénytermesztés esetén, élelmiszer-feldolgozás során, stb.

Az eddig bemutatott vízszolgáltatási rendszer után jogosan merül fel a kérdés: Milyen értékeket tartalmazhat az ivóvíz? Ezt a 201/2001. (X.25) Kormányrendelet részletesen tartalmazza, és az értékeket szigorúan be szokták tartani, az adott vizsgálati időszakokat meghatározott rutinnal végzik a vízi közmű szolgáltatók. Az előírás szerint a víz akkor felel meg az ivóvíz minőségének, ha nem tartalmaz határérték feletti mennyiségű vagy koncentrációjú mikroorganizmust (Pl: *Escheria coli*), parazitát (Pl: *Giardia*), kémiai (pl: arzén, vas, nitrit) vagy fizikai anyagot, amely az emberi egészségre veszélyt jelenthetne. Továbbá, hogy ha a határértékeket nem is éri el a szennyeződés, emberi fogyasztásra alkalmas, de a vízfelhasználást zavaró tényezők vannak benne, akkor kifogásolt minőségű ivóvíznek kell tekinteni.

VÍZBIZTONSÁGI KÉRDÉSEK

A vízminőség védelem egy nagyon fontos és új aspektusa a vízgazdálkodásnak. Vizeink védelménél kiemelt figyelmet kell biztosítani a felszíni vizeinknek, mert nyitott jellegénél fogva sokkal több szennyeződés érheti a felszín alatti vízbázisokhoz képest. A felszín alatti vizek szennyezése viszont gyakrabban lehet rejtett, meglepetésszerű. Mindegyik vízbázis típusnak megvan a maga előnye és a hátránya. Például a karsztvíz nagyon egészséges és tiszta vizet nyújt. Viszont a sérülékenységi kockázata igen magas, és emiatt bármely szennyeződés akár pár óra leforgása alatt a rendszerbe tud jutni. Mind a felszíni és felszín alatti vizeinket óvni kell a szennyeződésektől. A kibocsátások kapcsán pedig odafigyelni, hogy a megengedett értéknél jobban szennyezett víz ne kerüljön a körforgásba. Az ivóvízellátás egy olyan infrastruktúra, melyre ráépülnek egyéb létesítmények, és tőle függnek is. Emiatt működését biztosítani kell, még egyes katasztrófák esetén is. A kritikus infrastruktúra, vagy más néven a létfontosságú létesítmények legtöbbször hálózatos rendszerűek, és a fellépő problémák következtében az egész rendszerben akadozás, valamint üzemzavar léphet fel. Egy ilyen esemény nem csak a szolgáltatást gyengítené meg, hanem kihatna a közbiztonságára is, ami további prob-

lémákat generálna. [10] A vízbiztonság fontossága elismert, és jelenleg több szervezet is együttműködik a vízi közmű szervezetek biztonságos működtetéséért hazánkban.

A világban bekövetkezett terrorista cselekmények és az infrastruktúrákat ért természeti csapások rávilágítottak, mennyire fontos kiemelni, mit is jelent a kritikus infrastruktúra, mely elemek emelhetőek be ebbe a fogalomba, és milyen óvintézkedéseket kell megtenni a védelmük érdekében. [11] A védelem kialakításának szempontjából a kockázatok tekintetében az alábbi három kategóriát szokás megkülönböztetni:

- természeti eredetű veszélyek,
- civilizációs, technológiai veszélyek,
- szándékos, ártó jellegű cselekmények.

A vízbázist érintő egyik legjellemzőbb veszélyforrás a nem megfelelő körültekintéssel végzett mezőgazdasági munka, amely a szerves- illetve műtrágyázás által nitrátot, foszfort, káliumot, növényvédő szer maradványokat, és egyéb egészségre veszélyes anyagot juttathat a vízbázisokba. A másik veszélyforrást az ipari és közlekedési szennyezés okozza jellemzően. Továbbá meg kell említeni még az árvizek és belvizek során bekövetkező minőségromlást is az ivóvízellátásban. [12]

Ezen kívül fontos megjegyezni, hogy a vízbiztonsági terv készítése azért is fontos, mert a vízellátási rendszerek bekerültek a kritikus infrastruktúra körébe. 2004-ben a madridi, majd 2005-ben a londoni terrortámadások a kritikus infrastruktúrák ellen is irányultak, ami sürgetőileg hatott az Európai Unióra, és felgyorsította a veszélyeztetett létesítmények megnevezésének körét. Az alaptörvény módosulása és elfogadásának következtében változott a katasztrófavédelmi törvény is, és határozatban fogadták el az új nemzetbiztonsági stratégiát. [13]

A vízbiztonsági terv fontosságát az Egészségügyi Világszervezet is hangsúlyozza. Az ivóvíz üzembiztonsági tervezéshez az alábbi szakaszokat különítik el: rendszervizsgálatot, működési monitoringot, valamint a menedzsmentet és azok dokumentációit. Ezek segítségével a vízi közmű társaságok pontos terveket tudnak készíteni az általuk lefedett területekre. [14]

FENNTARTHATÓ VÍZGAZDÁLKODÁS

A legjobb minőségű ivóvizet a felszín alatti vízkészletek szolgáltatják, ugyanakkor hazánkban romlik a víz minősége, tisztasága fokozatosan csökken. Ha ez a tendencia folytatódik, akkor a felszín feletti vízkészletekből kell megoldani majd a vízellátást. [15] Annak ellenére, hogy jelenleg ez a helyzet még nem áll fenn, pont azért, hogy ki se alakuljon ez az állapot, a megelőzésről már most gondoskodni kell.

Az Egészségügyi Világszervezet egyre inkább sürgeti a tagállamait, hogy dolgozzanak ki vízbiztonsági terveket, és ezeket terjesszék ki a lehető legmagasabb szintre, még az extrém, és kis valószínűségű fenyegetettségekre is. Az elsődleges veszélyeztetettséghez, mely a vízforrást érheti, az árvizet, belvizet, a szándékos rongálásokat, földrengéseket, az extrém időjárási körülményeket lehet sorolni. Ezen felül a másodlagos veszélynek főképp a meghibásodásokat tartják, melyek folyamatos felülvizsgálattal elkerülhetőek vagy megelőzhetőek. [16]

A kibocsátások szempontjából az egyik igen fontos szempont a befogadóba engedett tisztított szennyvíz. A szennyvíztisztítás Magyarországon igen jó hatásfokkal működik, és a csatornázottság mértéke már elérte a maximális értéket. Viszont a klímaváltozással, valamint az ennek következtében kialakult szélsőséges időjárással a szennyvíztisztító telepeknek is számolniuk kell, hiszen a megemelkedett csapadékszint jelentkezni fog a befolyt vízmennyiségnél. Továbbá, a vízbázisok védelmét akkor is biztosítani kell, amikor épp árvíz vagy belvízhelyzet alakult ki. Fontos, hogy a lehetséges lépéseket még a bekövetkező probléma előtt kell megtenni, azaz megfelelő üzemfolytonossági tervet kell készíteni az ivóvízbázisokra, a

szennyvizet megfelelően kell kezelni, az iparbiztonsági előírásokat be kell tartani és tartatni, és az elérhető legmagasabb színvonalon kell az elhasznált vizet megtisztítani a környezeti körforgásba való visszaengedés előtt. [17] A megváltozott időjárási körülmények újfajta felkészülési stratégiát követelnek, mind a kárelhárítás, mind a mentési körülmények terén, akár az eddig kialakított gyakorlatok korrelációjával, az eddig bekövetkezett események analízisével. [18]

Az EU irányelve a vízpolitika terén a közösségi fellépés kereteinek meghatározásáról rávilágít az ivóvízellátás egyik fő problémájára, nevezetesen, hogy egyre növekvő igény mutatkozik meg a kielégítő mennyiségű, jó minőségű ivóvíz iránt. A jó minőségű ivóvízre alapozott ivóvíz-ellátó rendszer képes hatékonyan hozzájárulni a lakosság biztonságos ivóvízellátásához. [19]

2015 év végéig elkészült az Országos Vízgyűjtő-gazdálkodási Terv, melyhez a lakosság is javaslatokat tehetett. Továbbá elkészült Magyarország Árvízi Kockázat Kezelési Terve is. Mindezek tartalmazzák a vizeink terhelésére vonatkozó kockázatokat, valamint azok állapotát is. Célul tűzték ki a jó állapot megőrzését, valamint ezzel párhuzamosan az állapotromlás megakadályozását. Az Európai Uniónak új víz- és vízi környezetgazdálkodási politikája van. Hazánk, mint az Európai Unió egyik tagállama, ennek köszönhetően részt vesz abban a nemes küldetésben, hogy 2021-ig megtervezze, és 2027-ig végrehajtsa a felszíni és felszín alatti vizek jó állapotának elérést. [6]

A hazai vízgazdálkodás számára további megoldás lehetne a természet közeli vízrendezési eljárások megvalósítása. A hazai tájak – és ezzel együtt a folyómedrek, az elöntésekkel szemben védetté nyilvánított, lecsapolt területek, a felszíni és felszín alatti vízkészletek – az elmúlt néhány száz év alatt rengeteg változáson mentek keresztül, melynek hatásait napjainkban is meg lehet figyelni. A vízkészletek mennyiségi problémája, hogy a felszíni vizeink – nagyrészt a tájátalakítások következtében – hasznosítatlanul továbbfolynak hazánkon. A lecsapolt területeken a folyó nem végzi el a hordaléklerakást, a vizek gyorsabban vonulnak végig az adott területen, kiöntésekkel, árvizekkel fenyegetve a régiót. További probléma, hogy a földkéreg alatti vízbázisok nem jutnak vízutánpótláshoz egyes területeken, és ez által a víznyeréshez mind újabb és újabb kutakat kell fúrni, mind mélyebbre és mélyebbre. A tájak rehabilitációját, valamint a vízkészletek feltöltését is elősegítené a kistáji vízkörzések kialakítása. Kisebb területeken a megemelkedett vízszintnél az adott régiót időszakosan elárasztva a vízkészletekbe visszaszivárog a víz, a talajra a folyókiöntésekkel jó minőség hordalék kerülne, és a mezőgazdaság számára a víztározás kérdésének egy része is megoldódna. [20]

KÖVETKEZTETÉSEK

Hazánk felszín alatti vízkészletei fedezni tudják a vízfelhasználás során jelentkező igényeket. A lakossági vízfogyasztás tendenciájával sincsen gond. A társadalmat lényegileg nem arra kell ösztönözni, hogy kevesebb vizet fogyasszon, mert a hálózat rendelkezésre állása még egy 5-10 %-os vízigény emelkedést is ki tud elégíteni, és a felszín alatti vízkészleteink is elegendőek ennek támogatásához hosszú távon is. Továbbá, a rendszer méretei miatt, függetlenül a vízfogyasztástól, folyamatosan ki kell termelni az adott mennyiségű vizet. A száraz területeken, ahol a víz nehezen hozzáférhető, ott természetesen létfontosságú, hogy spóroljanak a vízzel.

A lakosságot arra kell ösztönözni társadalmilag, hogy olyan termékeket használjanak, melyek környezetbarátok, könnyen lebomlanak, semlegesíthetőek, nem okoznak maradandó károsodást a vizekben, és vízbe kerülve a lehető legkisebb környezetterhelést okozzák. A háztartási tisztítószereken át a mosóporokon keresztül a samponon át rengeteg lehetőség van erre.

A fenntarthatóság szempontjából a lényegi kérdés a felszíni vizeink, és felszín alatti vízbázisaink védelme a szennyeződéstől. Ehhez mind a lakossági, mind az ipari szennyvíz minőségi javulása hozzájárul. Így véleményem szerint nem a vízfogyasztáson van az igazi hangsúly, hanem a befogadóba visszaengedett víz minőségi értékein. Ahogyan a polgári lakosság változtatni tud a kibocsájtott értékein, ugyanúgy az ipari szektorban is fontos, hogy változások álljanak be a kibocsátott szennyvíz minőségi paramétereiben. A két szektor együttes odafigyelése lényeges javulást eredményezhet a felszíni és felszín alatti vízbázisaink minőségi értékeiben.

Végül, de nem utolsó sorban, az egyik igen fontos szempont a tájrendezés. A természetes – folyószabályozás előtti – állapotokhoz való részleges visszatérés mind a talaj termőképességét, mind a felszín alatti vízkészletek visszapótlódását elő tudná segíteni.

Felhasznált irodalom:

[1] Vermes L.: *Vízgazdálkodás*. Budapest: Mezőgazdasági Szaktudás Kiadó, 1997.

[2] Ligetvári F.:A vízgazdálkodás alapjai. www.tankonyvtar.hu/hu/tartalom/tamop412A/2010-0019_A_vizgazdalkodas_alapjai/ch01s02.html (Letöltve: 2016.01.29. 18:10)

[3] L. Muresan: The StrategyfortheDanube Action Plan. Berlin: EURISK Foundation, 2011. www.hss.de/download/110606_RM_Muresan.pdf (Letöltve: 2015.10.05. 16:20)

[4] Mádlné Szőnyi Judit (szerk.): Hidrogeológia. Elektronikus egyetemi jegyzet, 2013. elte.prompt.hu/sites/default/files/tananyagok/Hidrogeologia/book.pdf (Letöltve: 2016.02.09. 19:19)

[5] Kuti R.: A víz tűzoltói felhasználhatóságának lehetőségei, korlátai. Védelem, *Tűz- és Katasztrófavédelmi Szakkönyvtár*, 536 (2015) 1–8. www.vedelem.hu/letoltes/tanulmany/tan536.pdf (Letöltve: 2015.10.02. 19:50)

[6] EU Víz Keretirányelv honlapja. www.euvki.hu (Letöltve: 2016.01.27. 16:20)

[7] Magyar Víziközmű Szövetség: A magyar víziközmű ágazat bemutatása – Átfogó tanulmány. www.maviz.org/system/files/kpmg-maviz_vizikozmu_agazati_helyzetkep_20150513.pdf (Letöltve: 2016.01.21. 18:07)

[8] Károlyi A., Tolnai B.: Víz-rajz – 140 éve a főváros szolgálatában. www.vizmuvek.hu/jubileum/pics/konyv.pdf (Letöltve: 216.01.22. 13:40)

[9] Rácz L. I.: Magyarország felszíni és felszín alatti vizeinek minősége, védelme. *Hadmérnök*, IX 2 (2014) 257–266.

[10] Mógor J., Földi L., Solymosi J.: Lépések a kritikus infrastruktúra védelmének magyarországi szabályozása felé. *Hadmérnök*, III 4 (2008) 15–28.

[11] Laczik B.: A kritikus infrastruktúra védelem elveinek, céljainak és a veszélyes ipari üzemek biztonságának összefüggései, kapcsolatuk. *Hadmérnök*, VI 2 (2011) 55–68.

[12] Berek T., Rácz L. I.: Vízbázis, mint nemzeti létfontosságú rendszerelem védelme. *Hadmérnök*, VIII 2 (2013) 120–133.

[13] Horváth A.: A kritikus infrastruktúra védelem komplex értelmezésének szükségessége. In: Horváth A.:*Fejezetek a kritikus infrastruktúra védelemből II*. Budapest: Magyar Hadtudományi Társaság, 2013.

[14] Berek T.,Dávidovits Zs.: Vízbiztonsági terv szerepe az ivóvízellátás biztonsági rendszerében. Hadmérnök,VII 3 (2012) 14–25.

[15] Dávidovits Zs.: A lakossági vízellátás környezetbiztonsági kockázatai és a vízminősítés laboratóriumi módszerei. *Védelem*, 2011. december. 1–11. www.vedelem.hu/letoltes/tanulmany/tan374.pdf (Letöltve: 2015.10.03. 18:20)

[16] Dávidovits Zs.:What extent can drinking water safety plan reduce the risks coming from disasters in the public water supply? *Hadmérnök*, IX 2 (2014) 241–249.

[17] Földi L.: A klímaváltozás által jelentkező új kihívások a kritikus infrastruktúra védelmében. In: Horváth A.:*Fejezetek a kritikus infrastruktúra védelemből I.* Budapest: Magyar Hadtudományi Társaság, 2013.

[18] Kuti R., Nagy Á.: Weather Extremities, Challenges and Risks in Hungary. *Aarms*, XIV. 4 (2015), 299-305.

[19] Berek T.,Dávidovits Zs.: Vízbiztonsági terv az ivóvízellátás minőségirányítási rendszerében. *Hadmérnök*, VII 3 (2012) www.hadmernok.hu/2012_3_davidovits_berek1.pdf (Letöltve: 2016.01.27. 14:49)

[20] Molnár G.: Az ártéri gazdálkodás - a Kárpát-medencei gazdasági-politikai kontinuitás alapja V. rész : Az ártéri gazdálkodás és az egyes ártéri haszonvételek. *Országépítő*: 1992. III. 3-4. Pp: 69.

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Molnár Robin
robin.molnar105@gmail.com

A TŰZOLTÓI BEAVATKOZÁSOK KÖRNYEZETRE GYAKOROLT HATÁSAI

Absztrakt

Az utóbbi években folyamatosan szigorodnak a környezetvédelmi normák, Magyarországon is egyre nagyobb figyelmet kap a környezetvédelem. Az extrém időjárási jelenségek egyre jobban éreztetik hatásukat, egyre sűrűbben következnek be természeti csapások, katasztrófák. Írásomban bemutatom, hogy a hazai tűzoltók tevékenysége a különféle kárfelszámolások során milyen hatást gyakorol a természeti és a humán környezetre. Kutatásom során vizsgáltam, hogy egy-egy tűzeset, vagy műszaki mentés, milyen hatással van az épített és a természetes környezetre, a beavatkozást végző tűzoltók hogyan járulhatnak hozzá a környezetterhelés csökkentéséhez.

Environmental protection standards are continuously getting stricter in recent years; focus is changing towards environmental protection in Hungary as well. Extreme weather conditions and natural catastrophes occur increasingly more often. In my work, I am showcasing the effects of the different actions of the Hungarian firefighters -- in cleaning up and reconstructing after natural disasters – on the natural and the human environment. During my research I have investigated the effects of fires and technical rescues on the man-made and the natural environment, and how the firefighters in action can decrease the ecological footprint of the intervention.

Kulcsszavak: *környezetvédelem, tűzoltói beavatkozások, környezeti elemek, környezeti károk ~ environmental protection, fire intervention, environmental elements, environmental damage*

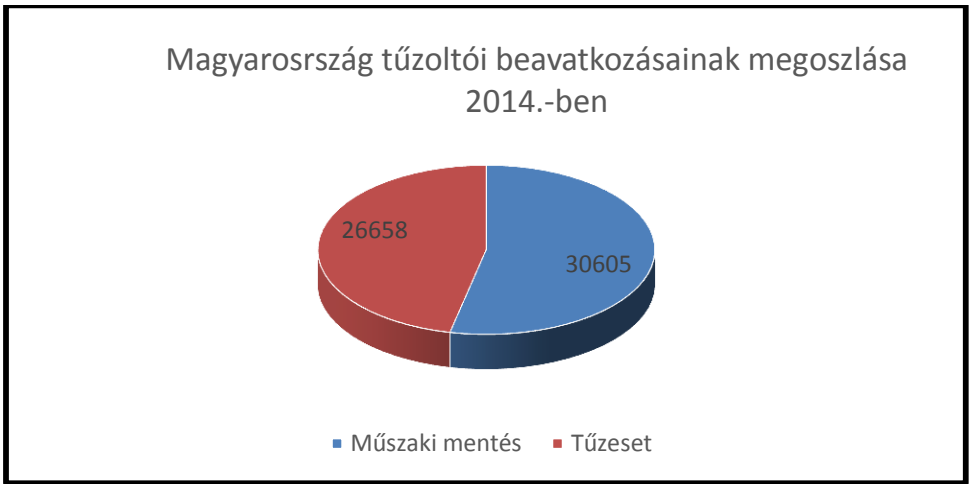
BEVEZETÉS

Magyarországon a tűzesetek és műszaki mentések elhárítása a tűzoltók feladata. A prevencióra nagy hangsúlyt fektetnek a hatóságok, de időről-időre bekövetkezik egy-egy nagyobb szerencsétlenség. A káreset méretétől függetlenül hatással lesz a természeti vagy az épített környezetre.

Írásomban vizsgálom a tűzoltói beavatkozások környezeti elemekre gyakorolt hatásait, fel kívánom hívni a figyelmet a környezetvédelem fontosságára, hogy a különféle kárfelszámolások során lehetőleg megelőzhető legyen a további károkozás, valamint lehetőségeket mutatok be annak csökkentésére.

KÁRFELSZÁMOLÁSOK KÖRNYEZETI HATÁSAI

A katasztrófavédelemnél operatív munkát végezve gyakran találkozom környezetkárosító tényezőkkel. Általában ez a káresetek fajtájától és mértékétől függ, de gyakran a beavatkozó állomány nagymértékben kiveszi részét a környezet rongálásából. A tűzoltók egy-egy beavatkozás során bontással vagy roncsolással kell, hogy behatoljanak épületekbe, az ilyen esetekben az épített környezetet károsítják. Egy-egy műszaki mentés során favágást kell alkalmazni, mert például másképpen az árokba hajtott autót nem lehet kiemelni. A tűzoltók erőd és vegetáció tüzeknél járműeikül az ép részeket károsíthatják. Erdőtüzek során a tovább terjedés elkerülése érdekében ép, egészséges fákat kell eltávolítani. Ezek az esetek a természeti környezet károsítják természetesen a nagyobb kár megelőzésének érdekében. Természetesen életmentésnél, robbanás veszély elhárításánál keveset lehet mérlegelni egy esetleges károkozás tekintetében. A tűzoltóság egységei leggyakrabban tűzesetek és műszaki mentések során végeznek beavatkozásokat, melyet a következő ábra jól szemléltet.



1. ábra Tűzoltói beavatkozások megoszlása 2014. évben [1]

Ezek az események már magukban is környezet-károsító hatásokat fejtenek ki, ezeket gyakorlati példák bemutatásán keresztül vizsgálom külön-külön tűzesetek és műszaki mentések tekintetében. A környezetbiztonság problémakörének kezelése napjaink aktuális kérdésköre, amelyet a kárfelszámolások során is figyelemmel kell kísérni [2]. A megelőzés és a környezeti károk csökkentésének érdekében fontosnak tartom a következő környezeti elemekre gyakorolt hatások vizsgálatát:

- Levegő,
- Víz,
- Talaj,

- Élővilág,
- Táj,
- Mesterséges környezet.

Fontos ismernünk a környezeti ártalmak terjedésének formáit, ennek ismeretében könnyebben behatárolhatók az események káros hatásainak kitett területek.

- Kibocsátás (emisszió), ez lehet pont, vonal, vagy felületi forrás,
- Szétterjedés (transzmisszió), szennyező anyagok terjedése a környezetben,
- Kiülepedés (immisszió), szennyező anyagok megjelenése a környezetben [3].

TŰZESETEK KÖRNYEZETI HATÁSAI

A tűzeseteket vizsgálva megkülönböztetünk nyílt téri és zárt téri tüzeket, ez környezetvédelmi szempontból is fontos, továbbá a szennyezés tekintetében külön kell elemezni a természetes, illetve mesterséges anyagok égését. Előbbi megkülönböztetés szerint egy vegetációtűz és egy lakástűz példáján mutatom be a környezeti hatásokat.

Levegő

A vegetációtüzek komoly füstképződéssel járnak, az égés nem tökéletes, ennek oka a különböző nedvességtartalmú anyagok égése. A növények égése során nagy mennyiségű szén-dioxid keletkezik, amely gyorsítja a globális felmelegedést. Keletkezik szén-monoxid is, amely káros az élőlényekre. Amennyiben az égés zöld területekre is átterjed, további mérgező égéstermékek kerülnek a levegőbe. A tűz által gerjesztett gázcsere következtében az égéstermékek belekerülnek a magasabb légmozgásokba, amelyek a tűztől akár 10-20 km távolságra is elszállítják az égéstermékeket, ahol kihullva kifejtik szennyező hatásukat.

A lakástüzek során nemcsak szerves anyagok égnek, hanem különféle műanyag származékok, gumitermékek is. Az égés során ezeknél a tüzeknél is keletkezik szén-monoxid és szén-dioxid, viszont a műanyag és gumitermékek tüzeinél nagymennyiségű toxikus gáz és korom is képződik. A tűzoltói beavatkozások gyorsaságától függően kerül kevesebb, vagy nagyobb mennyiség a levegőbe. A toxikus gázok rendkívül veszélyesek az élő szervezetekre, ezért fontos lakástüzek esetén a bent lévő személyek kimenekítése. A légszennyezés csökkentésének érdekében fontos tehát a jól szervezett, hatékony tűzoltói beavatkozás.

Víz

A nagykiterjedésű vegetációtüzek közvetlen és közvetett módon is szennyezhetik a vizeket. Közvetlenül a tűz közelében lévő élővizekbe kerülve a füstből kihulló pernye és a kisebb növénymaradványok szennyeznek, közvetve a magasabb légáramlatokba kerülő szennyezők távolabb kihullva fejtik ki károsító hatásaikat. Ezek az anyagok a vizekben veszélyeztetik a vízi élővilágot.

Lakástüzek során a kiáramló füstből kihulló égéstermékek a fentiekben leírt módon veszélyeztetik a vizeket, itt további problémaként jelenik meg az elfolyó oltóvíz, vagy egyéb oltóanyag (hab), amely a vízelvezető csatornákon keresztül közvetlenül az élővizekbe kerülhet [4]. Az elfolyó oltóvízben a füstből kicsapódó toxikus anyagok is lehetnek, amelyek a vízi élővilág károsításához okozhatja. A vízszennyezés csökkentésének érdekében fokozottan kell figyelni az optimális oltóanyag felhasználásra.

Talaj

A vegetációtüzek során az érintett területen teljesen kipusztul a növényzet. Az égés során fellépő intenzív hő terheléstől a talaj felső rétege elporlik, termőképtelen lesz, abban a növények életéhez szükséges mikroorganizmusok kipusztulnak. Az eső hatására erózió léphet fel. Az eredeti területen őshonos növényekhez képest más növényfajták is megjelenhetnek a későbbiekben, amelyeknek a megváltozott körülmények is megfelelnek.

A lakástüzek csak abban az esetben jelentenek veszélyt a talajra, ha az elfolyó oltóvíz közvetlenül a talajra kerül, ebben az esetben a vízben található mérgező anyagok bemosódnak a talajba és ott fejtik ki károsító hatásukat. Ebben az esetben meg kell jelölni az elfolyó oltóvíz által érintett területet.

Élővilág

A vegetációtüzek komoly hatást gyakorolnak a terület élővilágára. Azok az emlősök, amelyek, képesek elhagyni a tűz által érintett területet életben maradhatnak, a többi állat elpusztul. Ugyanez igaz a madarakra is. Az érintett területen élő rovarok nagy része szintén elpusztul a tűz közvetlen hatásai miatt. Azok az élőlények, melyeknek járatai a föld alatt olyan mélységben találhatók, amit a hőhatás nem ért, túlélhetik a tüzet, viszont a kialakult körülmények jelentős hatással lehetnek táplálékforrásaikra, ezáltal további életükre is. A lakástüzek csak a képződő füst és hő hatásainak kitett emberekre és állatokra nézve jelentenek közvetlen veszélyt. A tűz elől menekülni képtelen élőlények könnyen szenvedhetnek füstmérgezést, valamint égési sérüléseket, amelyek később halálhoz vezethetnek. Lakástüzek felszámolása során fontos a személyi védőfelszerelések használata, továbbá a hatékony hő és füst elvezetés biztosítása.

Táj

Egy nagy kiterjedésű vegetációtűz után a táj nagyban átalakulhat. Első változás a teljesen üres, szürke terület képe. Ez a kép az új növényvilág megjelenéséig is folyamatosan változik az eső és a széleróziónak köszönhetően. További változást az új növényfajták megjelenése okozza, melynek hatására szintén átformálódik a táj képe.

Lakástüzek akkor idéznek elő változást a tájban, ha az érintett ingatlan természeti környezetben épült és a tűz kitört az épületből és továbbterjed, valamint annak teljes megsemmisüléséhez vezet.

Mesterséges környezet

Vegetációtűz közvetlenül abban az esetben gyakorol hatást a mesterséges környezetre, ha a tűz lakóövezetbe is továbbterjed és ott az épületekben is kárt okoz. Közvetve a tűz során keletkezett füst is káros hatást gyakorolhat a mesterséges környezetre, ha az annak irányába terjed.

Lakástüzek már az égés során is megváltoztathatják a környezet képét, ha a tűz kitör az ingatlanból. Ha a tűz során az ingatlan olyan mértékben károsodik, hogy az bontásra kerül, akkor teljesen átalakulhat az adott városrész képe.

TŰZESETEK, TŰZOLTÁSI TEVÉKENYSÉG KÁROSÍTÓ HATÁSAINAK CSÖKKENTÉSI LEHETŐSÉGEI

A tűzoltóság egységei legtöbb esetben vizet használnak tűzoltásra, a belső szabályozók kis mértékben kitérnek a másodlagos károk elkerülése érdekében végzendő cselekményekre, de

egy V. emeleti panellakás tüzének oltása során elkerülhetetlen hogy az alatta lévő lakások ne szenvedjenek vízkárt. A hagyományos sugarak alkalmazása során, annak ellenére, hogy a hazai tűzoltóknak meg van határozva az, hogy sugárcsövüket szakaszosan használják, nagy mennyiségű oltóvíz kerül kijuttatásra a tűzre és a lakás visszahűtésére. Ennek értelmében csak a minimálisan szükséges vízmennyiséget jutassák ki a tűzre, az épületelemek alkotórészeire visszahűtés céljából. Tűzoltóink erre nagy hangsúlyt fektetnek, bevetések során kötött sugarat csak akkor használhatnak, ha kifejezetten erre kapnak utasítást. A tűzoltó eszközök fejlesztésének következtében kevesebb víz felhasználásával is kiváló oltóhatás érhető el, erre jó példa a vízköddel oltó berendezés [5]. Ezek alkalmazásával az oltóvíz felhasználás a hagyományos sugarakhoz képest lényegesen kevesebb, a másodlagos károkozás pedig elenyésző [6]. A tűzoltó szakfelszelések alkalmasak vízeltávolításra is, belvizes időszak esetén az épített környezet megóvása érdekében alkalmazhatóak, ugyanakkor intenzív esőzések után a telített pincéket is képesek vízteleníteni [7]. Pozitív nyomású ventilláció alkalmazásával pedig csökkenthető a hőterhelés és gyorsabban lehet eloltani a tüzeket.

MŰSZAKI MENTÉSEK KÖRNYEZETI HATÁSAI

A természeti környezetbe legtöbb alkalommal a közlekedési balesetek elhárítása során avatkoznak be a tűzoltók. Magyarországon a tűzoltóegységek a 2014. évben 57.263 alkalommal kerültek riasztásra ebből 30.605 db műszaki mentésnél és 26.658 tűzesetnél avatkoztak be (1. sz. ábra). Egységeink 12.009 alkalommal működtek közre közlekedési balesetek felszámolásánál, ez a legnagyobb számban előforduló műszaki mentés, így ezek környezeti hatásait elemzem részletesen. A közlekedési balesetek, valamint ezek felszámolása során legtöbb esetben az eset közvetlen környezetére fejt ki hatást, de veszélyes anyagokkal kapcsolatos balesetek során, nagyobb területen is bekövetkezhet környezeti károkozás.

Közúti balesetek során sűrűn előfordul, hogy a járművek lesodródnak az úttestről, ezért az életmentés érdekében, vagy rendőrségi baleseti helyszínelés után, a forgalmi akadály megszűntetésére útszéli fákat, cserjéket kell kivágni a tűzoltó egységeknek. Sok esetben a járművek fának csapódnak, cserjék közé szorulnak, extrém esetekben, vagy nagyobb járművekkel kapcsolatos balesetek következtében fák is dőlhetnek az útra, a járművekre. Ilyen esetekben legtöbbször a favágást is el kell elvégezni a további munkálatok érdekében. Ezek a munkálatok nyomot hagynak a tájban.

Közúti balesetek során nagy számban fordul elő motorolaj, vagy üzemanyagfolyás, illetve szivárgás. A beavatkozás ennek a felitatására, továbbterjedésének megakadályozására is irányul. Általában kis mennyiségű üzemanyag és/vagy kenőanyag (max. kb. 50l) szabadba jutása történik, de tehergépjárművek balesetei során ennek többszöröse is az úttestre kerülhet. A tűzoltóság a gépjárműfecskenőkre málházott homokkal vagy a káreset helyszínén összegyűjtött földdel felitatja a kiáramlott anyagot, ezzel megakadályozva a további balesetveszélyt. Nagyobb káresemények felszámolásánál a műszaki mentő bázisokon található abszorbens anyagok állnak rendelkezésre a felitatásra. A szennyezett felitató anyagot a tűzoltóság egységei nem szállítják el. Az eljárás következő lépéseként a közútkezelő küld egy aszfalttisztító gépet, mely összesöpri és az útszélére tereli az így kialakult „masszát”. További intézkedés ezzel a földes/homokos, motorolajos/üzemanyagos kialakult anyaggal legtöbb esetben nem történik. Egy eső hatására a szennyező anyagok a talajba szivárognak. A 2. számú képen egy közúti baleset következtében a lejtős útszakaszon az eső hatására a kifolyt üzemanyag terjedt, végül az útról lefolyva a környezetet szennyezve tovább.

2. ábra Kifolyt üzemanyag terjed az esőben (saját készítés)

VESZÉLYES ANYAGOKKAL KAPCSOLATOS BALESETEK HATÁSAI

Fontos feladat a veszélyes anyagokkal történő balesetek felszámolása. Akkor is károsodik a környezet, ha kis mértékben sérül a szállított anyag csomagolása, nagyobb eseményeknél akár ki is szóródhat vagy folyhat a termék, ezáltal jelentős hatást gyakorolva a környezeti elemekre és a beavatkozást végzőkre. A veszélyes anyagok jelenlétében történő beavatkozások szigorú szabályok alapján történnek a tűzesetek, a műszaki mentések esetében is. A beavatkozások tervezésénél és szervezésénél a parancsnokoknak intézkednie kell a személyi állomány védelméről, a veszélyes anyag továbbterjedésének megakadályozásáról, az erők- eszközök mentesítéséről és a kifolyt anyag felitatásáról [8].

Elsődleges intézkedések

Az elsődleges intézkedésekre a német szakirodalomban egy a teendők betűiből összeállított betűszóval jellemzett főszabály (GAMS szabály) terjedt el:

- veszély felismerése
- lezárás, biztosítás
- emberéletek mentése
- speciális erők riasztása (pl. műszaki mentőbázisok, KML[1], mentők, szakértők)

Amennyiben a veszélyes anyag baleset környezetében emberek közvetlen életveszélyben vannak, akkor az életmentés érdekében a beavatkozók sűrített levegős légzőkészülékben és a szükséges szintű vegyi védőruhában azonnal beavatkozhatnak.

A beavatkozás és a környezeti károk csökkentésének érdekében folyamatosan figyelemmel kell lenni:

[1] Katasztrófavédelmi Mobil Labor

- A szabadba áramló anyag tulajdonságainak, mennyiségének, terjedési irányának megállapítására.
- A tűz és a veszélyes anyag egymásra hatásából adódó veszélyek megismerésére (a keletkező bomlás- és égéstermékek hatásaira).
- Az életmentés lehetséges módozatainak meghatározására.
- Az időjárási viszonyokra.
- A kiürítendő területek behatárolására.
- Az alkalmazandó oltó-, közömbösítő, felitató és mentesítő anyagokra illetve azok kirendelésére.
- A biztonságos, átmeneti és a veszélyes zóna meghatározására.
- A lezárandó terület, útvonalak kijelölésére.

A fő cél a veszélyes anyagokkal (por, folyadék, direkt gázsugár) való közvetlen érintkezés elkerülése [9]. A beavatkozásokat megfelelő algoritmus szerint, összehangoltan kell végezni a felderítéstől, a veszélyes anyagokkal kapcsolatos utómunkálatok befejezéséig [10]. A kárfelszámolások során nagyon fontos a veszélyes anyagok beazonosítása, melyhez különféle detektáló eszközök kerültek rendszeresítésre, ezek használata elengedhetetlen, ha a kísérő okmányok sérültek, vagy hiányosak [11]. A folyamatban nagy szerep jut a Katasztrófavédelmi Mobil Laboroknak (KML), melyek a málházott eszközök segítségével képesek a veszélyes anyagot kimutatni és beazonosítani. A rendszeresített eszközökkel időjárási modelleket tudnak készíteni ezzel előre jelezni, hogy az anyag merre terül el, így támogatva a döntéshozókat.

A kárfelszámolási munkálatok befejezése után vegyimentesítést kell végezni. Lehetőség szerint meg kell gátolni a mentesítő folyadékok környezetbe jutását is, annak felfogására, elszállítására a mentésvezetőnek intézkednie kell [12]. Természetesen a beavatkozások alatt is kötelességünk a környezet védelme, erre rendszeresített eszközök megtalálhatók a Regionális Műszaki Mentőbázisok vegyi elhárító konténereiben. Képesek vagyunk csatorna szemeket elfedni, réseket tömíteni, kifolyt anyagok továbbterülését megakadályozni, gátat felállítani és a kifolyt anyagokat összegyűjteni, valamint kármentő edényekben tárolni. A rendszeresített eszközök alkalmasak a beavatkozások biztonságos végrehajtásához, a teljes testvédelemre szolgáló védőruhák megfelelő védelmet nyújtanak.

A veszélyes anyagokkal kapcsolatos balesetekről elmondható, hogy a szabadba jutott anyagok fajtájától, halmazállapotától függően komoly szennyező hatást fejtenek ki a levegőre, a vízre, a talajra, veszélyt jelentenek az élő szervezetekre.

A levegőbe került szennyező anyagot lehetőség szerint vízzel le kell csapatni, ha víz nem használható, akkor figyelemmel kell kísérni a felhő továbbterjedését, mérni a veszélyes anyag koncentrációt, meghozni a szükséges lakosságvédelmi intézkedéseket.

A vízbe került szennyeződéseket lehetőleg el kell távolítani a vizekből, különféle technológiai berendezések alkalmazásával, vagy ha ez nem lehetséges, akkor közömbösítő vegyi anyagok vízbe juttatásával kell csökkenteni a károsító hatásokat.

A talajba került szennyező anyagok eltávolítása nem a tűzoltóság feladata, fel kell venni a kapcsolatot az illetékes társ-hatósággal, akik intézkednek a továbbiakról [13].

A káresemény felszámolását követően az esetleges talajcserét a Megyei Kormányhivatalok, Környezetvédelmi és Természetvédelmi Főosztálya rendeli el és gondoskodik is róla, így anyagtól függően meggátolható legyen a további környezetkárosítás. A nem természeti katasztrófánál az előidézőnek kell intézkednie és közreműködnie a felszámolásról és helyreállításról, erről a 2011. évben elfogadott új katasztrófavédelmi törvény rendelkezik az alábbiak szerint:

„(1) A védekezést és a következmények felszámolását az erre a célra létrehozott szervek és a különböző védekezési rendszerek működésének összehangolásával, az állampolgárok,

valamint a polgári védelmi szervezetek, a gazdálkodó szervezetek, a Magyar Honvédség, a rendvédelmi szervek, a Nemzeti Adó- és Vámhivatal, az állami meteorológiai szolgálat, az állami mentőszolgálat, a vízügyi igazgatási szervek, az egészségügyi államigazgatási szerv, az önkéntesen részt vevő civil szervezetek és az erre a célra létrehozott köztestületek, továbbá nem természeti katasztrófa esetén annak okozója és előidézője, az állami szervek és az önkormányzatok (a továbbiakban együtt: katasztrófavédelemben részt vevők) bevonásával, illetve közreműködésével kell biztosítani." [2]

ÖSSZEGZÉS

Írásomban bemutattam a tűzesetek és különféle balesetek környezeti hatásait, valamint rávilágítottam, hogy a tűzoltói beavatkozások is komoly hatásokat gyakorolnak a környezetre. Magyarországon a tűzoltó egységek környezetvédelmi feladatai csak kis mértékben vannak leszabályozva, a jelenlegi beavatkozási szabályok sem térnek ki minden területre. A káreset utóélete nincs egy kézben tartva, az esetleges veszélyes hulladékok eltávolítása és megfelelő kezelése többnyire nincs hatóságilag ellenőrizve. Véleményem szerint a katasztrófavédelem egy egységként kell, hogy kezelje a megelőzést, védekezést, helyreállítást. A helyreállításon belül fontos szerephez kell, hogy jusson a hulladékok kezelése. Bízom benne, hogy környezetünk védelme érdekében ezeket a problémákat hamarosan megoldják a döntéshozók.

Felhasznált irodalom

[1] Szerző összeállítása a BM OKF adatai alapján.

[2] Földi László – Halász László: Környezetbiztonság, ISSN 2060-8047. Complex Kiadó Kft. Budapest, 2009

[3] Rácz László – Tölgyessy György – Papp Lajos – Lesny György: Környezeti Kémia, EKF Líceum Kiadó Eger, 2002

[4] Nagy Zsolt – Kuti Rajmund: Tűzoltóhabok környezeti hatásai, Hadmérnök on-line, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar és a Katonai Műszaki Doktori Iskola on-line tudományos folyóirata, X. Évfolyam. 3. szám, 2015, URL cím: http://hadmernok.hu/153_12_nagyzs_kr.pdf (letöltés ideje: 2015. 11. 30.)

[5] Kuti Rajmund: Miben rejlik a vízköd tűzoltási hatékonysága? Védelem Online: Tűz-és Katasztrófavédelmi Szakkönyvtár, 501, pp 1-7. 2014, URL cím: http://www.vedelem.hu/letoltes/tanulmany/tan501.pdf

[6] Rajmund KUTI – László FÖLDI: Extreme weather phenomena 2. The Process of Remediation, Hadmérnök on-line, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar és a Katonai Műszaki Doktori Iskola on-line tudományos folyóirata, IX. Évfolyam 2. szám, 250-256. o. 2014. július. ISSN 1788 1919. URL cím: http://hadmernok.hu/142_23_foldil_kr.pdf

[7] Kuti Rajmund: Advantages of Water Fog Use as a Fire Extinguisher, AARMS, Volume 14, No. 2 (2015) pp. 259-264. http://uni-nke.hu/uploads/media_items/aarms-2015-2-nyomdai.original.pdf (letöltés ideje: 2015. 11. 30.)

[8] Kuti Rajmund: Milyen mentesítő anyagokat használjunk, milyen eljárásokat alkalmazzunk veszélyes anyag beavatkozások után? Védelem Online: Tűz-és Katasztrófavédelmi Szakkönyvtár, 203, pp. 1-6. 2008, URL cím: http://www.vedelem.hu/letoltes/tanulmany/tan203.pdf

[9] Heizler György tű. ezds.: Bevetés-taktikai alapelvek veszélyes anyagoknál, Védelem-online Tűz-és Katasztrófavédelmi Szakkönyvtár, URL cím:

[2] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

http://www.vedelem.hu/letoltes/anyagok/338-bevetes-taktikai-alapelvek-veszelyes-anyagoknal.pdf (letöltés ideje: 2015. 11. 30.)
[10] Kuti Rajmund - Zólyomi Géza: Intézkedési algoritmus veszélyes anyag balesetek felszámolásához, Védelem katasztrófa- tűz– és polgári védelmi szemle, XV. évf. 4. szám 14-15. o. 2008. ISSN 1218-2958, URL cím: http://vedelem.hu/letoltes/ujsag/v200804.pdf
[11] Kuti Rajmund: Veszélyes anyag balesetek felderítését támogató eszközök a svájci tűzoltóságnál, Védelem katasztrófa- tűz– és polgári védelmi szemle, XIX évf. 3. szám 26-27. o. 2012. ISSN 1218-2958, URL cím: http://vedelem.hu/letoltes/ujsag/v201203.pdf
[12] Rajmund Kuti, László Földi: Possible use of mobile water fog generators for decontamination tasks, AARMS Academic and Applied Research in Military Science Vol. 8, Issue 1 (2009) Budapest p. 127–132. ISSN 1788-0017 (Online), ISSN 1588-8789 (Print) URL cím: http://www.zmne.hu/aarms/docs/Volume8/Issue1/pdf/12kuti.pdf
[13] Dr. Földi László, Dr. Halász László – Környezetmérnökök katasztrófavédelmi feladatai Környezetmérnöki Tudástár XXXIII. kötet ISBN: 978-963-396-000-4 Veszprém 2013 Pannon Egyetem – Környezetmérnöki Intézet http://mkweb.uni-pannon.hu/tudastar/anyagok/33-Katasztrofa.pdf (letöltés dátuma: 2015.10.16.)

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Pál Angéla
palangelaviri@gmail.com

A KOMMUNÁLIS HULLADÉKOK KÖRNYEZETI HATÁSAI, A HULLADÉKGAZDÁLKODÁS, MINT ELLENHATÁS

Absztrakt

Korunkban a keletkező kommunális hulladékok egyre növekvő mennyisége, összetételének szélesedő skálája, hatásaival komoly veszélyt jelent élő és élettelen környezetünk számára, társadalmunk egészségi állapotára. Megfelelő, környezet- és biztonságtudatos kezelése ezért létszükséglet. A környezetkímélő hulladékgazdálkodás stratégiájával megvalósítható a hulladékokanyagok mennyiségének csökkentése, azok újrahasznosítása, energetikai értékesítése, vagy környezetbarát módon történő ártalmatlanítása.

In our modern times, nowadays the volume of generated communal waste is higher from day to day, their composition is constantly expanding. Environmental impacts of waste are dangerous for the animate and inanimate nature and for the health of human society. Environmentally responsible and safe waste handling is a requirement for the life. With the strategy of environmental waste management program is possible to reduce the amount of waste, to utilize in its material, to regain its energy, or it is possible to disposal the waste with environmental friendly methods.

Kulcsszavak: *kommunális hulladék, biztonságos hulladékkezelés, környezetkímélő hulladékgazdálkodás, stratégia, újrahasznosítás, újrahasználat, ártalmatlanítás ~ communal waste, safe waste management, environmental friendly waste management, strategy, recycling, disposal*

BEVEZETÉS

A környezeti problémák okai legtöbbször visszavezethetők azokra a téves feltételezésekre, miszerint a természet kiapadhatatlan energiaforrásokkal rendelkezik, a gazdasági növekedés folyamatosan kikényszeríthető, a technikai fejlődés végtelen lehetőségekkel bír, és képes válságok kezelésére.

Azonban minél sürgetőbbé válik természeti értékeink, erőforrásaink megóvása, annál nyilvánvalóbbá lesz, hogy környezetünkhöz való viszonyunkat, gazdasági céljainkat át kell értékelnünk. A korlátlan növekedés és fogyasztás célja helyett, a természeti környezettel összhangban, a fenntartható fejlődésre kell törekedni.

Ez nem jelenti a szükségletek korlátozott kielégítését, csupán azt, hogy a megelégedést kevesebb energia és anyag felhasználásával, valamint a szennyezés minimalizálásával próbáljuk meg elérni [1].

A jövőben nagyobb hangsúlyt kell tehát fektetni környezetünk védelmére, a környezet és biztonságtudatos hulladékgazdálkodásra, a káros anyagok kibocsátásának mennyiségére, ezáltal a globális felmelegedés csökkentéséhez is hozzájárulunk [2]. A globális felmelegedés káros hatásai – melyek Földünk minden pontján érzékelhetőek – egyre nagyobb intenzitással jelentkeznek, az általuk okozott károk mértéke folyamatosan növekszik [3]. Előbbiek miatt rendkívül fontosnak tartom cikkemben bemutatni a hulladékok környezeti hatásait, fel kívánom hívni a figyelmet a környezetbarát hulladékgazdálkodás előnyeire.

A HULLADÉK FOGALMA

A természeti folyamatokban a hulladék fogalma ismeretlen, azt az emberi tevékenység hozta létre. A természetben nincsen felesleges anyag, káros hulladék, mert amit létrehozott, azt képes elbontani, illetve visszajuttatni saját körforgásába.

„Általános értelemben hulladéknak tekintendő az ember mindennapi élete, munkája, gazdasági tevékenysége során keletkező, a keletkezés helyén feleslegessé váló, ott közvetlenül fel nem használható, különböző minőségű és halmazállapotú anyag, anyag-együttes, termék, maradvány, tárgy, leválasztott szennyező anyag, szennyezett kitermelt föld, amelyet birtokosuk sem felhasználni sem értékesíteni nem tud, és amelynek kezeléséről külön kell gondoskodni” [4].

A hulladék fogalmának igen célratörő meghatározása olvasható a Magyarországon jelenleg hatályos, 2012 évi CLXXXV. törvényben a hulladékokról: Első fejezet 2. pont Értelmező rendelkezések: „23. hulladék: bármely anyag vagy tárgy, amelytől birtokosa megválik, megválni szándékozik vagy megválni köteles” [5].

A HULLADÉKOK CSOPORTOSÍTÁSI LEHETŐSÉGEI

A hulladékok csoportosításának egységesítésére számos törekvés található, ezek megnyilvánulási formája az ún. hulladék-katalógus. (Ilyen nemzetközileg alkalmazott például az OECD, EU katalógus, vagy a német Abfallkatalog) A hulladék-katalógusok többségénél a „párhuzamossági átfedési” elv érvényesül, vagyis egy hulladékfajtát egyidejűleg több csoportosítási szempont tesz azonosíthatóvá [13]. Ezek többségében a következők:

- hulladék azonosító kód (egységes informatikai feldolgozás miatt),
- hulladék eredet (kibocsátó „forrás”) meghatározása,
- anyagi tulajdonságok,
- kezelhetőség.

E csoportokon belül a hulladékok környezetre és az emberi egészségre gyakorolt hatása szerint megkülönböztetünk [6]:

- *veszélyes,*
- *nem veszélyes* hulladékokat.

Veszélyes hulladéknak tekintjük azt az anyagot (anyagmaradványt) amely:

- önmaga vagy bármelyik bomlásterméke,
- közvetlenül vagy közvetve,
- azonnal vagy késleltetetten az emberi életre, egészségre illetve az élővilágra, környezetre károsító hatást fejthet ki.

A veszélyesség jellege szerint a hulladékfajták a következő hatásokat válthatják ki:

- mérgezés (toxikus hatás),
- fertőzés,
- tűz-és robbanás okozta hatások,
- mutagenitás (karcinogén hatás),
- korrozivitás,
- ionizáló hatás.

A 2012 évi CLXXXV. törvény a hulladékról kimondja, hogy veszélyes hulladéknak számít mindazon anyag, amely rendelkezik ugyanezen törvény 1. számú mellékletében felsorolt tulajdonságok valamelyikével. Veszélyes hulladék származhat kommunális és termelés

A HULLADÉK-KELETKZÉS NÖVEKEDÉSÉNEK LEHETSÉGES OKAI [7]

A hulladékok keletkezésének lehetséges okait több szempontból is lehet vizsgálni, véleményem szerint a következő tényezők nagymértékben befolyásolják, a keletkező hulladékmennyiségeket:

- Profitorientált korunkban nagyobb az előállított termékmennyiség, ezért több melléktermék, selejt, hulladék keletkezik.
- A fogyasztói társadalom szükséglete a folyamatos vásárlás, ezért több maradék, szemét, csomagolóanyag kerül a hulladéktárolókba.
- A folyamatos gazdasági növekedési kényszer miatt egyre korszerűsödnek a termelő eszközök, ezért a még el nem használt gépek is a hulladéktemetőbe kerülnek.
- Gyorsan változik a divat a fogyasztásban, ezért a használati tárgyakat elhasználódás előtt selejtezik.

A HULLADÉKOK OKOZTA KÖRNYEZETI HATÁSOK

A természetbe került hulladékok hatása hosszú időn keresztül nem haladta meg a környezet tűrőképességét, mivel a korabeli hulladékok összetétele hasonló volt a természetes körfolyamatokban meglévő anyagokéhoz, mennyiségük is a feldolgozható tömeg határán belül mozgott, ilyen formán különösebb zavart nem okoztak.

Korunkra, azonban az emberi tevékenységből keletkező hulladékok mennyiségében és összetételében is jelentősen megváltoztak. A környezetbarát alapanyagokat felváltották az idegen, szintetikus anyagok, melyek könnyebb, olcsóbb előállíthatóságuk miatt vonzóak az profitéhes világ számára.

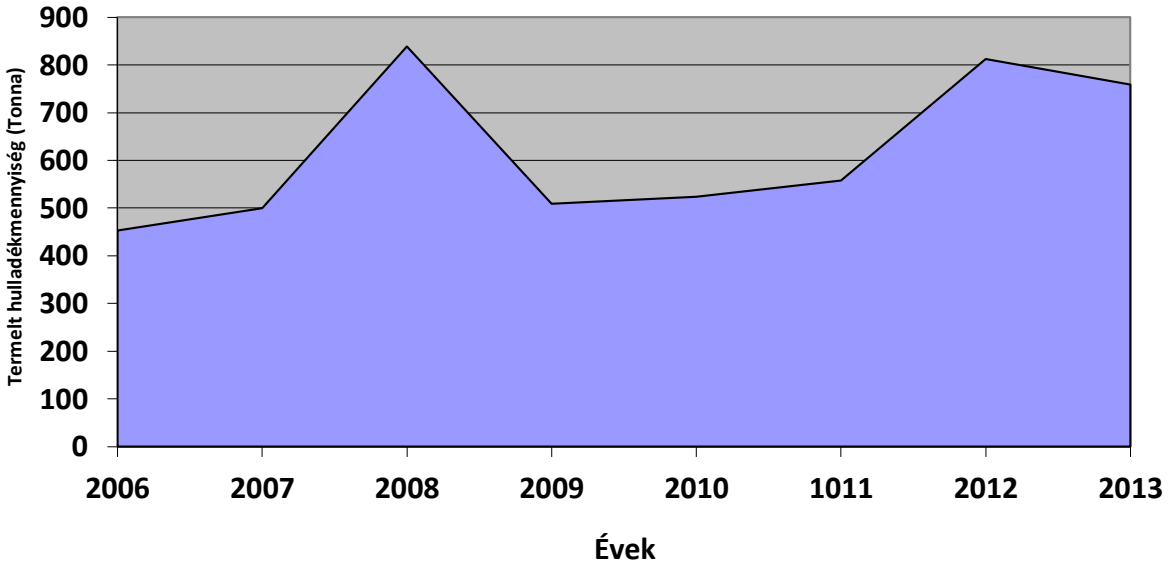
Hosszú, esetenként több száz évet igénybe vevő bomlási idejük miatt azonban előrevetíthető szeméthegyekben való felhalmozódásuk, szennyező hatásuk.

A következő táblázat mindennapi életünk során elhasznált, majd a szemétbe került anyagok bomlási idejét mutatja be.

Hulladékanyag:	Bomlási idő a talajban:	Bomlási idő tengervízben:
Rágógumi	5 év	5 év
Alumínium	10-100 év	500 év
Polisztirol	≥1000 év	100 – 1000 év
Telefon kártya	≥100 év	1000 év
Cigaretta vég	1-2 év	2 – 5 év
Alma héj	3 hónap	3 – 6 hónap
Gyufa	6 hónap	6 hónap
Újságpapír	6 hónap – 10 év	2 hónap
Üveg	≥400 év	1000 év
Műanyag táska	100 – 1000 év	1000 év
Eldobható pelenka	≥400 év	200

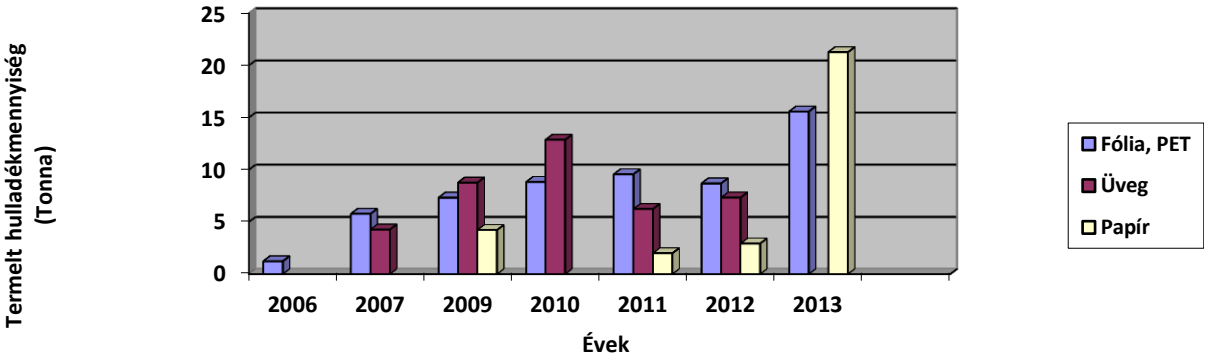
1. táblázat: A kommunális hulladék anyagok lebomlási ideje földben és tengervízben, (Forrás: szerző összeállítása [8] adatai alapján)

A következő ábrán a kevert kommunális hulladék mennyiségnek alakulása figyelhető meg, egy vizsgált településen, a szlovákiai Bátorkeszin 2006-tól, 2013-ig.



1. ábra: A kevert kommunális hulladék mennyisége Bátorkeszin 2006-tól, 2013-ig,
(Forrás: Szerző összeállítása [10] adatai alapján)

A következő ábrán az előbbiekben is vizsgált településen keletkezett fólia, üveg és papír hulladékok mennyiségének alakulása látható 2006-tól 2013-ig.



2. ábra: A vizsgált településen keletkező fólia, üveg és papír hulladék mennyiségének változása 2006-tól 2013-ig, (Forrás: Szerző összeállítása [10] adatai alapján)

A hulladékok egy része műszaki, vagy gazdasági okok miatt, illetve emberi mulasztásból eredően a környezetbe, illetve védett környezeti közegbe kerül, ott kifejtve káros hatásait.

A legtöbb szennyezési problémát:

- a rendezetlen elhelyezés (pl. „a hagyományos" szeméttelepek),
- helytelenül megválasztott hulladékkezelés,
- vagy a gondatlan fogyasztói magatartás okozza.

A szennyezés kiterjed a környezeti elemekre, ezáltal nagy népességet érint, és a hatása sok esetben, időben elhúzódó. A hulladékok egyes alkotórészei beépülnek a növényi, állati szervezetekbe, és a táplálkozási láncon keresztül is károsítják az élőlényeket, a környezetre káros, mérgező hatású anyagok bioakkumulációja és toxicitása révén. A települési és egyes termelési hulladékok fertőző mikroorganizmusai különböző fertőző betegségek okozói lehetnek. A hatékony megelőzési intézkedések kidolgozásának és a környezeti károk csökkentésének érdekében fontosnak tartom a következő környezeti elemekre gyakorolt hatások vizsgálatát:

- Talaj,
- Víz,
- Levegő,
- Élővilág,
- Táj,
- Mesterséges környezet.

A talaj, talajvíz, (felszín alatti vizek) és felszíni vizek szennyeződése

A hulladékoknak leggyakrabban szükségszerű természetes befogadója a talaj. A nem megfelelően kezelt hulladékokat, azok bomlástermékeit a csapadékvíz bemossa a talajba, így az elszennyeződik, majd a szennyező anyagok a csurgalékvízzel bekerülnek a talajvízbe, ahol vízbázisokat veszélyeztetnek.

A kommunális hulladékok anyagi összetétele széles, teljesen nem behatárolható skálán mozog, komponensei önmagukban és egymással új vegyületeket képezve is károsító hatást fejtenek ki a talajok természetes tulajdonságaira, termőképességére, élő flórájuk, faunájuk életfolyamataira. A megfelelő védőrendszer nélkül tárolt háztartási hulladékból tisztítószerek, rovarirtó szerek, gyógyszerek, nehézfémek és egyéb fertőzést okozó anyagmaradványok vegyületei oldódnak ki, és jutnak a termőtalajba, talajvízbe, majd a terményeken keresztül a fogyasztók szervezetébe.

A felszíni vizek közvetett és közvetlen szennyeződését eredményezi a nem megfelelően kezelt kommunális és ipari szennyvizek bevezetése, melyek szintén tartalmazhatnak méreganyagokat, detergenseket, nehézfémeket, kórokozó mikroorganizmusokat. Esetenként a káresemények, veszélyes anyag balesetek során szennyezett felszíni természetes víztömegek és csapadékvizek is szennyezhetik vízbázisainkat [9].

A levegő szennyeződése

A szervesanyag-tartalmú hulladék bomlása során jellegzetes bűzös gázok keletkeznek (ammónia, hidrogén-szulfid stb.), a kezelés nélküli hulladékhalmok finom porát, illetve nagyobb darabjait a szél, vagy kisebb légmozgás is a levegőbe emeli. Jelentős a hulladéklerakók üvegházhatást növelő metán- és szén-dioxid kibocsátása. A hulladéklerakókon öngyulladás miatt vagy a hulladékok nyílt téri – tiltott - égetésekor keletkező égéstermékek (füstgáz, korom, pernye) közvetlenül szennyezik a levegőt [11].

A növények égése során nagy mennyiségű szén-dioxid keletkezik, amely gyorsítja a globális felmelegedést. Égéstermék a szén-monoxid is, amely a vörös vértestek oxigén szállítását akadályozza. Amennyiben az égés zöld területekre is átterjed, további mérgező gázok kerülnek a levegőbe. A tűz által gerjesztett gázcsere következtében az égéstermékek belekerülnek a magasabb légmozgásokba, amelyek a tűztől akár 10-20 km távolságra is elszállítják az égéstermékeket, ahol kihullva kifejtik szennyező hatásukat. A kommunális hulladékokban nemcsak szerves anyagok égnek, hanem különféle műanyag származékok, gumitermékek is. Az égés során ezeknél a tüzeknél is keletkezik szén-monoxid és szén-dioxid, viszont a műanyag és gumitermékek tüzeinél nagymennyiségű toxikus gáz és korom is képződik. Jelentős a hulladéklerakók üvegházhatást növelő metán- és szén-dioxid-kibocsátása [12].

Az élővilág károsodása

A települési hulladékok kórokozó mikroorganizmusai különböző fertőző betegségek előidézői lehetnek (vírusok, baktériumok, féregpeték stb.). Megfelelő körülmények között a kórokozók a hulladékban hosszabb ideig életképesek maradnak, onnan a talajba, a vízbe kerülhetnek és közvetlen érintkezés útján is fertőzést okozhatnak.

A nem megfelelően végzett települési hulladékkezelés következtében a rovarok (legyek) és rágcsálók (patkány, egér) nagymértékben elszaporodhatnak, melyek közvetítői egyes fertőző betegségek terjedésének. Károkozásuk mezőgazdasági termények fogyasztásában, minőségük rontásában is megjelenik.

A növényzet károsodása a hulladékokból származó természetidegen vegyületek, nehézfémek, növényvédő szerek, herbicidek, egyéb mérgező anyagok talajból, talajvízből való felvétele után, életfolyamataik romlásában, vagy azok megszűnésében nyilvánul meg.

A táj, az épített környezet károsodása

A nem megfelelő hulladékkezelés, a rendezetlen, szétszórt hulladék látványa tönkreteszi a táj eredeti szépségét, amellyel csökkenti a pihenés, rekreáció lehetőségét. A hulladékok korrozív, maró hatású összetevői lebontják az épített környezeti elemek alapanyagát [13].

HULLADÉKGAZDÁLKODÁS A KÖRNYEZETVÉDELEMÉRT

A hulladékgazdálkodás a környezetvédelem fontos szakterülete. Kulcsszerepe van a környezeti elemek (víz, föld, levegő, élővilág, táj, épített környezet) minőségének megőrzésében, és a természeti erőforrások védelmében.

A hulladékgazdálkodás lényege a hulladékokkal való zárt körforgalmú anyaggazdálkodás, vagyis a hulladékok összetevőinek a termelési-fogyasztási folyamatba való visszaforgatása. Ezzel biztosítva a természeti erőforrások kímélését, és az ártalmatlanítandó hulladék mennyiségének csökkentését, a termelési-fogyasztási folyamatok korlátozása nélkül.

A hulladékgazdálkodás stratégiai elemei [13]

A környezetkímélő hulladékgazdálkodás az alábbi, egymásra épülő stratégiai elemekből áll:

1. A hulladékkeletkezés megelőzése, illetve a keletkező hulladékok mennyiségének és veszélyességének csökkentése:
   - az anyag- és energiatakarékos, hulladékszegény technológiák alkalmazásával,
   - az anyagnak, illetve a hulladéknak a termelési-fogyasztási körfolyamatban tartásával,
   - a legkisebb tömegű és veszélyességű hulladékot eredményező termékek előállításával,
   - a hulladékként kockázatot jelentő anyagok kiváltásával,
2. A keletkező hulladékok másodnyersanyagként vagy energiahordozóként történő hasznosítása:
   - Az a tevékenység, amelynek során az eredeti rendeltetésük szerint tovább nem használható anyagokat, termékeket közvetlenül – átalakítás nélkül-, vagy közvetve – átalakítást követően-, a termelési vagy szolgáltatási folyamatba visszavezetik
   - Hasznosítást követően a hulladék másodnyersanyagként, energiahordozóként, vagy mint félkész-, illetve késztermék kerül vissza a gazdasági folyamatba, fontos, hogy a hulladék hasznosítható anyag-, illetve energiatartalma minél nagyobb hatásfokkal, a lehető legegyszerűbb módszerekkel és elviselhető anyagi ráfordításokkal legyen kinyerhető.
3. A nem hasznosítható hulladékok környezetvédelmi követelményeket kielégítő ártalmatlanítása:
   - A hulladékártalmatlanítás a hulladék anyagi minőségének megváltoztatása – különböző kémiai, termikus és biológiai kezelési eljárások segítségével, ezek rendszerint valamilyen hasznosítási elemet is tartalmaznak, pl. hőhasznosítás hulladékégetésnél -, illetve a hulladéknak a környezettől való elszigetelése, mely megakadályozza a környezetszennyezést.
   - Ártalmatlanításra csak az a hulladék kerülhet, amelynek anyagában történő hasznosítására, energiaforrásként történő felhasználására a műszaki vagy gazdasági lehetőségek nem adottak, vagy a hasznosítás költségei az ártalmatlanítás finanszírozásához képest aránytalanul magasak.
   - A hulladéklerakás az anyagi minőség megváltoztatásával nem járó, a környezet elemeitől való elszigetelésen alapuló ártalmatlanítási eljárás. Célja a hulladék és a környezet kölcsönhatásának megakadályozása, amely a talajban vagy a talaj felszíne felett rendezett lerakás formájában valósítható meg.

A KOMMUNÁLIS HULLADÉKKEZELÉS KÖRNYEZETI HATÁSAI

Kommunális hulladékok alatt a lakosság körében keletkező vegyes összetételű hulladékokat értjük, ezek kezelésével kapcsolatos tevékenységek a következők:

- Gyűjtés,
- Szállítás,
- Tárolás,
- Előkezelés,
- Hasznosítás,
- Ártalmatlanítás,

A hulladékok gyűjtése és szállítása

A hulladékkezelés technológiai folyamatának első fázisa a hulladéknak a keletkezés üteméhez igazodó, szervezett, környezetkímélő összegyűjtése, és készletezése az elszállításig. Két formája használatos:

- Együtemű hulladékgyűjtés:

A hulladék átrakás nélküli mozgatása ugyanazzal a szállító célgéppel, a gyűjtőponttól a hasznosítást vagy ártalmatlanítást végző létesítményig.

- Kétütemű hulladékgyűjtés:

A hulladék mozgatása a hasznosítást, vagy ártalmatlanítást végző létesítményig, átrakodó állomáson való átrakás (esetleg előkezelés) beiktatásával. A szállítási távolságok jelentős növekedése miatt regionális rendszerek kiépítése alakult ki. A kétütemű szállítást leginkább körzeti, regionális kezelőtelepekhez kapcsoltan alkalmazzák a teljesítmények fokozása és a költségek csökkentése érdekében.

Környezeti hatásai:

Pozitív hatásként könyvelhető el, hogy a kommunális hulladékok gyűjtőpontokon való elhelyezése csökkenti azok kioldódó vegyületeinek talajt, talajvizet, felszíni vízfolyásokat szennyező hatásait, csökkenti a felszínükről a levegőbe kerülő por légszennyező hatását, valamint védelmet biztosít a hulladékból táplálkozó állatfajok ellen. A hulladékok rendszeres elszállítása biztosítja a lakott területek tisztán tartását.

Negatív környezeti hatású azonban a fosszilis üzemanyagokkal működő, hulladékszállítást végző gépjárművek kén, nitrogén, ólom, stb. tartalmú kipufogógázainak légszennyezése.

A hulladékok tárolása

A hulladéknak termelője, vagy kezelője által, a környezet veszélyeztetését kizáró módon végzett, a hulladékok három évnél rövidebb ideig tartó elhelyezése. A tároló telep nyílt téri és fedett kivitelben egyaránt kialakítható. Szigetelési rendszerének az alábbi elemeket kell tartalmaznia: szilárd térburkolat, csurgalékvíz elvezetésére szolgáló csatornarendszer, műszaki védelem.

Környezeti hatásai:

A szükséges védelmi berendezések alkalmazásával lehetővé teszi a hulladékok ártalmatlanná tételét a környezeti elemekkel szemben.

A hulladékok előkezelése

A hulladék begyűjtését, tárolását, hasznosítását, ártalmatlanítását elősegítő, azok biztonságát növelő, a környezetterhelést csökkentő tevékenység, amely a hulladék fizikai, kémiai, biológiai tulajdonságainak megváltoztatásával jár.

Eljárásai közé tartoznak: aprítás, tömörítés, rostálás, víztelenítés, méregtelenítés, semlegesítés, fertőtlenítés, komposztálás.

A hulladékok hasznosítása

A hulladékok kezelésének hosszú távú megoldása, melynek során az eredeti rendeltetésük szerint tovább nem használható anyagokat közvetlenül, vagy közvetve a felhasználók igényeinek megfelelő termékké alakítják, és ezzel megszüntetik a hulladék jellegét. A hulladékhasznosítás maradék anyagai további ártalmatlanítást igényelnek. A hulladék anyagok hasznosíthatóak: fűtőanyagként, oldószerek visszanyerésére, olajok újrafinomítása, fémek visszanyerése, papír alapanyagként, térburkolatok alapanyagaként stb.

Környezeti hatásai:

A tevékenység előnyös hatásaként említhető meg, hogy nyersanyagforrásként, csökkenti a kitermelni szükséges alapanyagok mennyiségét, energia megtakarítást jelent, csökkenti az ártalmatlanításra, lerakásra kerülő hulladék mennyiségét.

A hulladékok ártalmatlanítása

A hulladék okozta környezetterhelés csökkentése, a környezetet veszélyeztető, szennyező, károsító hatásának megszüntetése, kizárása – a környezet elemeitől való kizárásával, vagy anyagi minőségének megváltoztatásával. A hulladékok ártalmatlanná tételére, illetve végleges elhelyezésére kidolgozott eljárások, a környezetvédelmi hatóság engedélyéhez kötött tevékenységek:

- Biológiai módszerek,
- Kémiai módszerek,
- Beágyazás,
- Égetés,
- Lerakás.

Biológiai hulladékkezelés

A hulladékok szerves és szervetlen anyagait mikroorganizmusok, illetve azok enzimjei vizes környezetben, aerob és anaerob körülmények közt alakítják át vagy bontják le. Módszerei: komposztálás, biogáz termelés.

Környezeti hatásai:

Csökkenti az ártalmatlanítani, vagy tárolni szükséges hulladék mennyiségét, és visszavezeti a szerves anyagokat a biológiai energia-körforgás rendszerébe.

Negatívumként említhető meg a kénvegyületeknek, mint bűzanyagoknak a megjelenése. A kénvegyületek korrozív hatásai miatt a depónia gáz közvetlen nem hasznosítható, e vegyületek eltávolítása előzetes kémiai eljárást igényel [11].

Kémiai hulladékkezelés

Célja lehet ártalmatlanítás, vagy hasznosítás, de lehet bizonyos veszélyes komponens mennyiségének, koncentrációjának, veszélyességének csökkentése is. Módszerei: csapadékos leválasztás, hidrolízis, redukció, oxidáció, dehalogénezés, elektrokémiai módszerek, sugárkémiai reakciók.

Környezeti hatása:

A kémiai anyagok megjelenése a folyamatokban, a károsító hatások kifejtését meggátoló, különleges környezetvédelmi intézkedéseket, valamint költséges technológiai berendezések alkalmazását igényli.

Beágyazás

Más néven szilárdítás, vagy solodifikáció. Olyan hulladékkezelési eljárás, melyben a folyadékot, iszapot és más veszélyes hulladékot vázképző anyagokkal összekeverve mechanikailag és kémiailag stabil, szilárd anyagokká alakítjuk, melyben a mérgező hulladékkomponensek kioldódó képessége lényegesen kisebb.

Környezeti hatásai:

A szennyező anyagok halmazállapotának megváltoztatásával, azok kezelhetőségének, elhelyezésének megkönnyebbítése, ezáltal a káros környezeti hatásaik csökkentése.

Negatívuma, hogy a szilárdított káros anyagok környezetben való ártalommentes elhelyezése nem minden esetben megoldható.

Égetés

Minősülhet ártalmatlanításnak, de hasznosításnak is, lényege a hulladék összetevőinek hőenergia közlésével való megváltoztatása. Az égési folyamat végeredményeként a képződő égéstermékek az eredeti hulladéktól teljesen eltérő tulajdonságúak lesznek, melyek könnyebben kezelhetőek.

Környezeti hatásai:

Az égetéssel a hulladékok jelentős térfogatcsökkenését érhetjük el, higiénikus eljárás, a keletkező hőenergia hasznosítható, megfelelő füstgáztisztítással a környezetre kevésbé veszélyes, mint a lerakásos ártalmatlanítás.

Negatív hatásként a korszerűtlen égetőművek jelentős mértékű szennyezőanyag kibocsátása említhető meg. Kén-dioxid, kén-trioxid, szén-monoxid, nitrogén-oxidok, kloridok, fluoridok, nehézfémek, arzén kerülnek a légkörbe. Az égetés termékeit – salak, hamu, pernye, füstgázmosó szennyvíz, mosóvíz tisztítási iszap - is ártalmatlanítani, vagy a környezet elemeitől elszigetelve lerakni szükséges [14].

Lerakás

A települési szilárd hulladékok ártalmatlanítására a leggyakrabban alkalmazott eljárás a talajon, terepmélyedésekben történő lerakás. Az Európai Unió hulladékgazdálkodási prioritási sorrendjében az utolsó helyen áll. Európában átlagosan 63%-os a lerakás aránya.

A rendezett hulladéklerakónak ki kell zárnia a talaj- és talajvízszennyezést, csak olyan hulladékot szabad elhelyezni a területén, melynek káros hatásai ellen az képes megfelelő védelmet nyújtani. Hosszú távú védelmet kell nyújtania a tárolt anyagok szennyező hatása ellen, lehetővé kell tennie, hogy az elkerülhetetlen bűz, kiporzás és levegőszennyezés, kedvezőtlen esztétikai hatása minimális legyen.

A hulladéklerakót sem használata alatt, sem lezárása után nem szabad ellenőrizetlenül hagyni. Lezárása után meg kell oldani a terület optimális hasznosítását és tájba illesztését.

Környezeti hatásai:

A megfelelően kialakított, szükséges védőrendszerrel ellátott hulladéklerakó telepen a környezeti elemektől elzártan helyezhető el a kommunális hulladék.

Negatív hatása, hogy nagy területet foglal el a természeti környezetből, megváltoztatva a táj eredeti képét, légszennyezést, esetenként talaj- és vízszennyezést, kártevők elszaporodását okozhatja [15].

ÖSSZEGZÉS

Az emberi tevékenység bármely területén keletkező hulladékok káros környezeti hatásainak felismerése óta a vonatkozó jogi szabályozások folyamatos fejlesztése, nemzetközi összefogás mellet is tapasztalható, hogy a termelődő kommunális hulladék komoly problémát jelent globális szinten.

Mennyisége folyamatosan nő, helytelen kezelésének hatásai egyre szélesebb körökben mutatkoznak meg.

Élő és élettelen környezetünket, saját egészségünket a hulladékgazdálkodás eszközrendszerével, stratégiájával védhetjük meg a hulladékok káros hatásai ellen. A hulladékgazdálkodás védő, megelőző tevékenységek összehangolt sorozata. Gyakorlatilag a hulladékok keletkezésének megelőzését, mennyiségének csökkentését, a keletkezett hulladékok elkülönített gyűjtését és hasznosítását, a nem hasznosítható hulladékok környezetszennyezés nélküli átmeneti tárolását és ártalmatlanítását foglalja magában.

Felhasznált irodalom

[1] Janklovics Ildikó: A fenntartható fejlődés: a települési szilárd hulladékkezelés az Európai Unióban, Magyarországon és a budapesti Erzsébetvárosban, Budapesti gazdasági Főiskola, Külkereskedelmi, Főiskolai Kar, Nemzetközi Kommunikáció szak.

[2] Rajmund KUTI - László FÖLDI: Extreme weather phenomena, improvement of preparedness, Hadmérnök on-line, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar és a Katonai Műszaki Doktori Iskola on-line tudományos folyóirata, VII. Évfolyam 3. szám, 60-65. o. 2012. szeptember. ISSN 1788 1919. URL cím: http://hadmernok.hu/2012_3_kuti_foldi.pdf (Letöltés ideje: 2016. 01. 21.)

[3] Rajmund KUTI – László FÖLDI: Extreme weather phenomena 2. The Process of Remediation, Hadmérnök on-line, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar és a Katonai Műszaki Doktori Iskola on-line tudományos folyóirata, IX. Évfolyam 2. szám, 250-256. o. 2014. július. ISSN 1788 1919. URL cím: http://hadmernok.hu/142_23_foldil_kr.pdf (Letöltés ideje: 2016. 01. 21.)

[4] Dr. Nagy Géza, Kovács Barnabás, Buruzs Adrienn, Dr. Torma András, Vagdalt László, Horváth László: Hulladékgazdálkodás, 1. fejezet - Hulladékok fogalma, fajtái, környezeti hatásai, http://www.tankonyvtar.hu/hu/tartalom/tamop425/0021_Hulladekgazdalkodas/ch01.html (Letöltés ideje: 2016. január 21.)

[5] 2012. évi CLXXXV. törvény a hulladékokról: I. Fejezet, Általános rendelkezések, 2. Értelmező rendelkezések

[6] Dr. Barótfi István: Környezettechnika. Mezőgazda Kiadó http://www.tankonyvtar.hu/hu/tartalom/tkt/kornyezettechnika-eloszo/ch06s02.html (Letöltés ideje: 2016. 01. 21.)

[7] Dr. Várkonyi Tibor: Hulladék a családi házban http://www.kvvm.hu/szakmai/hulladekgazd/oktatas/csaladihaz/kiadvany.htm (Letöltés ideje: 2016. 01. 21.)

[8] http://www.legambienteonline.it (Letöltés ideje:2016. január 21.)

[9] Nagy Zsolt – Kuti Rajmund: A tűzoltóhabok környezetre gyakorolt hatásai, Hadmérnök on-line, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar és a Katonai Műszaki Doktori Iskola on-line tudományos

folyóirata, X. Évfolyam 3. szám, 156-164. o. 2015. ISSN 1788 1919. URL cím: http://www.hadmernok.hu/153_12_nagyzs_kr.pdf (Letöltés ideje: 2016. 01. 21.)

[10] Ing. Bárczy Tibor: Program Odpadového Hospodárstva Obce Bátorove Kosihy do Roku 2015

[11] Földi László, Kuti Rajmund: Characteristics of Forest Fires and their Impact on the Environment, ACADEMIC AND APPLIED RESEARCH IN PUBLIC MANAGEMENT SCIENCE 15: (1), ISSN 2498-5392, http://uni-nke.hu/uploads/media_items/aarms-vol-15_-issue-1_-2016.original.pdf (Letöltés ideje: 2016.04.02.)

[12] Kuti Rajmund – Zólyomi Géza: Vegyes tüzelésű fűtőberendezések használatának kockázatai, VÉDELEM ONLINE: TŰZ- ÉS KATASZTRÓFAVÉDELMI SZAKKÖNYVTÁR (2016) pp. 1-7. (2016), http://www.vedelem.hu/letoltes/anyagok/741-vegyes-tuzelesu-futoberendezesek-hasznalatanak-kockazatai.pdf (Letöltés ideje: 2016.01.21.)

[13] Dr. Nagy Géza, Dr. Bulla Miklós, Dr. Hornyák Margit, Vagdalt László (2002): Hulladékgazdálkodás. Széchenyi István Egyetem, Környezetmérnöki Tanszék, egyetemi jegyzet, Győr. http://www.sze.hu/~nagyg/hulladekgazd.pdf (Letöltés ideje: 2016.01.21.)

[14] Környezetvédelmi és Vízügyi Minisztérium, Hulladékgazdálkodási és Környezettechnológiai Főosztály, (2002). A hulladékgazdálkodás általános kérdései, alapelvei. Köztisztasági Egyesülés munkacsoportja, Budapest, 2002. július http://www.kvvm.hu/szakmai/hulladekgazd/szakmaifuzet1.htm#1_5 (Letöltés ideje: 2016.01.21.)

[15] Zimler Tamás (szerkesztő) (2003): Hulladékgazdálkodás, Tertia Kiadó, Budapest

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Teknős László – Kóródi Gyula
teknos.laszlo@uni-nke.hu – korodi.gyula@uni-nke.hu

A VÍZZEL KAPCSOLATOS VESZÉLYEZTETETTSÉG ÉGHAJLATVÁLTOZÁSSAL KAPCSOLATOS ASPEKTUSAINAK KATASZTRÓFAVÉDELMI SZEMPONTÚ ELEMZÉSE ÉS KIÉRTÉKELÉSE I.

Absztrakt

Az éghajlat jelenlegi (rohamléptű) változásának üteme számos kihívást jelent a társadalmaknak. A klíma módosulása az egyik legvitatottabb és legtöbbet kutatott környezetbiztonsági, gazdasági, társadalmi témaköre a tudományos szimpóziumoknak. Ennek értelmében a szerző kísérletet tesz arra, hogy az éghajlatváltozás okozta, a vízzel kapcsolatos fenyegetések elleni küzdelemben javaslatokat, ajánlásokat tegyen, a hazai hidrológiai sajátosságokat a megfigyelt változások alapján - a jelenlegi reagáló képességét - értékelje, a lehetséges prognózisokat figyelembe véve kijelölje a hivatásos katasztrófavédelmi szervezet valószínűsíthető jövőbeni feladatait.

The present (accelerating) pace of climate change poses several challenges to societies, thus it is one of the most debated and studied environmental, economic and social topic of scientific symposiums. In the light of this, the author attempts to make recommendations on the fight against water-related hazards caused by climate change, to evaluate the hydrological characteristics of Hungary – and response skills – based on changes observed as well as to assign potential future tasks for disaster management in view of probable future projections.

Kulcsszavak: *globális éghajlatváltozás, csapadékkal kapcsolatos szélsőségek, árvíz-belvíz, katasztrófavédelem, hatósági feladatok ~ global climate change, extreme precipitation, fluvial and pluvial flooding, disaster management, authority tasks*

BEVEZETÉS

A Föld olyan egyértelmű globális mértékű veszélyes anomáliákat jelez (szélsőséges időjárás, árvizek, hideg-meleg rekordok, egyéb természeti katasztrófák, stb.) amelyek nagymértékben már most hatással vannak a környezetre és többek között a lakosságra is.[1] A hazai időjárást vizsgálva nem új keletű a rendkívüliség, a szélsőségesség. Ami viszont gondolkodásra, cselekvésre késztet, hogy az utóbbi 10-15 évben az évszázados meteorológiai és vízállási rekordok mind megdőlnek. Az ezeket alátámasztó (kár)események azonban nem csak számukat, hanem természetüket, jellegüket és kárterületüket tekintve is megváltoztak, térben és időben „hirtelen" és komplexen érkeznek.

Jelen írásmű kutatási vezérfonala az éghajlat változásából adódó negatív hatások vizsgálata, kiemelten a csapadék hullásának intenzitásával, mennyiségével kapcsolatos kérdésekre vonatkoztatva. Egyik legfontosabb célja a műnek a klímaváltozás vizekre gyakorolt hatásainak és a vízzel kapcsolatos lakossági és anyagi javak veszélyeztetettségének katasztrófavédelmi szempontú elemzése, a megfigyelt hatások értékelése.

A szerző jelen cikkében kísérletet tesz arra, hogy ismertesse, a rendkívüli időjárás és a globális éghajlatváltozás kapcsolódási pontjait, keresi, hogy mik lehetnek azok a veszélyességi faktorok, amelyek alapján a védekezési potenciált átalakítani, fejleszteni szükséges. Továbbá elemzésre kerülnek egy-egy káresemény kapcsán a rendkívüli időjárás okozta kárterületeken jelentkező teendők, és az egységessé vált katasztrófavédelem (2012) óta hatályos jogszabályi keretek között fellépő, szükségszerű katasztrófavédelmi feladatok.

A cikk terjedelmi okokból nem tér ki az éghajlatváltozás széleskörű, kiterjedt elemzésére, a vízgazdálkodás teljes értékű elemzésére, a hidrológiai események esettanulmányként történő bemutatására, de törekszik összefoglaló képet adni a vízzel kapcsolatos veszélyeztetettség éghajlatváltozással kapcsolatos aspektusairól, kiemelten a katasztrófavédelem értékelési szempontrendszerére vonatkoztatva.

MAGYARORSZÁG ÉGHAJLATI ÉS HIDROLÓGIAI ELEMZÉSE

A globális klímaváltozásnak két tábora van. Az egyik tábor szerint a mostani klímaváltozás is természetes eredetű, így azt befolyásolni „emberileg" nem lehet. A másik tábor pedig a mostani klímaváltozásban a természetes ciklikusság mellett az emberi beavatkozó szerepet is látja.[2] A földtörténet során a melegebb (interglaciális) és hidegebb (glaciális) időszakok ciklikusan váltották egymást, amelyek között a Földünk átlagos hőmérséklete több °C -ot is változott. Ezeket a geokémiai kutatások támasztják alá.[3] Amióta létezik a Föld, éghajlata folyamatosan változik, hol gyorsabban, máskor pedig lassabban. Az iparosodás időszaka óta (1750-től) viszont, de különösen az elmúlt évtizedektől azonban eddig sosem tapasztalt tempóban melegszik. Az üvegházhatás természetes jelenség, ami lehetővé teszi az élet jelenlétét a Földön azáltal, hogy 33 °C-kal növeli a globális átlaghőmérsékletet (jelenleg + 15 °C). Ha nem lenne üvegházhatás, akkor Földünkön -18 °C lenne. De az antropogén tevékenységek hatására (főleg a 20. században) az üvegházgázok koncentrációja jelentősen megemelkedett. A mind gyakoribbá váló forró, aszályos nyarak és enyhe telek, a világszerte tapasztalt rendkívüli időjárási események egy globális mértékű veszélyes folyamat tünetei. A klíma változása valószínűleg az emberiség egyik legnagyobb kihívása a 21. században. Az éghajlat változása tény, sőt az is egyre nagyobb valószínűséget kap, hogy a felmelegedés üteméért az antropogén eredetű, a légkörben feldúsuló üvegházhatású gázok a felelősek. Az Európai Bizottság a 2007. 06. 29-én Brüsszelben kiadott Zöld Könyvében elismeri, hogy a globális klímaváltozás káros hatásai gyorsan és veszélyes mértékben erősödnek. Az Éghajlatváltozási Kormányközi Testület szintetizálja az éghajlattal kapcsolatos új

tudományos eredményeket, és összefoglaló jelentéseket publikál. Öt Helyzetértékelő Jelentést adott ki (1990, 1996, 2001, 2007, 2013), melyek összefoglalják a globális klímaváltozással kapcsolatos legfontosabb és legújabb nemzetközi kutatási eredményeket. Mindegyik jelentés az emberi tevékenységet feltételezi az éghajlatváltozás ütemének gyorsulása mögött, a vizsgálati módszerek és a technológia fejlődése alapján a jelentések egyre pontosabb képet adnak a jelenlegi tendenciákról.

Nagy Rudolf egyik cikkében azt írja, hogy az emberiség környezetalakító tevékenysége az utóbbi évtizedekben egyre jobban érvényesül.[4] Szerinte a fő probléma az emberiség energiaigénye és annak kielégítése miatt van, mivel az energiaszükséglet biztosításának folyamatában számos légkört szennyező anyag kerül kibocsátásra, amelyek között számos üvegházhatású gáz szerepel. Az üvegházhatású gázok pedig az üvegházhatást erősítik, ami a Föld melegedéséhez vezet, és az éghajlat módosul. Mika János éghajlatkutató szerint két hibát kellene elkövetni ahhoz, hogy azt lehessen mondani, hogy nem az ember okozza a jelenlegi változásokat: az egyik, ha túlbecsülik az üvegházhatású gázok éghajlat módosító szerepét, illetve a másik, hogy valami mégis okozza a változást, amiről nem vettek tudomást. Az Éghajlatváltozási Kormányközi Testület (Intergovernmental Panel on Climate Change - IPCC) becslése szerint 90 %, hogy az antropogén tevékenységek hozzájárulnak az éghajlat változásához.[5]

A globális éghajlatváltozás és a rendkívüli időjárás kapcsolata

A huszadik század óta a földön már kb. 0,76 fokot emelkedett az átlaghőmérséklet, ami hozzájárult ahhoz, hogy a természeti eredetű katasztrófák megszaporodjanak (ami végső soron a civilizációs eredetű ártalmak kialakulását vagy felerősödését eredményezik / okozzák).

A változásokat indikátorok (meteorológiai,- környezeti,- ökológiai,- egészségügyi, hidrológiai, társadalmi-gazdasági) segítségével lehet nyomon követni. [6] Az indikátorok és mérési eredmények alapján nagy bizonyossággal lehet kijelenteni, Magyarország hőmérsékleti értékeinek növekedése követi a Föld hőmérséklet emelkedésének tendenciáját. Az 1970-es évektől kezdve egy erőteljesebb melegedési ütem tapasztalható, ami az utóbbi 10-12 évben még nagyobb intenzitást mutat.[7] A csapadék tekintetében az évszázados trendekhez képest elmozdulás van (egy adott térségben lehulló csapadék teljes mennyiségét, intenzitását, eloszlását figyelembe véve). Ami megfigyelhető, hogy a meteorológiai eseményekhez köthető anomáliák (és az abból lekövethető hidrológiai eredetű események) száma az utóbbi években megszaporodott. Világban tapasztalt éghajlati szélsőségek példátlan (pusztító) hatásúak voltak a 2001-2010-es évtizedben. A Meteorológiai Világszervezet (World Meteorological Organisation - WMO) 2013. júliusi jelentése szerint 1971 és 2010 között (vizsgált időszak) a globális hőmérséklet növekedési mértéke felgyorsult. A 2001-2010-es évtized átlaghőmérséklete 0,14°C-kal magasabb az 1981-1990-es átlagnál és 0,21°C-kal melegebb az 1991-2000-és időszakénál. A 139 nemzeti meteorológiai és hidrológiai szolgáltató adatai szerint az évtized folyamán az áradások voltak a leggyakrabban előforduló események, ahol intenzitásnövekedést lehetett tapasztalni. 2001-2010-es évtized során több mint 370 000 ember halt meg rendkívüli időjárási és éghajlati körülmények, többek között hőhullámok (Magyarországon főként a 2003-as és 2007-es években), hideg idő, aszály, viharok és árvizek miatt. Ez 20%-kal magasabb az 1991-2000-es értéknél. Az elmúlt évtized statisztikái azt mutatják, hogy a természeti katasztrófák több mint 80 %-a meteorológiai vagy hidrológiai eredetű. [8] Másrészről ugyanakkor a veszélynek kitett területek népességének növekedése ellenére az árvizek áldozatainak száma 43%-kal csökkent (az országok fejlettebb meteorológiai

előrejelző rendszerei és a jobban szervezett katasztrófák elleni felkészülések, védekezések miatt).

A Kárpát-medencében a csapadék mennyiségét és a csapadékos napok számát tekintve negatív irányba történik az elmozdulás. A téli hónapokban tapasztalható, hogy a hazai és a külföldi vízgyűjtő-területeken egyre több csapadék hullik le, de a melegedés hatására a hóidény rövidül, így inkább eső, ónos eső formában hullik le a csapadék, ami azt jelenti, hogy a téli lefolyás mértéke nagyobb (kb. 10-20%), ezért az árvízi kockázat esélye magasabb.[9] A Dunántúlon megfigyelhető, hogy a 20 mm-t meghaladó nagy csapadékú (a vízkárelhárítás szempontjából problémát okozó) napok száma növekedett. Az extrém csapadékindex ilyen irányú változása a hazai vízgazdálkodásban (is) komoly problémákat eredményez, mivel az egyenlőtlenebb csapadékeloszlás következtében nyáron például a hidrológiai aszállyal lehet számolni. [9] A VAHAVA jelentésnek (2003-2006), mint a hazai éghajlatváltozás egyik legnagyobb, több tudományterületet összefoglaló kutatásának a válasza az volt a szélsőségekkel kapcsolatban, hogy az erőteljes melegedés miatt a hőmérsékleti,- és csapadékváltozások miatt számos rendkívüli hatással kell számolni, ami az eddiginél gyakoribb és intenzívebb meteorológiai, hidrológiai eredetű (kár)eseményeket idéz elő. [10] A VAHAVA projekt és a Nemzeti Éghajlatváltozási Stratégia a nagyobb és közepes folyóinkon az árvízi szélsőségek megnövekedésével számol. Az előrejelzések szerint az árvízi kártételek 20 %-os növekedése várható a XXI. században, amely már érezhető. Az előrejelzések szerint egyértelmű, hogy a hegy- és dombvidéki kisvízfolyásokon a nagycsapadékos események hatására a gyors levonulású heves árhullámok gyakorisága nőni fog.

Magyarország vízzel kapcsolatos veszélyeztetettségének értékelése katasztrófavédelmi szempontból

Magyarország a mérsékelt övben helyezkedik el a szoláris felosztás szerint. A 45°45' és 48°35' északi szélességek között fekszik a Kárpát-medencében, ami nagyjából az Egyenlítő és az Északi-sark közötti középhelyzetnek felel meg. Magyarország az Északi tengertől, az Uráli hegységtől (szárazföldi, kevesebb csapadékú), a Földközi tengertől (mediterrán, az őszi csendes esőzések és a tél eleji havazások), az Atlanti-óceántól (csapadékosabb, nyáron) szinte azonos távolságra van. Az országban a csekély magasság és szélesség különbség (3^0) miatt azt lehet kijelenteni, hogy az éghajlat egyöntetű, mivel a tengerszint feletti magasság nagyrészt 200 méternél alacsonyabban van és a 400 méternél magasabb területek kevesebb, mint 2%-os arányt érnek el (ez az árvíz és belvíz szempontjából lesz kiemelten fontos információ). A kontinentális légáramlatok nyáron szárazságot és forróságot, télen pedig tartós hideget okoz(hat)nak. Az atlanti-óceáni és a földközi-tengeri párás légáramlatok pedig mérsékelhetik a szélsőséges hőmérsékleti értékeket, ugyanakkor nagy mennyiségű csapadékot is hozhatnak. Ezek a légáramlatok az év bármely időszakában nagy intenzitású és kiterjedt esőzéseket okozhatnak. Ennek következtében bármely folyón és vízgyűjtő területén, heves és tartós árvizekre, valamint belvízre lehet számítani.

Árvizek, belvizek, sodró árhullámok okozta kihívások, környezet terhelése

Magyarországon 22 folyó található, amelyek hossza 2.800 km. Négy kisebb folyó kivételével (Zala, Zagyva, Tarna, Sió) valamennyi folyó forrásvidéke, vízgyűjtőterülete Magyarország határán kívül található. A hazai folyóvízkészletek 75%-át a Duna, Tisza, Dráva, Száva vízfolyások teszik ki, a fennmaradó 25% kisvízfolyásokból származik. [11] A hegyek vízfeleslege a folyóvizeken és a felszín alatti víztartókba beszivárogva jut el a medence belsejébe. A medencébe három oldalról érkeznek vizek, és azok egy irányba távoznak.[12] Magyarország vízviszonyait tekintve a folyóvizek szempontjából átmenő

ország, a kilépő víztömeg 95%-a külföldről érkezik, ezért kitettsége nagy, vízhálózata egyenetlen.

Magyarország földrajzi helyzete alapján megállapítható, hogy árvíz és belvíz szempontjából lavórként működik, hiszen a területeinek 73%-a síkság, 20%-a dombvidék, 7%-a csak a hegyvidék, ezért Európa egyik árvizektől leginkább fenyegetett területének számít (hasonló helyzetű ország csak egyetlen egy van Európában, Hollandia, ahol az árterületes földterület az összterület 20%-a, Magyarországon ez 23%). A domborzati adottságot súlyosbítja az ország éghajlata. Egyrészt a tengeri légáramlatok az év bármely szakaszában, a Duna vízgyűjtőjének bármely területén nagy intenzitású esőzéseket eredményezhetnek, [13] amik nagy árvizeket okozhatnak, másrészt a klímaváltozás miatt egyre gyakrabban kell szélsőséges helyzetekre számítani. A szélsőséges időjárási helyzetek (a nagyintenzitású esőzések) miatt a kisebb vízfolyások is gyakrabban fognak kiönteni, nagyobb árvizeket okozva. Ezek alapján kijelenthető, hogy az egyik „legaktívabb" hidrológiai eredetű katasztrófa típus Magyarországon az árvíz. Árvízről akkor beszélünk (és ekkor okoz problémát), ha a folyó vízszintje olyannyira megemelkedik, hogy a folyó kilép a medréből és a vízzel nem borított földterületek ideiglenesen víz alá kerülnek. Három nagy árvízveszélyes időszak alakulhat ki, úgy, mint a hóolvadásból tavaszi árvíz, jégtorlódásból jeges árvíz és tavaszi vagy nyári esőzésből (zöldár). Országosan a települések 40 %-a erősen, mintegy 80 %-a valamilyen mértékben veszélyeztetett a vizek kártételeitől. [14] Az árterületeken található az ország megművelhető területének egyharmad része, kb. 1,8 millió hektárnyi terület. A hazai vasúthálózat több mint 10 százaléka tartozik árvízveszélyes vonalak közé, [15] a közutak 15 %-a. Mintegy 800 településen 2,5 milliónyi lakos él árvízi fenyegetettségű területen. Ezek az árvíz által veszélyeztetett területek jelentős része az ország legsűrűbben lakott és legértékesebb területei.

Ha kisvízfolyásokra vagy vízgyűjtő területeikre nagy mennyiségű lokális csapadék rövid idő alatt hull le, akkor ún. sodró árhullám (villámárvíz) léphet fel. A rövid idő alatt lehulló nagy intenzitású csapadék mennyisége meghaladja a talaj vízfelvevő képességét, így a felszínen gyorsan megjelenik a lefolyás, és az hirtelen eljut a befogadóba, településre. A villámárvíz hasonló az árvízhez, ugyanakkor az esemény lefolyása sokkal gyorsabb. A nagy esőzéssel az a baj továbbá, hogy a nyáron és ősszel lehullott csapadékvíz a talaj nedvesség-befogadó kapacitását telíti, és ha télen is nagy csapadékmennyiség hull le, akkor ez a vízmennyiség a fagyott talajba nem tud leszivárogni. A következménye hatalmas árvíz lehet. A belvíz, felhőszakadás vagy árvíz folytán felgyülemlett csapadék vagy feltörő talajvíz a termőföldek tönkretételén túl súlyosan veszélyezteti a belvizes területre épült lakóházakat és gazdasági létesítményeket. A belvíz veszélyeztetettség szinte valamennyi ártéri öblözetben (összesen 151 db van, 21.200 km^2-es kiterjedésű ártéren) fekvő települést, községet, várost érint, fenyeget. A belvízzel potenciálisan veszélyeztetett területek nagysága közel eléri a 2 millió hektárt (kb. 18 ezer km^2). Kedvezőtlen időjárási viszonyok között alkalmanként a belvízi elöntések súlyosabb pusztításokat okoztak, mint az árvizek (pl. 1999., 2010-2011.). [16]

Gyakran gyűlik össze egy lejtő tetején hatalmas mennyiségű víz, ami akkora terhet jelent a talaj számára, amit már nem bír el, így földcsuszamlás várható.

Az aszály (tartós csapadékhiány) gyakran előfordul Magyarországon. Aszály idején valószínűbb az erdő és bozóttüzek kialakulása (de az többnyire emberi felelőtlenség, mulasztás következménye), illetve az aszály a mezőgazdasági kultúrákban okoz jelentős károkat. Az elmúlt évtizedben az aszály következtében az okozott károk miatt megalkották az aszálystratégiát, melynek fő alapelvei a megelőzés, az integrálás és az élőhelyekre épülő vízgazdálkodás. [17]

A hazai szélsőséges időjárás, mint kockázati tényező jellemzése az elmúlt évek rendkívüli időjárás által keletkezett káresemények, veszélyhelyzetek alapján

Az időjárási szélsőségek fokozódását az éghajlatváltozás számlájára lehet írni?

Erre így egyértelmű választ nem lehet adni, viszont vannak olyan tények, kutatási eredmények, amik nem zárják ki a klímaváltozást mint az időjárási események extrémebb mértékű befolyásolóját. Magyarország időjárási anomáliáival kapcsolatos rendkívüli esemény mindig található (árvíz, belvíz, özönvízszerű esők, jégesők, hőséghullámok, aszályos periódusok, korai és késői fagyok, hóakadályok, szélviharok, viharok stb.). Hazánk területi jellegéből adódóan az időjárás változékony és nem kizárt a szeszélyes időjárás sem. Van egy sor olyan szélsőség, amely valóban szaporodik, de vannak olyanok is, amelyek csökkennek. Szaporodik például az egy-egy nappal lehulló csapadéknak a mennyisége, de egyértelműen csökken például a nagyon-nagy hidegek (a mínusz 20-25 fokos hidegeknek) a gyakorisága. Egy-egy rendkívüli időjárási esemény, évszak, év alapján nem lehet levonni ilyen irányú következtetéseket. Eredményt akkor lehet elérni, ha pl.: 30 éves időszak átlagát vizsgálják, s a változásokat általában két, harmincéves időszak összehasonlításával fejezik ki. Az, hogy az átlaghőmérséklet a jövőben emelkedni, a nyári átlagcsapadék csökkenni fog, nem jelenti azt, hogy a jövőben ne fordulhatna elő az átlagosnál hűvösebb év, illetve az átlagosnál is csapadékosabb nyár. Egy-egy szélsőséges eseményt úgy kell megvizsgálni, hogy az adott jelenség gyakorisága változott-e a kijelölt referencia-időszakhoz viszonyítva.

Az elmúlt években a csapadékok (egy adott terület időjárásának és éghajlatának alapvetően meghatározó jellemzője) tekintetében a gyors (pár óra alatt), hirtelen történő lehullás figyelhető meg. Az intenzitás növekedése a megszokottnál nagyobb mennyiséget jelent, ami több problémát okoz. Rövidtávon talajfelázást, villámárvizeket, csatorna- és szennyvízhálózatok elöntését (hidraulikai túlterhelést okoz a rendszerben), közlekedési balesteket, pinceelöntéseket, középtávon sárlavinákat, földcsuszamlásokat, házak összeomlását, hosszútávon hidrológiai aszályt okoz. Amikor az erős széllökések mellett rendkívüli csapadékhullás párosul, akkor számolni kell épületkárokkal, antennatornyok sérüléseivel, ipari berendezések megrongálódásával, különleges technológiával készült épületek károsodásával stb. A komplex időjárási események kiterjedtebb kárterületein számolni kell azzal, hogy a hivatásos tűzoltó parancsnokságok, katasztrófavédelmi őrsök, önkéntes tűzoltó egyesületek erői le lesznek terhelve és a viharkárok elhárítása, a mentés érdekében polgári védelmi szervezeteket, mentőcsoportokat kell igénybe venni.[18]

Az 1. táblázat a hőmérséklet és csapadékkal kapcsolatos értékeket mutatja be. A táblázat számadatainak leolvasása után szembetűnő, hogy azokban az években, melyekben (katasztrófavédelmi szempontból nagyobb) hidrológiai jellegű káresemény következett be (2001, 2002, 2006, 2010), ott nem biztos, hogy a csapadék mennyiség kiugróan magas értéket képviselt. Erre példa a 2006-os, mikor a legnagyobb évi csapadékösszeg (mm) értéke nem sokkal haladta meg, a 2012-es év értékét, mely rendkívül aszályos évnek tekintendő. Ez bizonyítja a csapadékeloszlás egyenlőtlenségét. De egy másik szembetűnő ok is felfedezhető, úgy, mint a külföldi vízgyűjtőkre érkezet nagymennyiségű csapadék. Erre példa a 2013. év júniusi dunai árvíz. A 2010-es árvíz nagyobb volt, mint a 2001-es, 2002-es, 2006-os, és jól látható, hogy a legnagyobb csapadékmennyisége jóval nagyobb, mint az adott éveké. Ebben az esetben a csapadékosabb tendencia okozta a rendkívüli árvizet. Csapadék tekintetében a 2005-ös év is kiemelkedik a táblázat szerint. A lokális nagy mennyiségű csapadék a Mátrában okozott ún. sodró árvizeket. Az kijelenthető, hogy csapadékban dúsabb években számolni kell sodró árvízzel. Ebben az esetben nemcsak a mennyiséget, hanem az intenzitást is figyelembe kell venni. A 2007-es évben a legnagyobb évi csapadékösszeg 1011 mm volt, ami jócskán megelőzte a 2006-os évet, ahol árvíz okozott

gondokat. Érdekesség, hogy a 2007-es év az erdő- és bozóttüzeiről, hőhullámairól volt híres, míg a 2006-os év a dunai árvízéről és a csapadékban gazdag augusztus 20-i viharról. Ebből megint csak az következik, hogy a csapadékeloszlás nem egyenletes. A 2007-es évnél az leszögezhető, hogy a legmagasabb mért hőmérséklettel rendelkező időszak. A magasabb hőmérsékletnél az erdő- és bozóttüzek kialakulásának az esélye nagyobb (még akkor is, ha döntően emberi mulasztás, szándékosság a fő okozó). A csapadékhiány elősegíti a károsító tényező fennállásának az időtartamát is.

	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
A legmagasabb mért hőmérséklet (°C)	37,8	38,4	39,4	37,2	36,9	36,9	41,9	39.1	37.2	36.8	39,2	40,4
Legalacsonyabb mért hőmérséklet (°C)	-26,1	-28,3	-39,4	-21,8	-26,5	-25,1	-14,8	-19.2	-25.5	-23.7	-18,7	-26,4
Legnagyobb évi csapadékösszeg (mm) éves összeg egy településen	1042	1005	710	1070	1171	887	1011	1001	1087	1555	756	844
A legkisebb évi csapadékösszeg (mm)	378	343	270	494	565	402	414	403	346	643	251	324
A legnagyobb 24 órás csapadékösszeg (mm)	141	141	177	128	164	107	94	97	157	114.4	114	112

1. táblázat. Az elmúlt évek időjárásának hőmérséklettel és csapadékkal kapcsolatos összefoglaló táblázata (Készítette: szerző, 2014, az OMSZ adatai alapján)

ÖSSZEFOGLALÁS

Magyarország éghajlata nem tartozik az erőteljesen szélsőséges éghajlatok közé, habár az időjárása lehet szélsőséges is. A szeszélyességért többek között az Európában való földrajzi elhelyezkedése a felelős. Magyarország éghajlata egyre melegebb és szárazabb. A telek melegebbek és csapadékban gazdagabbak (árvíznövekedés várható), a nyarak melegebbek, a csapadék mennyisége csökkent (területenként változó), az aszály veszélyének a kialakulása nagyobb. Kevesebb a talajba szivárgó téli csapadék, s a kevesebb csapadék intenzíven érkezik, gyakorta kis területre koncentrálódva. Következményei aszály, sárlavinák, helyi elöntések, árvizek. A hosszan tartó és magas hőséggel, melyhez a csapadékszegénység társul az alacsony relatív páratartalommal az a gond, hogy megnő az erdő- és bozóttüzek keletkezésének a valószínűsége (ami mint, tudjuk, az emberi gondatlanságból jön létre általában). Az időjárási események (árvizek, özönvizek, sárlavinák, viharok, óriási jégesők stb.) súlyos környezeti károkat és halálos áldozatokat eredményezhetnek, így komolyan oda kell figyelni rájuk. A meteorológiai modellek szerint, hasonló extrémitású évekkel, mint a 2010-es év a jövőben is számolni kell. Általánosságban elmondható, hogy a klímaváltozás az ár- és belvizek gyakoribb kialakulásával, az aszályos időszakok meghosszabbodásával,

intenzív tüzek keletkezésével, szélsőséges időjárási helyzetek rendszeressé válásával és az édesvíz készletek problémájának súlyosbodásával jár.

A csapadék változását vizsgálva meg kell említeni, hogy a múltban is voltak szélsőségesebb időszakok. Az elmúlt évek szélsőségesebb kimeneteleinek gyakorisága és erőssége tapasztalható, amit a hazai tudományos elit a klímaváltozás egyik valószínűsíthető negatív hatásaiként tart számon. Az éghajlatváltozásból adódó magyarországi hatások hatnak a társadalomra, a természetes és épített környezetre, egyes gazdasági ágazatokra, hidrológiai jellemzőkre, vízellátásra stb. A kérdés az, hogy fel vagyunk-e rá készülve?

KÖVETKEZTETÉSEK

Jelen cikk két tényt állapít meg. Az egyik az éghajlat változásából adódó időjárás módosulásához kapcsolódik. Megfigyelhető az adott hónapok átlagát nézve, hogy egyre magasabb hőmérsékleti értékeket mérnek. A globális szintű melegedésnek tehát van időjárást érintő módosító hatásai. A hőmérséklet emelkedése a csapadékok változását is befolyásolja. A csapadék változása miatt egy-egy év bizonyos évszakában lehetnek szokatlanul nedves időszakok, amelyek az éves csapadékmennyiség értékét növelhetik.

Az elmúlt évek időjárásait vizsgálva megállapítható, hogy aszályok, hőhullámok, rendkívüli csapadékhullások követik egymást (akár) egy éven belül, ami ellentétes helyzeteket generál, megnövelve a szélsőséges eseményeknek való kitettséget. Az általános melegedési ütem a mérsékelt övben – Magyarországon – a ciklonpályák módosulásához vezet. Ha figyelembe vesszük azt, hogy hazánk klímaérzékenysége nagyobb a világ átlagához képest, akkor ez a pályaváltozás nem zárható ki és nem is annyira távoli biztonsági fenyegetés. A ciklonpálya módosulása a csapadékviszonyok megváltozását okozhatja, ezáltal több szélsőséges meteorológiai, hidrológiai (kár)esemény keletkezik.

Az írásműben főként a csapadékkal kapcsolatos időjárási anomáliák kerületek elemzésre, ezzel is érzékeltetve, hogy egy ilyen országban, ahol a folyók vízgyűjtő területe döntően külföldi országokban találhatóak, fontos a csapadék víz (többlet) megfogása. Bár a csapadékhullással is számos hidrológiai esemény keletkezik, az kijelenthető, hogy a kárterületek mérete, jellege, időtartama szerint az árvizek és belvizek a fő természeti veszélyeztető tényezők Magyarországon. Az árvizek kialakulásában a rendkívüli csapadékmennyiségnek köze van, illetve a már kialakult árvíz vízutánpótlását tekintve is nagy szerepe van a nagy mennyiségű csapadékhullásnak, amely a fennálló helyzetet tovább súlyosbítja. Problémaként jelentkezik, hogy a vasutak 10 százaléka árvízi, belvízi területen van. Szükséges lenne, ha a jövőbeli árvízi veszélyeztetettséget újból kiértékelné a szakma, mivel vannak olyan felvetések, hogy a rendkívüli árvizek nem 10-12 évente fognak bekövetkezni, hanem rövidebb időperiódus alatt, ez viszont érinti és érintheti azt a 10 százalékos vasúti pályahálózati részeket (is). Az is megállapítható, hogy az árvizek elleni védekezésnek nagy múltja van, mely jól használható hidrológiai események elleni védekezésben. Azonban itt fontos megjegyezni, hogy a változó éghajlat és annak időjárási leképezése miatt a jelenlegi vizek kártételei elleni védekezési rendszert katasztrófavédelmi szempontok alapján változtatni kell.

Felhasznált irodalom

[1] TEKNŐS, László: A globális éghajlatváltozás egészségügyi aspektusai - a magyar lakosság sebezhetőségének vizsgálata. In: Bolyai szemle, 2013. XXII. évf. 1. szám. p. 281. ISSN 1416-1443 http://portal.zmne.hu/download/bjkmk/bsz/bszemle2013/1/15.pdf (letöltés: 2014. szeptember 16.)

[2] TEKNŐS, László: A globális klímaváltozás és a katasztrófavédelem kapcsolata. In: Hadmérnök, IV. Évfolyam 2. szám - 2009. június. p. 81. ISSN 1788-1919 http://hadmernok.hu/2009_2_teknos.pdf (letöltés: 2014. szeptember 16.)

[3] GMÉLING, Katalin et.al: Prompt gamma aktivációs analitikai vizsgálatok vulkáni, kőzeteken a Balaton-felvidéktől Észak-Patagóniáig. In: Magyar Kémiai Folyóirat. p. 91. ISSN: 1418-9933 http://www.iki.kfki.hu/about_us/archive/MKF/MKF_03.pdf (letöltés: 2014. szeptember 16.)

[4] NAGY, Rudolf: A klímaváltozás hatása a kritikus infrastruktúrák védelmére, Nemzet és Biztonság, 2010. p. 35. ISSN: 1789-5286 http://www.nemzetesbiztonsag.hu/letoltes.php?letolt=126. (letöltés: 2014. szeptember 16.)

[5] MIKA, János: Mi a bizonyíték az emberi hatásra (videó). http://owww.met.hu/pages/idegenek_az_uveghazban.php?part=8 (letöltés: 2014. szeptember 16.)

[6] SOLYMOSI, József: A klímaváltozás várható a klímaváltozás várható nemkívánatos hatásai, kritikus szektorok és a katasztrófavédelmet érintő indikátorok vizsgálata, kidolgozása. Felkészülés a klímaváltozásra: Környezet-kockázat-társadalom, pp.55-78. ISBN: 978-963-878637-0-7 Letölthető: http://www.vedelem.hu/letoltes/tanulmany/tan166.pdf (letöltés: 2014. szeptember 16.)

[7] TEKNŐS, László: A rendkívüli időjárás okozta veszélyhelyzetek és a kárterületeken végzendő polgári védelmi feladatok rendszere Magyarországon. Konferencia kiadvány "Katasztrófavédelmi Díj" Tudományos Konferencia 2013.: c. tudományos rendezvényen elhangzott előadásokhoz. Budapest: Nemzeti Közszolgálati Egyetem, 2013. p. 89. ISBN:978-615-5305-18-4 http://kvi.uni-nke.hu/uploads/media_items/teknos-laszlo-a-rendkivuli-idojaras-okozta-veszelyhelyzetek-es-a-karteruleteken-vegzendo-polgari-vedelmi-feladatok-rendszere-magyarorszagon.original.pdf (letöltés: 2014. szeptember 19.)

[8] Szerző nélkül: Időjárás, klíma és víz az információs társadalom korában. http://cspv.hu/04/holnaputan/omsz.hu.html (letöltés: 2014. szeptember 19.)

[9] HORVÁTH, Levente: Alkalmazkodási kihívások és eszközök az éghajlatváltozási kerettörvényben, 2009. pp. 1-35. http://www.nfft.hu/dynamic/Alkalmazkodasi_kihivasok_es_eszkozok_az_eghajlatvedelmi_kerettorvenyben.pdf (letöltés: 2014. szeptember 19.)

[10] LÁNG, István- FARAGÓ Tibor et.al.: Climate change and hungary: mitigating the hazard and preparing for the impacts (the “vahava” report), Budapest 2010. http://www.vahavahalozat.hu/files/vahava-2010-12-korrigalt-2.pdf (letöltés: 2014. szeptember 19.)

[11] BAKONDI, György et. al.: Nemzeti Katasztrófa Kockázat Értékelés (szerk.: Gyenes Zsuzsanna). Budapest. 2011. p. 9. http://vmkatig.hu/KEK.pdf (letöltés: 2014. szeptember 20.)

[12] CZAUNER, Brigitta et. al.: Hidrogeológia. (szerk.: Mádlné Dr. Szőnyi Judit). 2013 Eötvös Loránd Tudományegyetem, Budapest. http://elte.prompt.hu/sites/default/files/tananyagok/hidrogeologia/index.html (letöltés: 2014. szeptember 20.)

[13] NAGY, Károly - Halász László: Katasztrófavédelem. Budapest, 2002. p. 28. http://hhk.uni-nke.hu/uploads/media_items/nagy-halasz-katasztrofavedelem.original.pdf (letöltés: 2014. szeptember 20.)

[14] KONCSOS, László – BALOGH, Edina: Belvízkockázatok számítása korszerű hidroinformatikai eszközökkel. http://www.hidrologia.hu/vandorgyules/27/dolgozatok/04koncsos-balogh.htm (letöltés: 2014. szeptember 20.)

[15] TEKNŐS, László – ENDRŐDI, István: A szélsőséges időjárás hatása a magyarországi közlekedési alrendszerekre – kiemelten a közút és vasút álágazatokra, In. Horváth Attila (szerk). Fejezetek a kritikus infrastruktúra védelemből. Magyar Hadtudományi Társaság, Budapest, 2013. p. 88. ISBN 978-615-5305-30-6

[16] BÁRDOS, Zoltán – MUHORAY, Árpád: A belvíz kialakulása és az ellene való védekezés lehetőségének vizsgálata. In: Hadmérnök. VII. Évfolyam 1. szám - 2012. március. p. 84. ISSN 1788-1919 http://hadmernok.hu/2012_1_bardos_muhoray.pdf (letöltés: 2014. szeptember 21.)

[17] Szerző nélkül: Árvíz, Belvíz, Aszály. http://www.kvvm.hu/index.php?pid=10&sid=56 (letöltés: 2014. szeptember 21.)

[18] ZELLEI, Gábor- HORNYACSEK, Júlia: Lakosságtájékoztatás, felkészítés és kríziskommunikáció a globális klímaváltozás okozta veszélyhelyzetekben. http://www.vedelem.hu/letoltes/tanulmany/tan173.pdf (letöltés: 2014. szeptember 21.)

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Csanádi Győző
gyozo.csanadi@gmail.com

AZ INFORMÁCIÓMENEDZSMENT SZABÁLYOZÁSA AZ AMERIKAI EGYESÜLT ÁLLAMOK HADEREJÉBEN A KILENCVENES ÉVEKTŐL NAPJAINKIG

Absztrakt

Egy nagyhatalom vezető pozícióját csak a magas technológiai színvonal fenntartásával képes tartósan biztosítani. Az Egyesült Államokban az utóbbi húsz évben egyebek mellett megfelelő válaszokat kellett adnia arra a kérdésre is, hogy miképpen lehetséges hatékonyan menedzselni a posztmodern korszak katonai kihívásaival szembenéző haderő információs folyamatait. Tekintettel a stratégiai szerepkörben, és rendelkezésre álló erőforrásokban mutatkozó jelentős eltérésekre, önmagában az Egyesült Államok katonai információmenedzsmentjének a puszta leírása nem feltétlenül biztosít a magyar viszonyokra azonnal hasznosítható ismeretet. Ahhoz, hogy a rendelkezésre álló szakirodalomból hazai vonatkozásban alkalmazható következtetéseket lehessen levonni, fel kell tárni a feladat és szervezeti felépítés, valamint a technológiai fejlődés mélyebb ok-okozati összefüggéseit. Ennek megfelelően jelen publikáció az Egyesült Államok katonai információmenedzsmentjének bemutatása mellett az eltelt 20 éves időszakra vonatkozó szakirodalom áttekintésével azt a célt tűzi ki maga elé, hogy egy átfogó kutatás részeként hozzájáruljon a Magyar Honvédség információmenedzsmentjének újragondolásához.

Without maintaining the level of technology a great power cannot keep worldwide dominance. The recent 20 years United States had to create proper response for the post-modern challenges against military information management. Considering the significant differences in strategic role and level of resources the pure description of US military information management is not relevant to the Hungarian situation. In order to draw useful conclusions it is necessary to analyse causal relations of functions and structures. Thus this paper aims to establish theoretical basis of future elaboration of the Hungarian Defence Forces information management system describing the present US military information system and its doctrinal evolution of the recent 20 years.

Kulcsszavak: *Információmenedzsment, USA haderő, történeti áttekintés, technológia, eljárások ~ Information management, US Defense Forces, historical overview, technology, procedures.*

BEVEZETÉS

A történelem során valamennyi szervezett emberi tevékenységben az információ, mint erőforrás kritikus szerepet töltött be. Információ hiányában az ember nem lett volna képes fenntartani a korai közösségeit, majd később megszervezni a társadalmi és gazdasági struktúráit.

Az információ számtalan tudományos meghatározásából a jelen írásban legjobban alkalmazható kezdeti leírása első közelítésben úgy foglalható össze, hogy az információ „az emberi tevékenységek során létrejövő tudati visszatükröződés, amely új ismeretet nyújt és bizonytalanságot szüntet meg". [1: 15-16] A továbbiakban jelen munka külön foglalkozik az Egyesült Államok katonai gondolkodását meghatározó dokumentumokban az információ definíciójának fejlődésével.

Mivel az információ elősegíti más értékes erőforrások birtoklását, ezért jelentős előnyt jelent versengő helyzetekben, azaz hatalmi értéke van. [1: 17] Az információ birtokosa képessé válik egy tevékenység irányítására, vagy másképp fogalmazva, semmilyen emberi tevékenység nem lehet hosszú távon sikeres megfelelő információ rendelkezésre állása nélkül, így a katona vagy védelmi jellegű tevékenységek sem. [2: 120]

Az információ menedzsment vagy információ gazdálkodás nem más, mint az információnak az egyéb erőforrásokhoz hasonló kezelése. Melynek legfontosabb meghatározója a hatékonyságra törekvés [3: 28-29] és magában foglalja az alábbi alapvető tevékenységeket:

1. szükségletek felmérése
2. tervezés
3. beszerzés vagy előállítás
4. tárolás
5. karbantartás
6. elosztás
7. rendelkezésre bocsátás
8. hasznosítás –felhasználás
9. a felhasználás nyilvántartása elemzése
10. felesleges erőforrások hasznosítása [4: 4]
11. az irányelv ellenőrzése, valamint betartására felügyeleti rendszert kellett létrehozni.

A stratégiai fontosságú technológiák és eljárások, létrehozása erőforrás igényes feladat. A szükséges kutató, technikai infrastrukturális, illetve pénzügyi eszközöknek a hatékony koncentrálására általában csak a technikai és gazdasági nagyhatalmak képesek. Ezek az eredmények és képességek politikai és katonai vezető szereppé konvertálhatók.

A szövetségi rendszerekben a vezető szerepet betöltő nagyhatalmak kettős problémával kell szembesülnie. A hatalmi pozíció megtartása érdekében a legfejlettebb eljárásokat mindenképpen meg kell őrizni kizárólagos használatban, azonban a központi szerepből adódóan a szövetségesek részére bizonyos késéssel elérhetővé kell tenni a technikai és eljárásbeli eredményeket, egyébként az erőforrásokban szerényebb képességű partnerek az együttműködési képesség meghiúsulásával járó lemaradást szenvednek.

A fenti logikából következőleg a vezető technológiai hatalmak eljárásainak és nyomon követése egy hazai volumenű nemzeti rendszer optimalizálása érdekében, hasznos és tanulságos eredményeket hozhat.

Tekintettel arra, hogy az általában más technikai színvonalon álló nagyhatalom eljárásainak közvetlen implementálása a szerényebb képességekkel rendelkező hazai rendszeren belül rendkívül könnyen kontra-produktív lehet, ezért az eljárások egyszerű lemásolása jó eséllyel nem működő, mindemellett igen költséges eredményre vezet.

A Huntingtoni[1] értelemben nyugati civilizációs tömbnek nevezett egység jelenlegi egyik vezető hatalma az Amerikai Egyesült Államok, amely az általa vezetett koalícióban kivívta és megőrizte vezető hatalmát. [5: 17] Tekintettel arra, hogy Magyarország a nyugati civilizáció politikai és katonai tömbjének a tagja ezért az Egyesült Államok haderejében alkalmazott információ menedzsment tanulmányozása értékes eredményeket hozhat.

Jelen cikk nem koncentrál a kétségtelenül érdekes történeti tények bemutatására, hanem a hasznosítható elemek és összefüggések feltárását kívánja elvégezni ezért a vizsgált időszaknak korlátozottnak kell lennie. A jelenkori helyzetre értelmezhető technikai és egyéb logikai összefüggéseket húsz évnél hosszabb időtartamban nem célszerű vizsgálni, mivel a távolabbi összefüggések és tények feltárása elveszti a jelen kori alkalmazásra vonatkozó relevanciáját és a kitűzött feladat szempontjából fölösleges és csupán technikai és információelméleti érdekességként kezelhető.

Jelen kutatás fő célja az Egyesült Államok haderejének utóbbi két évtizedben kidolgozott információ menedzsmentjének megismerése és annak vizsgálata, hogy milyen a Magyar Honvédségre is alkalmazható elvek, módszerek és technikai megoldások azonosíthatók be a vizsgált témakörben. Azonban az alkalmazás, implementálás konkrét lehetőségeit a szerző ebben a munkában nem célozza meg, ez a problémakör egy nagyobb, átfogó kutatásnak tárgyát képezi, és azt készíti elő. A készülő doktori tézisben jelen eredmények, más államok és a NATO, információ menedzsmentjének megoldásai együttesen kerülnek feldolgozásra azzal a céllal, hogy támogassa a Magyar Honvédségben, informatikai rendszerekkel támogatott információ menedzsment megvalósítási lehetőségeinek vizsgálatát.

A fő cél elérése érdekében két mellék célt is teljesíteni kell. Egyrészről, szükséges egy megbízható módszer kidolgozása, a különböző szintű belső szabályzók fogalmi és tartalmi és összehasonlításának érdekében, amellyel feltárhatók az esetleges fogalmi és egyéb tartalmi átfedések. Ez azért fontos, mert a vizsgált dokumentumok komplex összefüggések szabályozását hivatottak megvalósítani, így a kognitív elemzés a nagy terjedelmű és bonyolult információ halmazban az emberi memória korlátai miatt segédeszköz alkalmazását igényli. Másrészről a vizsgálat során adódik a lehetőség a gazdasági, technológiai és védelempolitikai szituáció kihatásainak vizsgálata. Az eredmény két oknál fogva is érdekes, önmagában a tény, hogy megfigyelhető bármilyen közvetett hatás, igazolja a feltételezést, hogy az információ menedzsment, és ilyen formán az információ, egy kulcs fontosságú tényező, amellyel kapcsolatban egy tudatos állami vezetés nem engedheti meg, hogy ne adaptálja a politikai és gazdasági szituációkhoz. Továbbá, tekintettel a kialakulóban lévő történelmi helyzetre, hazánknak sincs semmilyen garanciája arra, hogy a nyugati koalíció részeként, egy napon ne kelljen szembenéznie a saját 9/11-évl.

FORRÁSOK FELDOLGOZÁSA

Dokumentumok

A feldolgozott források két nagy típusba sorolhatók. A téma feldolgozása vonatkozásában primer forrásként kezelt írások a szabályzók szerepét betöltő dokumentumokból állnak. Ezen források vizsgálatával időben előre haladva és a különböző vezetési szintenként is elkülönülő mintákat lehet venni az információ menedzsment elképzeléseire és annak fejlődésére vonatkozólag.

---

[1] Samuel P. Huntington (1927-2008) politikatudós, leghíresebb művében a Civilizációk összecsapása és a világrend kialakulása című könyvében határozza meg a nyolc civilizációt, (kínai, japán hindu iszlám ortodox nyugati latin-amerikai afrikai) melynek kiterjedése nem feltétlenül az országok határait követi.

A feldolgozott források másik típusa az ismeretanyag értelmezését megkönnyítő, elsősorban általános és háttér információkat nyújtó dokumentumokból áll.

A vizsgálat a különböző szintű dokumentumok összehasonlításával és nyomon követésével történik. Az Egyesült Államok Védelmi Minisztériumában a szabályzók az alábbi rendet követik. Stratégiai szinten *irányelveket, direktívákat* adnak ki, összhaderőnemi szinten összhaderőnemi *doktrínát,* haderőnemi szinten haderőnemi doktrínát és *szabályzatokat* készítenek.

A védelmi szektor egészére vonatkozólag az Egyesült Államok Védelmi Minisztériumának Irányelvei[2] határozzák meg a működés stratégiai szintű szabályait.

Az információ menedzsment vonatkozásában a vizsgálat tárgyát képezi a „Védelmi Információs Menedzsment (IM) Program" tárgyban 1992 október 27-én kiadott 8000.1 számú irányelv[3], melynek változása nyomon követhető a 2002, 2003, 2009–es kiadások összehasonlításával.

A Védelmi Minisztérium 7740.1 számú, „Védelmi Minisztérium Információ Erőforrás Menedzsment Program" tárgyban, 1994 november 16-án kiadott irányelve[4] csatlakozó és hivatkozott dokumentumként képez forrást a feldolgozáshoz.

Doktrinális szinten az irányelvek feldolgozása, végső soron a katonai szabályzatok és szakutasítások formájában jön létre. A szabályzat fejlesztés és a legfelsőbb szintű irányelvek között legtöbbször az úgynevezett doktrínák képeznek kapcsot. [6: 1] A doktrínák kidolgozására külön szervezetek specializálódnak, a haderőnemi doktrinális központok illetve az összhaderőnemi kérdések vonatkozásában a Légierő, Szárazföldi és Tengeri (Összhaderőnemi) Alkalmazási Központ, a továbbiakban ALSA.5

Az ALSA által 1999 áprilisában kiadott „az információgazdálkodás több haderőnemi doktrínája"6 tárgyú kiadványában [6: 4] hozta létre a katonai információ menedzsment összhaderőnemi doktrínáját.

Ez a dokumentum az Egyesült Államok haderőnemi doktrinális központjainak együttműködésével jött létre és ennek megfelelően a különböző haderőnemi számokat egyszerre viseli. Minden haderőnem a saját elnevezést és számozást használ a doktrínák nyilvántartására. [6: 3] Így a fenti JTF-IM7 összefoglaló nevű dokumentum haderőnemenként az alábbi számokat kapta:

12.Szárazföld: FM 101-4
13.Tengerészgyalogság: MCRP 6-23A
14.Haditengerészet NWP 3-13.1.16
15.Légierő: AFTTP(I) 3-2.22

Szabályzat szintjén a szárazföldi haderőnem AR 25-1 „Szárazföldi Csapatok tudásmenedzsment és információ technológia menedzsmentje" [8] című szabályzat két változata kerül megvizsgálásra 2004 és 2013 évi kiadásban.

Időbeliség

[2] Department of Defense Directive (DoDD)
[3] Hivatkozásokban DoDD 8000.1
[4] Hivatkozásokban DoDD 7740.1
[5] ALSA: Air Land Sea Application Center, Légierő, Szárazföldi és Tengeri (Összhaderőnemi) Alkalmazás Központ
[6] Multiservice Procedures for joint task force information management
[7] Joint Task Forces Information Management
[8] Army Regulation 25-1 Information Management, Army Knowledge Management and Information Technology Management

A szabályzók eloszlása a vezetési szintje és időbeli változatok követésével biztosítja a folyamat vezetési szintek közötti és időbeli változásainak megfigyelését is, melyet az 1. táblázat foglal össze.

Vezetési szint	Szabályzó	1990-94					1995-99					2000-04					2005-09					2010-14				
irányelvek	DoDD 8000.1			■										■	■						■					
	DoDD 7740.1				■																					
doktrína	JTF-IM									■															■	
szabályzat	AR 25-1														■										■	

1. táblázat. A feldolgozott dokumentumok

Az 1. táblázat elemzéséből, látható, hogy a doktrinális szinten a témában csak egy összhaderőnemi doktrína készült, egyéb az informatikai haderőnemi alkalmazásával foglalkozó több nyilvános doktrína nem került kiadásra. [6: 2]

A táblázatból megállapítható továbbá, hogy a változások jól nyomon követhetőek az időben és a rendelkezések hierarchiája tekintetében is.

ELŐZMÉNYEK

Az Egyesült Államokban a haderő számítástechnikai eszközök alkalmazása az ötvenes évek közepéig nyúlik vissza. [7: 33-35] A „Tömeges megtorlás”9 stratégiáját 1961-ben leváltó „Rugalmas reagálás”10 doktrínájával alapvetően megváltozik a katonai gondolkodás, ez kihatással van a haditechnikai eszközök alkalmazására, [8: 1-2] így a fegyveres erők vezetési rendszereire is. A vezetési elemek egységesítésével az adatok és kódok szabványosításával [4: 8-9] és korszerű vezetés automatizálási eszközökkel történő ellátása után egységesített és automatizált hírközlő rendszerek kerültek bevezetésre. A hetvenes években elfogadott „Reális elrettentés”11 stratégiájával a vezetési eszközök, eljárások modernizálása a csapatok létszám és nukleáris csapásmérő képességek csökkentése mellett a hatékonyság és a rugalmasság megtartása érdekében, még nagyobb hangsúlyt kapnak. A nyolcvanas években az eszközpark bővülése és a hálózatba kapcsolás fejlesztése tovább folytatódik, amely a beszerzési és alkalmazási eljárások szabványosítására való törekvéssel jár. [7: 38-40]

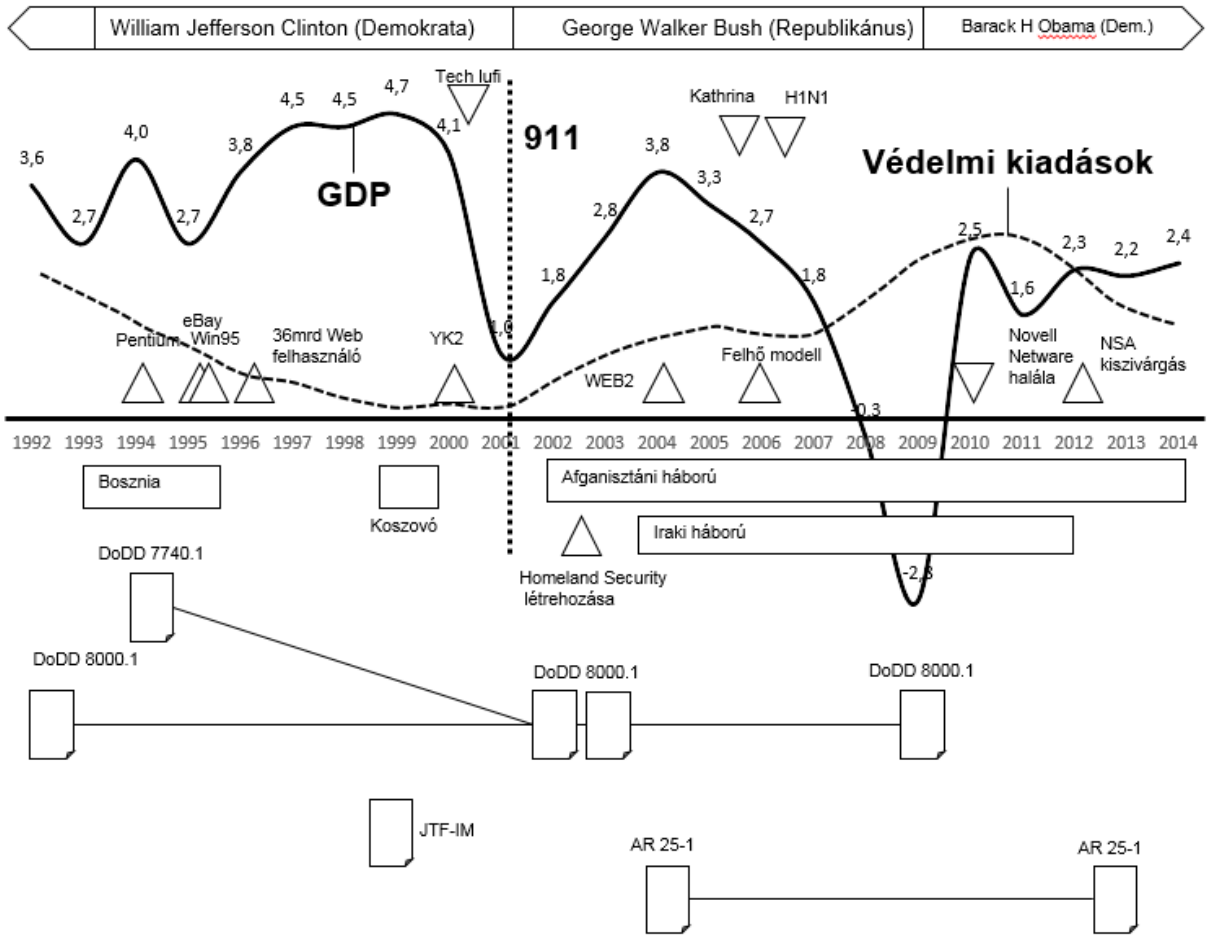
AZ USA ÁLTALÁNOS HELYZETE A 90’ ÉVEKTŐL NAPJAINKIG

A vizsgált időszak gazdasági, technológiai és védelempolitikai jelenségeit foglalja össze az 1. ábra, ahol gazdasági indikátorként a GDP változása szolgál. A technológiai változásokat fontosabb események, feltüntetésével, a katonapolitikai szituáció pedig az USA védelmi kiadásainak alakulásával, illetve a főbb katonai tevékenységek feltüntetésével mérhető.

[9] Strategy of massive retaliation: Az USA katona stratégiája 1954-1961 között, elsősorban a nukleáris eszközök jelentős fölényére a „tömeges megtorlás” lehetőségének fenntartásán alapul [9: 3]

[10] Strategy of flexible response : Az USA katona stratégiája 1961-1971 között, amely nem veti el a nukleáris konfrontációt, de törekszik a hagyományos fegyverrendszerekkel felszerelt haderő rugalmas alkalmazására [9: 3]

[11] Strategy of realistic threat: Az USA katona stratégiája 1971-1991-ig a hidegháború befejezéséig, a rendelkezésre álló gazdasági és katonai potenciál korlátozott lehetőségeinek realisztikus becslésén alapszik, melynek eredményeképpen a haderő korszerű elektronikai és lézer eszközökkel történő modernizálásával, az ambíciószintek és haderő csökkentéssel járt, miközben alapjaiban megegyezik a „rugalmas reagálás” stratégiájával [9: 3]



1 ábra:[12] Gazdasági, katonai és technológiai események és a vizsgált dokumentumok kiadásainak időben történő ábrázolása

Az Egyesült Államok hidegháborút követő katonapolitikai tevékenységét két fő szakaszra lehet bontani, a hidegháború befejezésétől a 9/11-ig tartó időszakra, ezt az egyszerűség kedvéért 90' éveknek, illetve az azt követő – napjainkig tartó – időszakra.

STRATÉGIAI SZINTŰ SZABÁLYOZÁS A HIDEGHÁBORÚ UTÁN 09/11[13]-IG

A 90' évek, a hidegháború utáni időszak jellemzése

Az USA a hidegháború 1992-ben bejelentett hivatalos befejezésével14 [14: 1] új típusú kihívásokkal kellett, hogy szembe nézzen. A posztmodern korba lépő világban az USA hegemóniáját látens módon meghirdető azóta többszörösen cáfolt Fukuyamai tétel szerint a világ egypólusúnak látszik [15: 721-723]. Majd a valós új típusú kihívásokra válaszul az Egyesült Államokban megfogalmazzák az új stratégiai elképzelések alapjait, mely a biztonság, konzultáció elrettentés és partnerség mellett a válságkezelésre helyezi a hangsúlyt. [16: 5] Az úgy-

[12] A GDP adatok vonatkozásában [10: 1]. A technológiai adatok vonatkozásában [11: 1] és [12: 1] A politikai információk vonatkozásában [13: 1]

[13] A 2001. szeptember 11-i terrortámadások alapjaiban megváltoztatják az Egyesült Államok kül- és belpolitikai törekvéseit.

[14] 1990 Február 1-én GW Bush és Borisz Jelcin Camp David-i tárgyaláson hivatalosan is bejelenti a több mint negyven éves hidegháború befejezését.

nevezett Pax Americana[15] a „demokrácia importjának” nevezett liberális intervencionista[16] politika [9: 20] következményeként a fegyveres erőknek új méretű és új típusú képességet kell kialakítani, melyben fokozott szerepet játszik a naprakész és rendkívül pontos információ áramlás.

Az 1. ábrán is jól megjelenik, hogy összességében a korszakot kezdetben a győztesek optimizmusa és stabil normál hullámzású gazdaság jellemzi és a csökkenő védelmi kiadások jellemzik. Az 1994–1996. időszak technológiai innovációi gazdasági fellendülést eredményez, ami a technológiai buborék[17] kidurranásával hirtelen zuhanásba kezd.

Stratégiai szintű szabályozás (direktívák) a kilencvenes években

Rögtön a hidegháború megnyerését követően, 1992 október 27.-én adja ki az Egyesült Államok Védelmi Minisztériuma a „*Védelmi Információs Menedzsment (IM) Program*” tárgyban készült *DoDD 8000.1* számú irányelvét [17: 1-6] A direktíva két fő célt tűz ki:

16. az 1992 február 12-én a C3I18 rendszer [18: 14] létrehozása érdekében kiadott DoDD 5137.119 direktívában meghatározottakat kiegészíti az Információ Menedzsment program végrehajtása érdekében.
17. az információ menedzsment alapvető elemeinek folyamatos fejlesztése céljából, szabályozza a Védelmi Minisztérium szervezeteinél alkalmazott eljárásrendek, az információs erőforrás menedzselés és a támogató informatikai eszközpark és szolgáltatások fejlesztésének rendjét. [17: 1]

A direktívában két fő irányelvet (policy) fogalmaznak meg, elsőként, hogy a minisztérium feladatának teljesítése érdekében a döntéshozóknak pontos és azonnali információt kell biztosítani. Ez az igény nyolc alpontban kerül kifejtésre. A pontok a 2. táblázatban összefoglalt szabályokat határozzák meg.

---

[15] A „Pax Romana” ókori kifejezés parafrázisa, amely a Fukuyamai gondolat alapján a béke alapját az amerikai értékrend általánossá válásával tekinti megoldottnak, ahogy a római birodalom is a világ uralásában látta a béke(Pax) lehetőségét.

[16] A Wilsoni elvekhez igazodó Bill Clinton külpolitikai irányelve.

[17] Az információ technológiába vetett gazdasági elvárások nem hozzák meg az elvárt eredményt, a gazdaság mélyzuhanásba kezd.

[18] C3I – Command, Control, Communications, and Intelligence: Híradó, Informatikai, és Felderítő Rendszerek. A csapatok tevékenységének tervezésében irányításában és ellenőrzésében a parancsnokokat támogató rendszerek [18: 14]

[19] A Védelmi Miniszter Helyettes (Deputy Secretary of Defense) 5137.1 számú 1992. február 12-én kiadott A Híradó Informatikai és Felderítő Rendszerekért felelős helyettes államtitkár feladatairól szóló irányelve nem kerül közvetlen feldolgozásra, mivel az ebben meghatározott rendelkezések csupán kiegészülnek a jelen munkában feldolgozott funkciókkal

Fsz.	Szabályozott tulajdonság	Szabály
1	Információ igény meghatározása	Funkciók és a végrehajtott feladatok szerint
2	Adatok és az információk tulajdonlása és strukturálása	Tulajdonos a minisztérium és teljes interoperabilitást biztosító struktúrát kell kialakítani
3	Informatikai rendszerek életciklusa	A kezdettől a kivonásig ki kell alakítani
4	A funkcionális eljárások alapvető elvei	Biztonság, integritás, és túlélő képesség
5	A funkcionális eljárások megváltoztatása	A minisztérium által jóváhagyott gazdaságossági vizsgálatok alapján
6	Az eljárások továbbfejlesztésének meghatározása és engedélyezése	Minisztérium által jóváhagyott működési és adatmodellek alapján úgy, hogy más területek információja is integrálható legyen
7	Díjjak felszámítása az információért és az informatikai eszközök használatáért	Ahol lehetséges alkalmazni kell
8	Igények és visszajelzések	Elfogadás és jóváhagyás és a visszajelzések rendszerének megszervezését a miniszteri irodavezető és az egyesített vezérkar főnöke hajtja végre

2. táblázat. A DoDD 8000.1 első fő irányelvben meghatározott szabályok

A második fő cél, hogy az informatikai rendszerek tervezése és beszerzése során a védelmi minisztérium egészének megfelelő nézőpontból kell eljárni. Ez az igény öt alpontban kerül kifejtésre, a pontok a 3. táblázatban folytatólagos sorszámokkal feltüntetett szabályokat határozzák meg. [17: 2-3]

Fsz.	Szabályozott tulajdonság	Szabály
9	Költséghatékonyság	Ahol lehetséges a minisztérium nézőpontjából, központi rendszer és biztonsági menedzsmentet kell kialakítani a funkcionális rendszereket integrálni kell.
10	Adatdefiníciók	Minisztériumi szinten szabványosított, beleértve a fegyver és informatikai rendszerek interfészeit is.
11	Informatikai rendszer felépítése	Haderőnemtől és funkciótól függetlenül az információigény modelljétől függően, ami magában foglalja a létrehozás, gyűjtés, feldolgozás továbbítás tárolás, rendelkezésre bocsátás elemeit
12	Információ biztonsági szintjének megállapítása az informatikai rendszerek felépítésénél	A felhasználóknak háborús szituációra készített kockázati elemzés alapján
13	Információs rendszerek fejlesztése modernizálása	Üzleti alapú költséghatékonysági alapon, amely magában foglalja a prototípus alapú fejlesztést, ha lehetséges központi raktárak használatával és a szabványos szoftverek használatával.

3. táblázat. A DoDD 8000.1 második fő irányelvben meghatározott szabályok

A dokumentum mellékletében felsorolás szerűen definiálják az információmenedzsment alapelveit, amelyek a 4. táblázatban szereplő folytatólagos folyószámokon szereplő szabályokat hozza létre. [17: 12]

Fsz.	Szabályozott tulajdonság	Szabály
14	Az információ menedzselése	Központi vezetéssel és decentralizált végrehajtással
15	Új rendszer fejlesztése	Egyszerűsítéssel, integrálással, összevonással
16	Üzleti eljárások	A magán és közszféra számára legjobb eredményt nyújtó költséghatékonyság elemzéssel, új üzleti eljárásokat csak vizsgálat és jóváhagyás után lehetséges bevezetni
17	Informatikai rendszerek	Az általános használatú eszközök preferálása
18	Feladatok szervezése	Minden előnyt és költséget vegyen figyelembe
19	Információ rendszer fejlesztés	Közös elvek és módszerek és szabványok alapján rövid fejlesztési időtartamban minél kisebb fejlesztési költségek és mihamarabbi használat érdekében a fejlesztés eljárási modellek alapján kell végrehajtani lehetőleg verseny alapú beszerzésekkel
20	A számítástechnikai és távközlési infrastruktúra	Legyen az információs rendszer által átlátható
21	Adatbevitel	Csak egyszer
22	Információhoz való hozzáférés	Ellenőrzött és a szükségleteknek megfelelően korlátozott módon, a szándékos és véletlen megváltoztatás és törlések megakadályozásával
23	Felhasználói felület	Legyen felhasználó barát és egységes

4. táblázat. A DoDD 8000.1 alapelveiben meghatározott szabályok

Az irányelv öt felelőst jelöl ki a feladatok végrehajtására, akiknek konkrétan meghatározza a feladatait. Feladat fő felelősének a Védelmi Minisztérium Híradó, Informatikai, és Felderítő rendszerekért felelős helyettes államtitkárt nevezi meg.

A dokumentum a mellékletében egyéb fogalom definíciók mellett definiálja az információ, az információ menedzsment és az információs erőforrás menedzsment fogalmát.

Információ (definíció)

„Az ismeretnek, azaz a tényeknek, adatoknak vagy elképzeléseknek bármilyen közlése vagy fogadása, ami magában foglalja, számszerű, grafikus vagy elbeszélő formákat, bármilyen szóbeli, vagy egyéb hordozón található, beleértve a számítógépes adatbázisokat, az írott, vagy mikrofilmen, illetve a mágnesszalagon tároltakat is.”[20] [17: 10]

Az információ menedzsment (definíció)

„A hatékony szervezeti működés szempontjából kritikus erőforrást jelentő, híradó, automatizált információs és felderítő rendszerek által előállított adatok, vagy információk létrehozását, megosztását és megsemmisítését támogató tevékenység, mely megfelel az Információs Menedzsment előírásainak.

Magában foglalja a minisztériumi vezetők által, a működési tevékenységek rendszerbe foglalt fejlesztését, annak érdekben, hogy létrehozzák az adatok szabályozott felhasználását, továbbá az információs erőforrás menedzsmentet, valamint az informatikai eszközöket és szolgáltatásokat.”[21] [17: 10]

Az információs erőforrás menedzsment (definíció)

„A tervezési, pénzügyi, szervezési, irányítási képzési, támogatási, vezetési tevékenység mely összefügg az ügynökségek információ gyűjtési, előállítási, terjesztési feladataival és

[20] A szerző saját fordítása
[21] A szerző saját fordítása

magában foglalja az információ kezelését és a hozzá kapcsolódó erőforrásokat, mint például az automatikus adatfeldolgozó rendszerek erőforrásait."[22] [17: 10-11]

Az ismertetett dokumentum szerint információmenedzsment és erőforrás-menedzsment egymásra épül, az információs erőforrás-menedzsment elsősorban az ügynökségek szintjén folyó erőforrásokra koncentráló tevékenység, míg az információ menedzsment a minisztérium szintjén elsősorban az információs folyamatokra koncentráló tevékenység, ami magában foglalja az információs erőforrás-menedzsmentet is.

A Védelmi Miniszter 1992 pénzügyi évére vonatkozó jelentésében külön említést tesz az Információ Menedzsment fejlesztésére, amit *Szervezeti*[23] *Információ Menedzsment* „Corporate Information Management (CIM)" kifejezéssel mutat be. Az Szervezeti Információ Menedzsment fő célja a munkafolyamatok és működési eljárások (business processes) fejlesztése, tekintettel az információs technológiák által kínált lehetőségekre. [19: 31-32]

Az 1992-ben kiadott „Védelmi Információs Menedzsment (IM) Program" tárgyban készült 8000.1 számú irányelvét követte a 1994 november 16-án a *DoDD 7740.1* számon kiadott *„Védelmi Minisztérium Információs Erőforrás Menedzsment"* tárgyú irányelv. A kiadvány deklarált célja, hogy elősegítse a koordinált és integrált információ menedzsment funkciókat. [20: 1]

Az irányelv egy egyszerű politikát határoz meg és ehhez rendel 12 eljárást. Eszerint minden erővel arra kell törekedni, hogy hatékony, gazdaságos beszerzésekkel és információ felhasználással fejlesszék a műveleti képességeket. [20: 1]

Az eljárások az 5. táblázatban felsorolt szabályokat definiálják [20: 2-3]

[22] A szerző saját fordítása

[23] Az eredeti angol kifejezés –corporate, a polgári életből kölcsönzött terminológia, eredetileg nagyvállalatot jelöl, jelen esetben, a Védelmi Minisztérium vonatkozásában a „szervezeti" kifejezés használata megfelelőbb.

Fsz.	Szabályozott tulajdonság	Szabály
1	Műveleti és döntési tevékenység támogatása	időben rendelkezésre bocsájtott, pontos és minőségi információ biztosításával
2	Beszerzések	gazdaságos és hatékony minél több képességgel és a feladatokhoz mért költségekkel
3	Informatikai rendszerek felépítése	úgy hogy a horizontális és vertikális információ megosztást segítse, beleértve más kormányzati és szövetséges szervezeteket is a biztonság előírások betartásával
4	Informatikai tervezés	biztosítsa, hogy a vezetési eljárások része legyen
5	Informatikai rendszerek fejlesztése	a felhasználók felelőssége és megbízhatósága szükséges (együttműködő felhasználók)
6	Információ, informatikai rendszerek kezelése	fegyelmezettséggel a bevezetéstől a beszerzésen át a kivonásig
7	Jelentések és felmérések	rendszeresen, az információ hasznosságának növelése, az árak csökkentése és a távolabbi célok elérése érdekében
8	Koncepciók megismertetése és kiképzés	minél szélesebb körben végrehajtani
9	információ menedzsment funkciók	a célok elérése érdekében szervezetten és integráltan kell megvalósítani
10	Adatok bevitele (gyűjtése)	nem duplikált módon, költséghatékonyan
11	Kapcsolatok más szervezetekkel	hatékony munkakapcsolatokat kell kiépíteni a szervezeten belül és más kormányzati szervekkel
12	Az informatikai erőforrások tervezése	az információs menedzserek békében és háborúban egyaránt törekedjenek a fenntarthatóságra és készenlétre

5. táblázat. A DoDD 7740.1 eljárásaiban meghatározott szabályok

Az irányelv hét felelőst jelöl ki, mivel a fő tárgy elsősorban erőforrások kezelése ezért a fő felelős ez esetben a számvevői feladatokkal megbízott államtitkár (Assistant Secretary of Defense -Comptroller[24]). [20: 3-7]

Az ajánlás eltérően, általánosabban definiálja az információ fogalmát, Az információs erőforrás menedzsment definíciójában, pedig az információ menedzsmenttel átfedő fogalmat ad meg, az információ menedzsmentet pedig nem definiálja.

Információ (definíció)

„A gondolkozó ember érdeklődése tárgyához adatokat rendel a tudása növekedése érdekében. Az információ az adatok összeillesztéséből analizálásából és összefoglalásából ered."[25] [20: 14]

Az információ erőforrás menedzsment (definíció)

„Az információval kapcsolatos szabályrendszer, eljárás vagy tevékenység (automatikus vagy nem automatizált), melynek kezelése biztosítja a szervezet jelenlegi általános vagy jövőbeli igényeit."[26] [20: 14]

A DoDD 8000.1 és a 7740.1 dokumentum szabályainak összehasonlítása során a 2–5. táblázatokban felsorolt szabályok összevetése a hatodik táblázatban lett összefoglalva[27].

[24] Comptroller, azaz számvevő, a pénzügyi és erőforrás ügyeket kézben tartó magas rangú hivatalnok [21: 1]
[25] A szerző saját fordítása
[26] A szerző saját fordítása
[27] Az összehasonlítás során mindkét táblázat mindkét mezőjében (szabályozott tulajdonság és szabály) lévő tartalommal végig kellett vizsgálni az összevetendő szabályrendszert, mivel átfedő fogalmak és absztrakciók lehetségesek.

Fsz.	DoDD 7740.1	DoDD 8000.1	Közös momentum
1	1	1	hasonló motívum, az információ igény kielégítése információ funkciók szerint
2	2	9, 13,17,19	a költséghatékonyság hasonló motívum, 8000.1 szorgalmazza az egységesített eszközrendszerek üzleti alapú beszerzését
3	3	6, 11,17	az informatikai rendszer felépítése vonatkozásában eltérő hangsúly, a 7740 a vertikális és horizontális kapcsolódását a 8000.1 pedig az információs modell és az általános használatú eszközök elsődlegességét hangsúlyozza
4	5	13,15	információs rendszer fejlesztése eltérő motívum a 7740.1 a felhasználók felelősségét emeli ki, a 8000.1 pedig a központosítást és üzleti alapú fejlesztést, egyszerűsítést és integrálást
5	6	3	közös motívum az informatikai rendszerek életciklusának igénye
6	7	8	jelentések, felmérések, visszajelzések 7740.1 célt a 8000.1 pedig felelősséget határoz meg
7	9	14	az információ menedzselése eltérő a 7704.1 a szervezettséget és integrálást a 8000.1 a központi vezetést és decentralizált végrehajtást határozza meg
8	10	21	hasonló motívum az egyszeres adatbevitel
9	12	4	közös motívum a biztonság, és túlélőképesség a 7704.1-nél az erőforrások a 8000.1-nél pedig az információs folyamatok vonatkozásában

6. táblázat. A DoDD 8000.1 és 7740.1 szabályainak összevetése

A vizsgálat alapján megállapítható, hogy a 7704.01 esetében leírt 12 szabály és a 8000.1 dokumentumban definiált 23 szabály esetén 9 kapcsolódó motívum van, melyből csupán 5 esetben fordul elő hasonló[28].

A kilencvenes években kiadott doktrína

Az összhaderőnemi szintű doktrína az érvényben lévő és 8000.1 (1992.10.27) és a 7740.01 (1994.11.16) után 1999 áprilisában adták ki a Légi Szárazföldi és Tengeri Alkalmazási Központ által készített „Az információgazdálkodás több haderőnemi doktrínája” címmel29. [22: 1-73]

A dokumentum hat fontos célt határoz meg [22: 6]

1. Meghatározza az Információ menedzsment fogalmait és eljárásait beleértve a szűrés, egyesítés, és rangsorolás kérdéseit.
2. Meghatározza az Információ menedzsment felelősségi köreit az információ kezelés megőrzés és védelem területén
3. Áttekintést nyújt a rendelkezésre álló információ menedzsmentet támogató rendszerekről
4. technológiákat mutat be, hogyan kell kezelni az elektronikus mail, hírcsoportok, weblapok a Globális Vezetési és Irányítási Rendszer (GCCS), irodai üzenetek és felderítő jelentések által létrehozott hatalmas adatmennyiséget
5. bemutatja az őszhaderőnemi vezetési központ (JOC) és az őszhaderőnemi Felderítő támogató Elem (JISE) közötti információ áramlásának megszervezéséhez szükséges eljárásokat
6. Iránymutatást nyújt a parancsnok kritikus információigényének kielégítéséhez és információ kérési eljárások, jelentések, eligazítások és hadműveleti parancsok kiadásával kapcsolatban

[28] A hasonlóság ebben az esetben is legfeljebb 55%

[29] A doktrína jelöléséről lásd a „Dokumentumok” alcímnél a 4. oldalon leírtakat.

Az információ menedzsment fogalma a 8000.01 direktíva logikáját követi és az információ beszerzésének kezelésének és irányításának eljárásaiként határozza meg. [22: , 12]

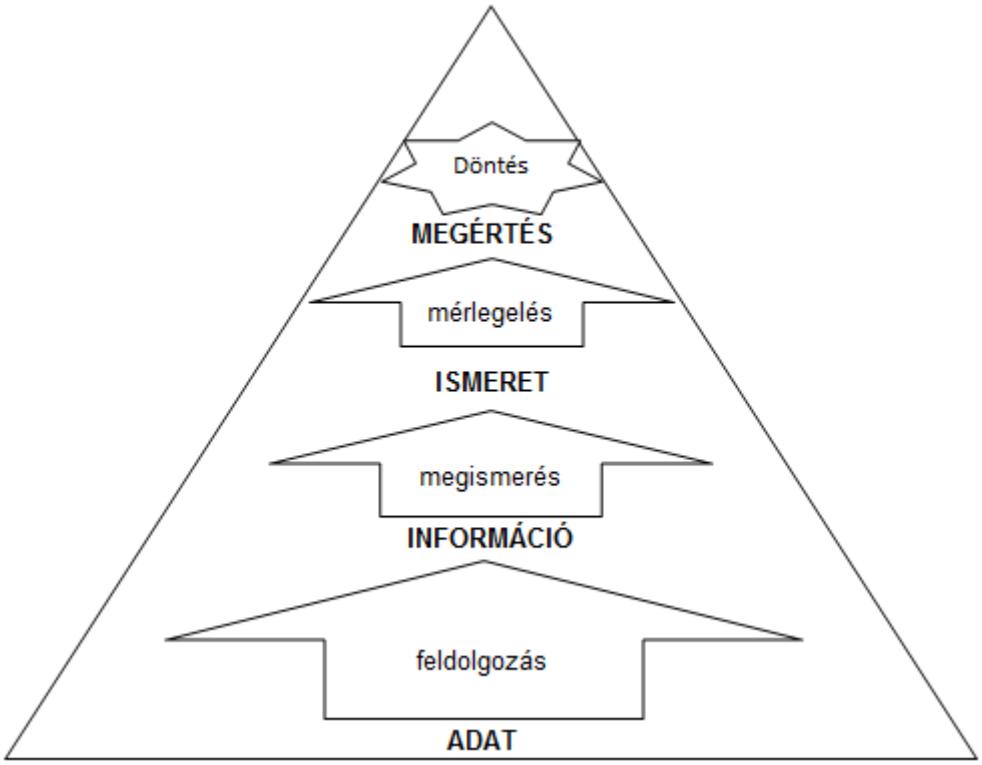
A doktrína bemutatja információ minőség a kognitív hierarchia és az és az információ áramlás jól hasznosítható fogalmait. [22: 13]

Az információ minőségi kritériumait a 7. számú táblázat foglalja össze.

Kritérium	Tartalom
biztonság	szükség esetén a megfelelő védelem biztosítottsága
tömörség	csak szükséges részletek rendelkezésre bocsátása
teljesség	a döntéshozónak a szükséges információk rendelkezésre állása
használhatóság	közérthető formában rendelkezezésre állás
időbeliség	mennyiben biztosít a döntéshez elégséges időt
relevancia	a faladhoz és a szituációhoz használhatóság
pontosság	menyiben tükrözi a valós szituációt

7. táblázat[30] Az információ minőségi kritériumai

A kognitív hierarchia magában foglalja az adat, feldolgozás, információ, megismerés, ismeret, mérlegelés, megértés, döntés elemeit magában foglaló folyamatot, melyet az 2. ábra mutat be.



2 ábra[31] A kognitív hierarchia

A hatékony információ áramláshoz szükséges alaptulajdonságok, a helyes pozicionálás, mobilitás, elérhetőség, összeolvasztás. [22: 15]

[30] A doktrína Figure I-1. Information Quality Criteria című ábrájának átdolgozásával és fordításával [22: 14]
[31] A doktrína Figure I-2. Cognitive Hierarchy című ábrája a szerző alkalmazásában magyar fordítással [22: 14]

A doktrína szerint információ menedzsment megvalósításához Információ Menedzsment Tervet[32] kell készíteni, amelynek tartalmaznia, kell az információ megfelelő kritériumok alapján történ szűrésére, a több forrásból érkező információk egyesítésére és a parancsnokság döntéshozási képességét támogató rangsorolásra vonatkozó eljárásokat. [22: 16]

A doktrína meghatározza az információ kezelésnek felelősségi köreit és feladatait azon belül a szervezetszerű vezetők, a parancsnok, a törzsfőnök a főnökségek feladatait, mely többek között kiterjed a harci munka rendjének[33] meghatározására, az Információ Menedzsment Tisztek (IMO) webmesterek és feladatok képzések megszervezésére. [22: 17-24]

A doktrína szerint összhaderőnemi szinten az alábbi bizottságokat kell létrehozni:

18. Információ Menedzsment Munkacsoport (Information Management Board, IMB) amely az információ menedzsment szakmai irányítója [22: 20]
19. Az Egyesített Helyzetkép Munkacsoport (JTF Common Tactical Picture Board, CTPB) mely megszervezi a szárazföldi, légi és tengeri helyzetinformációk összeálló Egyesített Helyzetkép kialakításának szabályait. [22: 21]

A doktrína részletezi az Információ Menedzsment tisztek, a támogató ügynökségek az információs rendszer felhasználók, a hálózatmenedzsment és információvédelem feladatait.

A doktrína az információ menedzsment támogatására szolgáló rendszerekként bemutatja a Globális Vezetési és Irányítási rendszert (Global Command and Control, GCCS)

Amely egy világméretű egységes rendszer a csapatok vezetési és irányítási képességének biztosítása érdekében.

Négy modulból épül fel [22: 25-27]

20. Az összhaderőnemi tervező és hadműveleti modul (The Joint Operations Planning and Execution System, JOPES)
21. Összhaderőnemi telepíthető felderítő támogató rendszer (Joint Deployable Intelligence Support System, JDISS)
22. Egyesített hadműveleti és harcászati helyzetkép információ rendszer (Common Operational Picture (COP) segment (chart)/ Common Tactical Picture (CTP)
23. a böngésző e-mail és hírcsoport szoftvercsomag

További támogató rendszerként sorolja fel a hálózati applikációk menedzsmentjét, amely magában foglalja a hálózati szolgáltatásokat, weblapokat, hírcsoportokat, e-mail szolgáltatást megosztott könyvtárakat és egyéb szolgáltatás automatizálási szolgáltatásokat.

A doktrinális elképzelés információ menedzsment támogató rendszernek tekinti a helyi hálózatot és Video Telekonferencia szolgáltatásokat is. [22: 27-37]

A doktrína bemutatja az információ menedzsment eljárásait és követelményeit, [22: 38-52] így a parancsnok számára kritikus információk követelményeit, (CCIR)34, illetve az információkérés eljárásait (RFI)35 illetve a különböző jelentések, eligazítások és a parancsok kiadásnak megszervezését. [22: 38-41]

A doktrína kitér az információ megvédésének kérdéskörére is. [22: 53-73]

Összességében a doktrína példákkal jól illusztrálva és gyakorlatiasan foglalja össze az információ menedzsment kérdéseit az őszhaderőnemi szintű vezetési szintnek megfelelő parancsnokság részére.

Összefoglalva a kilencvenes évek stratégiai elképzeléseit szabályozó két dokumentum eltérő nézőpontból viszonyul azonos feladathoz. A 7704.1 az erőforrások oldaláról közelít, míg a 8000.1 pedig az információs folyamatokat helyezi előtérbe. A két irányelv két különböző, de

---

[32] Information Management Plan IMP
[33] Harci munka rendje, battle rhythm
[34] Critical Information Requirements (CCIR)
[35] Requests For Information (RFI)

egymás mellett álló hivatalnokot bíz meg a legfőbb felelősséggel. A két ajánlás tartalmaz hasonló irányelveket, de egyik sem definiál szervezetet az információmenedzsment megvalósításához. Az irányelvek között megjelenik a gazdaságosság és hatékonyság illetve az általános kereskedelmi használatú eszközök felé fordulás. Az információmenedzsment, mint feladatkör az híradó és informatikai szakfeladatnak indul. Összevonásokra, központosításra és szabványosításra törekszenek, beleértve a beszerzési eljárásokat is. A szolgáltatásoknál a kereskedelmi –térítéses alapú modellt erőltetik. Ahol lehet, a célrendszerek helyett általános használatú erőforrások felhasználását szorgalmazzák. A koncepcióban felismerhetők az ekkor kialakuló és a stratégiai gondolkozásba bekerülő COTS[36] elmélet alapgondolatai, mely az ebben az időszakban a Védelmi Minisztérium vezetésében dolgozó William James Perry nevéhez köthető, újszerű megközelítés volt a fejlesztések és beszerzések végrehajtására. [23: 1] A kereskedelmi termékek felé való fordulás az üzleti szektornak a felélénkülésén alapszik, ami visszavezethető az időszak első harmadában megjelenő információ technológiai innovációkra és a csökkenő védelmi kiadások miatti takarékoskodási kényszerre. (1. ábra).

Az információ menedzsment összhaderőnemi víziója, gyakorlatias ellentmondásoktól mentes és jól követhető utasítási rendszert ír elő az információk kezelésére és a megvalósító informatikai eszközök használatára.

Az időszakra vonatkozó legfontosabb összefüggés, hogy az információ (menedzsment) szerepét elhomályosította az optimista politikai hangulat és a prosperáló gazdaság, az információ menedzsment kérdésit átlapoló fogalmak és felhalmozó jellegű erőforrás szemlélet uralja, ami elkerülte a vezetők figyelmét.

AZ INFORMÁCIÓ MENEDZSMENT SZABÁLYOZÁSA 9/11-TŐL NAPJAINKIG

A 2001. szeptember 11-két követő időszaknak két fő jellemzője van, a terror elleni küzdelem, ami két elhúzódó és költséges katonai beavatkozást eredményez, az afganisztáni és az iraki műveleteket, továbbá egy elmélyülő gazdasági krízis jelenik meg, melynek rendkívül sok összetevője van, és kifejtése kívül esik jelen munka látókörén. Az időszak kezdeti szakaszában a védelmi költségvetés emelkedése figyelhető meg, ami 2011-ben tetőzik, majd lassú csökkenést mutat. (1. ábra)

Stratégiai szintű szabályozás

A terrortámadások következtében keletkező sokk feldolgozása során az információ értéke felértékelődött, ezért az ellenlépések sorában a DoDD 8000.1 szabályzatot egymást követő két évben is kiadták, 2002. évben [24: 1-12] és 2003. évben. [25: 1-12]

A két dokumentum csak nyelvtani és stilisztikai javításokat tartalmaz, amelynek legfőbb eleme, a rövidítések kibontása, például a 4.8.5. pontban, a 2002 verzió az alábbi szöveget tartalmazza: „Commercial or NDI shall be used as much as possible, …" [24: 5] az „NDI" rövidítés a későbbi dokumentumban feloldva „non-developmental item"formában szerepel. [25: 5] Lényeges tartalmi differencia hiányában, a továbbiakban csak a 2003. évi kiadás kerül elemzésre.

Az ajánlás címe összevont formában tartalmazza a korábbi 8000.1 dokumentum és 7740.1 dokumentum címét: *„A Védelmi minisztérium információs erőforrás és információtechnológiai menedzsmentje"*. Ezzel egyesíti a két tartalmat és törli a 7740.01 dokumentumot.

[36] COTS Commercial Off-The-Shelf, kereskedelmi forgalomból beszerzett eszközök felhasználásán alapuló beszerzési és fejlesztési stratégia.

A dokumentum deklarált célja az információs erőforrás menedzsmentre vonatkozó előírások lefektetésére, mely magában foglalja az információ technológiát[37] és átalakítja a felsősségeket és feladatköröket. Továbbá iránymutatást biztosít a különböző szintű Informatikai Vezetők (Chief Information Officers CIOs) [25: 1] A felelősségi kör a személyek meghatározásán kívül kiegészül az információ életciklusára (teljes) vonatkozó előírással is.

A direktíva 10 alapvető irányelvet (policy) határoz meg melyet a 8. táblázat tartalmaz. [25: 2-6]

Fsz.	Szabályozott tulajdonság	Szabály
1	Informatikai Vezető (CIO)	minden komponensnél kötelező álkomponensnél létrehozható
2	fórumot kell biztosítani	a CIO- és az egyéb érintett vezetők között, a feladatok optimalizálása érdekében
3	döntéshozók információ ellátása	pontos és egyértelmű formációk biztosításával a szükséges információ biztosításával a duplikálás elkerülésével integrált együttműködő-képes szabványos biztonságos és hatékonyan beszerezhető munkakörnyezet biztosításával ahol lehetséges, költséghatékony egységesített rendszerek adatközpontok és hálózatok használatával életciklus menedzsment szemlélettel
4	döntésminőség növelése	integrált elemzés tervezés finanszírozás és értékelés használatával a vezetési eljárások fejlesztése a vertikális és horizontális erőforrás integrálással, költséghatékony tervezés és beszerzéssel,
5	Informatikai rendszer bevezetés előtt	fontosság mérlegelésével, a nem központi funkciók kiszervezésével, más magán és közszférában felhasznált módszerek figyelésével, COTS és NDI[38] eszközök használatának maximalizálásával
6	beszerzési stratégia	verseny és üzleti alapon COTS eszközök használatával
7	modernizáció biztonsági garanciái	pontos követelménytámasztással, felhasználói visszajelzések figyelésével, jól lépcsőzött eszközbeszerzésekkel, eszközök megosztásával és újrafelhasználásával,
8	szakember képzés	programok indításával a jól képzett szakértők érdekében
9	sérült személyek támogatása	az egészséges személyek hozzáférésének hasonló szintű információ elérésének biztosításával

8. táblázat A DoDD 8000.1 irányelveiben definiált szabályok

Felelősségek hét különböző szinten kerülnek kiosztásra a legfőbb felelős a Védelmi Minisztérium híradó, automatizált információs, és felderítő rendszerekért felelős helyettes államtitkár, aki egyben a Védelmi Minisztérium Vezető Információs Tisztje is. [25: 6-12]

A definíciók szintjén az információ fogalmát 8000.1 előző verziójából kiindulva határozza meg, és újra megkülönbözteti és világosan definiálja az információ menedzsment és az információ erőforrás menedzsment fogalmát

Információ definíciója megegyezik az előző verzióban megfogalmazottaknak, azzal a különbséggel, hogy a mikrofilm, illetve a mágnesszalag kifejezést felcserélik audiovizuális kifejezésre. [25: 14]

Az információ menedzsment (definíció)

[37] Information technology, magyarul legtöbbször „informatika” kifejezéssel fordítják

[38] NDI Non-Developmental Item, fejlesztést nem igénylő eszköz, olyan korábban már kifejlesztett eszköz, amely minimális beállítás után képes az igény kielégítésére

„Az információ teljes életcikluson át tartó tervezése finanszírozása manipulálása és ellenőrzése”[39] [25: 14]

Az információs erőforrás menedzsment (definíció)

„Eljárás, az információs erőforrások kezelésének az ügynökség feladatainak végrehajtása illetve teljesítményének növelése érdekében, beleértve az információ gyűjtés erőfeszítéseinek csökkentését.”[40] [25: 14]

A fogalmak alapvetően letisztultak és nem átfedő definíciókat hoznak létre. Összességében a direktíva egyesíti a két szülő direktíva előírásait, és ezzel megszünteti a kettős szabályozást, továbbá a fogalmi, felelősségi kör és feladat átfedéseket. Továbbra sem határoz meg konkrét szervezeteket, csak koordináló testületi munkát ír elő. A terrortámadás és a gazdasági sokk következtében a kormányzati funkciók újragondolásának eredménye. Levonható tanulság, hogy a jól definiált információ menedzsment vis maior helyzetek bekövetkezése és felszámolása során hangsúlyos szerepet kap. Erről árulkodik a biztonsági információk beszerzéséért felelős Homeland Security szervezet létrehozása is. Előtérbe kerül a folyamatok átgondolása, optimalizálása, központosítása.

Érvényben lévő stratégiai direktíva

A DoDD 8000.01 számú direktíva 2009.02.10.-én kiadott legfrissebb érvényben lévő változata a *„Védelmi Minisztérium szervezeti informatikai rendszer menedzsmentje”* címet viseli. [26: 1]

A direktíva két új fogalmat mutat be, a Globális Információs Rács, Global Information Grid, GIG[41] fogalmát, továbbá az Információs Fölény fogalmát [26: 1]

A direktíva deklarált fő célja az információ menedzsment felügyeleti jogkörének újra szabályozása, jogszabályi harmonizálás, továbbá az Informatikai Vezető (CIO) szerepkör és egyéb feladatok szabályozása, az információs fölény elérése érdekében, valamint az információ megosztás nemzeti stratégiájával kapcsolatos feladatok meghatározása. [26: 1]

A direktíva 11 alapvető irányelvet (policy) határoz meg, amit a 9. táblázat tartalmaz. [26: 2-3]

Fsz.	Szabályozott tulajdonság	Szabály
1	az információ	stratégiai eszközként kezelendő, megfelelően védett, és az életciklusban megfelelően megosztott bármely arra jogosult belső vagy külső együttműködő számára
2	a szakterületi eljárások	legyenek egyszerűsítve mielőtt jelentős informatikai fejlesztés kezdődik
3	Informatikai Vezető (CIO) megléte	Minden komponensnél
4	az információs megoldások	biztosítsanak megbízható, időbeli, pontos és védett információt, amely ellenáll az információs hadviselés, terrorizmus bűnözői tevékenység és a természeti katasztrófák és balesetek hatásainak
5	védelmi nagyvállalati információs	a Nemzeti Védelmi Stratégia elvei szerint kell tervezni,

[39] A szerző saját fordítása
[40] A szerző saját fordítása
[41] Globális Információ Rács, Global Information Grid (GIG) Speciális rendszer, amely globális mértekben biztosítja a kommunikációs csatlakozási lehetőségeket [27: 1]

	rendszer	fejleszteni, beállítani, annak érdekében, hogy a hálózat centrikus környezet elérhető legyen
6	szervezeti informatikai infrastruktúra	a szabványoknak megfelelően és a jövőbeli fejlesztések lehetőségét biztosítva kell kialakítani
7	információs beruházások	átfogó tervek alapján valósíthatók meg
8	beszerzési stratégiák	a kormányzat és a vállalkozó között helyesem megosztott kockázattal lehetőség szerint COTS és NDI eszközök költséghatékony alkalmazásával
9	nagy kockázatú információs beruházások	pilot, kísérleti és teszt megoldások alkalmazásával
10	szakállomány képzése	magas szintű képzés megvalósítása a legfontosabb szakértők részére és általános munkaerő képzés a lehetőségek maximális kihasználásához
11	sérült személyek támogatása	az egészséges személyek hozzáférésének hasonló szintű információ elérésének biztosításával

9. táblázat Az érvényben lévő DoDD 8000.1 alapvető irányelvei által előírt szabályok

A felelősségek vonatkozásában a feladatért a hálózatokért és információs integrációért felelős helyettes államtitkárt[42] ASD(NII)/DoD CIO nevezi meg fő felelősként. [26: 6-9]

A fogalmak vonatkozásában, az információ fogalma változatlan marad, az információ menedzsment és az információs erőforrás menedzsment fogalom beolvasztásra kerül egy közös fogalomba. [26: 10]

Védelmi minisztérium Szervezeti Informatikai Rendszer (definíció)

„A Védelmi Minisztérium információ erőforrásai, eszközei, és eljárásai, az információs előny elérése érdekében. Ami magában foglalja az információt magát és az életcikluson át tartó menedzsmentjét, az eljárásokat, beleértve a kockázatkezelést, ami a védelmi minisztérium feladatának és eljárásainak érdekében információt kezel. Továbbá a tevékenységeket, ami a szervezeti információs rendszer tervezésével, felépítésével, kezelésével, védelmével kapcsolatos, valamint a szükséges információs erőforrásokat –azaz személyeket, pénzügyi és technikai és informatikai eszközöket beleértve a nemzetbiztonsági rendszereket is.”[43] [26: 10]

Összefoglalva az érvényben lévő direktíva az információ és az információs erőforrások vonatkozásában egységes elveket fektet fel. Az Informatikai Vezetők (CIO) rendszerén kívül csak egy szervezeti elemet hoz létre a Védelmi minisztérium szintű Védelmi Szervezeti Informatikai Rendszer Osztályt, amely egyaránt felel az információs folyamtok és az információs erőforrások összehangolt és koordinált kezeléséért. A direktíva új elveket vezet be, mint a hálózat centrikus hadviselés és a Globális Információs Rács illetve az információs fölény.

A stratégiai szintű szabályozás a fejlődés során egyszerűsíti a fogalmakat, megszünteti az átfedő fogalmi és feladat meghatározásokat, beépíti a modernizált elveket. Egyszerűsítésre, szabványosításra és rendszerek összevonására törekszik, széleskörűen támogatja –erőlteti a COTS és NDI rendszerek használatát, költséghatékony és megtervezett rendszerek létrehozására törekszik. Integrál és a nem központi szolgáltatások vonatkozásában a szolgáltatások kiszervezésére törekszik. Ez a stratégiai szintű direktíva a gazdasági válság mélypontján (1.

[42] Hálózatokért és információs integrációért felelős helyettes államtitkár (ASD(NII)/DoD CIO), Assistant Secretary of Defense (Networks and Information Integration). 2003 májusában létrehozott új szervezet vezetője, aki felelős az informatikai, űr és felderítő, tevékenységekért, ez a személy egyben a Védelmi Minisztérium és a Védelmi Informatikai Rendszerek Ügynökségének Vezető Információs tisztje [28: 46]

[43] A szerző fordítása

ábra) a republikánus adminisztráció által preferált, neo-konzervatív gazdaságpolitikai felfogást tükrözi.

Szabályzatok

A szabályzat szintű előírások nyomon követhetők a szárazföldi csapatok részére kiadott *„Szárazföldi tudás menedzsment és informatikai menedzsment”* címen 2004 07 30.-án kiadott *AR 25-1* és a 2013-an kiadott frissítésből, melynek a címét *„Információ menedzsment, szárazföldi Információ technológia”* –ra változtatták meg.

Mindkét verzió egy új kiadású direktívát követ, ennek megfelelően aktualizálásra került a legújabb irányelveknek megfelelően.

A szabályzatok a meglévő állománytáblához igazított, szorosan nemzeti specifikus információt tartalmaznak ennek megfelelően a teljes részletességű kifejtése nem releváns a hazai képességek vonatkozásában. Így a továbbiakban a szabályozott kérdések köre és a változások kerülnek vizsgálat tárgyává. Korábbi kiadású szabályzatok, és egyéb haderőnemek szabályzatainak bemutatása még kevesebb relevanciával van, a jelenlegi rendszerek vizsgálata szempontjából ezért hely hiányában nem kerülnek feldolgozásra.

Az első szabályzat meghatározza a felsősségi köröket, direktívának megfelelően létrehozza és szabályozza az Informatikai Vezető (CIO) funkciót és feladatait. [29: 4-14] Bemutatja a szárazföldi informatikai rendszer infrastruktúráját, [29: 20-24] továbbá az információ biztonság kérdéseit. [29: 24-27] A híradó, informatikai, és felderítő rendszerekkel foglalkozó fejezetben külön kitér az informatikai támogatás alapelveire, illetve a szolgáltatásokkal kapcsolatban bemutatja a telekommunikációs szolgáltatásokat és a nagy-távolságú kommunikációs eszközöket, és kitér a katonai infrastruktúra létrehozása során az informatikai támogatás kérdéseire. [29: 27-49] Az álló és mozgóképes adatokat feldolgozó rendszerek Vizuális Információ címen önálló fejezetet kapnak. [29: 49-60] A szabályzat hátralévő részében az adatmentések és a nyomtatási szolgáltatások kérdései kerülnek kifejtésre.

A szabályzat több kiemelésre méltó elemet tartalmaz.

A szabályzat az *információt, mint erőforrást* tételezi. A megfogalmazás szerint: „ ...amikor nemzetbiztonsági, személy vagy –tulajdonjogi védelme, másként nem indokolja az információt, mint osztott erőforrást kell kezelni. Az információ kérelmeket és azt kiszolgáló informatikai rendszereket az információ kezelés költséges volta miatt körültekintően kell megtervezni. Az információkat és adatokat két nagy csoportra kell osztani –a publikus és a nem publikus információk csoportjába, az előbbi a Kormányzat tulajdonát képezi és nem köthető személyhez, nem minősített és egyébként az információ megismerésének alapelve alapján a közvélemény számára megismerhető kell, hogy legyen. Ezek az információk és adatok megoszthatók az interneten, szabadon elérhető weblapokon. A második csoportba a személyhez köthető, törvény által minősített vagy érzékeny adatok és információk találhatók ezeket az információkat a védelem fokától függően szabályozott elérésű weblapokon az érintettekkel meg lehet osztani.”[44][29: 8-9]

Az információ menedzsment kérdéskörét a híradó és informatikai szolgálat feladatkörébe vonja, az Informatikai Vezető (CIO) funkció a G-6 főnök felelősségi körébe kerül

A szabályzat bevezeti a *tudásmenedzsment* fogalmát, mely alatt a szárazföldi haderőnek egy stratégiáját érti, melynek célja a hálózat centrikus, tudás alapú haderővé történő átalakítás biztosítása.

[44] A szerző saját fordítása

A szárazföldi haderő szervezeti szintű híradó és informatikai struktúráját egy arra feladatra dedikált önálló szervezet a *Szárazföldi Szervezeti Hálózat Technológia Parancsnokság* biztosítja ez a NETCOM[45].

Érvényben lévő szárazföldi szabályzat

Az érvényben lévő 2013. 07. 25-én kiadott AR 25-1 szabályzat megváltoztatott címmel, mint *„Információ Menedzsment, Szárazföldi Információ Technológia"* került bevezetésre.

A szabályzat az előzőhöz képest öt kérdéskörben modernizálja a tartalmat. A szárazföldi információ technológia és weblap menedzsment, információ és biztonsági menedzsment, a szervezeti szintű kialakítás vonatkozásában illetve a katonai objektumok informatikai szolgáltatásai és biztosítása vonatkozásában.

A szabályzat tükrözi a szervezeti változásokat, a létrehozott *Szárazföldi Kiber-Parancsnokság* feladatinak beillesztésével a felelősségi körök aktualizálásával a változások mértékének megfelelően. A szabályzat beépíti a bevezetésre került Számítógép hardver szoftver beszerzési rendszer[46] használatának kérdéseit. A szövegből törli a mentések és nyomtatási szolgáltatások, információ biztonság és vizuális információ fejezeteket A telekommunikációs szolgáltatások kiemelésre kerülnek, mivel önálló szabályzat rendelkezik felőlük.

A szabályzatban megjelenő kiemelésre méltó új elemek jelennek meg. Az *információs elszámoltathatóság és átláthatóság* fogalma, mely két fő elemet foglal magában. Az mentés-archiválási kötelezettséget, melyhez kifejlesztett informatikai rendszert[47] és szervezetet kapcsol. A mentés és archiválási feladatokra kijelölt szervezet U.S. *Army Records Management and Declassification Agency* (RMDA) kezeli a web technikán alapuló szerep-alapú mentési rendszert, amely képes mind az elektronikus, mind az eredetileg papír alapon készített dokumentumok eltárolására és azokkal a törvényi kötelezettségek értelmében eljárni. Az információs elszámoltathatóság és átláthatóság második eleme az információnak, mint erőforrásnak a kezelése, amely már az előző szabályzatban megjelenik, és onnan szövegszerű átemelésre kerül. [30, 2. o.]

Új elem továbbá Szárazföldi Kiber-Parancsnokság feladatainak és felelősségeinek megjelenése, amely illeszkedik az újonnan létrehozott US Kiber-Papancsnokságok rendszerébe. A parancsnokságot a 2. hadsereg bázisán hozták létre és felelős a szárazföldi haderő szintű kiber-műveletek végrehajtásáért, továbbá a haderő katonai hálózat védelem szolgáltatója. A hálózati és információ biztonsági feladatok végrehajtója. [30: 6]

További kiemelésre érdemes gondolat az *információ erőgeneráló hatása* címen kerül bemutatásra, mellyel kapcsolatban három fontos momentum kerül befutásra [30: 2]

24. az erő sokszorozó hatás –azaz a pontos és időben nyújtott információ növeli a harcoló erők képességeit
25. a felhasználó központú információ technológia menedzsment, mely erősíti a szolgáltatások hatékonyságát.
26. a felhasználó részvételét az információ technikai menedzsmentben A felhasználók közvetlen bevonása az információ technológia kritikus voltát emeli ki, különös tekintettel a felhasználói igények kiemelt kezelése vonatkozásában.

Összefoglalva a szárazföldi haderő szabályzataiban innovatív és előremutató információk találhatók. A szabályzók követik a felső szintű ajánlásokat és implementálják a szervezeti változásokból adódó feladatokat. A szabályzatok az összhaderőnemi doktrína jól eltalált kere-

[45] Pontos nevén NETCOM/9th
[46] Computer Hardware, Enterprise Software and Solutions procurement system
[47] A mentés archiválási feladathoz létrehozott informatikai rendszer, Army Records Information Management System (ARIMS)

teit és alapelveit követik, a modernizált gondolatokat közvetlenül képesek beépíteni a szövegbe, így rugalmas és jól használható szabályzati rendszer építhető fel.

KÖVETKEZTETÉSEK

A bemutatott stratégiai doktrinális és szabályzati szintű dokumentumok jelentős tanulságul szolgálhatnak a hazai információmenedzsment funkció kialakítására és fejlesztésére vonatkozóan. A kutatás a kitűzött fő célját elérte, amennyiben a vizsgálat során a hazai szabályozások és technológiák szempontjából hasznosítható elemek beazonosíthatók voltak.

A stratégiai szintű dokumentumok vizsgálatánál felismerhető, hogy párhuzamosan létrejöhet az információ menedzsmentnek legalább két fő szempontú víziója.

1. az információs folyamatok szemszögéből vizsgált
2. az erőforrások szemszögéből vizsgált

Az előbbi nézőpontot elsősorban az alkalmazó, azaz a híradó informatikai illetve hadműveleti szemléletű szerveztek alkalmazzák, másodikat pedig a pénzügyi és beszerzéssel foglalkozó logisztikai szemléletű szervezetek.

A kettős, egymással párhuzamosan létező vízió átfedő fogalmakat és felelősségi köröket alakíthat ki, mint ahogy az a 8000.1 illetve 7440.1. dokumentum elemzésénél jól bizonyíthatóan megfigyelhető volt. A helyes tervezés tehát követi a felelősségi körök arányos és egyértelmű elosztására és a fogalmi illetve felelősségi átfedések kiküszöbölésére mutatott példát. A stratégiai szintű szabályozás anomáliáinak felszámolására azonnal sor kerül, amikor az információ menedzsment kérdésköre előtérbe kerül. Ezt a folyamatot vizsgált esetben a 9/11 kataklizma és a gazdasági recesszió együttes hatása váltotta ki.

A doktrinális azaz az összhaderőnemi szintű vízió esetén jól látható, hogy egy átgondolt dokumentum jól alkalmazható logikai alapot tud nyújtani a szabályzat kidolgozásához. A vizsgált szabályzatok vonatkozásában az irányelvek a későbbiekben közvetlenül is be tudnak épülni a szabályzatokba, ehhez csak a megfelelő kereteket kell felállítani.

A szabályzókban megjelenő és megfontolás illetve további vizsgálat tárgyát képező elvek és szervezeti elemek összefoglalása a 10. táblázatban található.

Fsz.	Elem	Hasznosítás	Forrás
1	Információs Tiszti feladatkör létrehozása	Az információ menedzsment kérdéskörének magas szintű vezetőhöz történő kötése	DoDD 8000.1 (2003.11.21) 8. sz. táblázat 1. folyószám
2	Integrált elemzés tervezés finanszírozás és értékelés bevezetése a vezetési eljárások fejlesztése a vertikális és horizontális erőforrás integrálással, költséghatékony tervezés és beszerzéssel	A döntésminőség növelése	DoDD 8000.1 (2003.11.21) 8. sz. táblázat 4. folyószám
3	Az információ stratégiai eszközként való kezelése,	Információs előny kivívásához szükséges alapgondolat	DoDD 8000.1 (2009.02.10) 9. sz. táblázat 1. folyószám, valamint az AR 25-1
4	Globális Információs Rács	Mint alapgondolat, megvizsgálandó, hogy mely technikai eszköz képes „lokális" –hazai információs rács kialakításához hozzájárulni esetleg olyan módon, hogy a kialakítandó nemzeti kommuni-	DoDD 8000.1 (2009.02.10) 9. táblázat 5. folyószám

		kációs eszköz illeszthető legyen a szövetségi erőforrásokhoz	
5	Hálózat Centrikus Hadviselés	Alapelvként felhasználható, az együttműködés és a nemzeti elképzelések fejlesztése érdekében	AR 25-1
6	Nagyvállalati informatikai rendszer	A stratégiai szintű rendszerek egységes kezelése érdekében a technikai és eljárásbeli eszközök részletesebb vizsgálata	DoDD 8000.1 (2009.02.10) AR 25-1
7	Hálózati technológia-parancsnokság	Az osztott erőforrások és szolgáltatások optimális kiszolgálása érdekében	AR 25-1
8	Kiber-Parancsnokság	A védelmi képességek és aktív kibernetikai tevékenységek képességének megteremtése érdekében	AR 25-1
9	Records Management and Declassification Agency	Megoldást jelenthet a törvényeknek megfelelő archiválási és minősített információk kezelésének kérdéskörére	AR 25-1
10	Globális Vezetési és Irányítási Rendszer (GCCS)	A szolgáltatások logikája és technológiája vezérfonalat nyújthat a védett vezetési információs rendszerek hazai megszervezése érdekében	JTF-IM

10. táblázat A megfontolás és további vizsgálat tárgyát képező elvek

A feldolgozott anyagokból jól látható, hogy az olyan komplex kérdések, mint az információ menedzsment megszervezése több összehangolt vezetési szint egymásra épülő erőfeszítését igényli.

A stratégiai szintű szabályzás esetén feltétlenül el kell kerülni a funkciók, feladatok és fogalmak átlapolását, illetve törekedni kell a tisztázás mihamarabbi végrehajtására. Az elemzések során a hazai szabályozások modernizálása érdekében jól beazonosíthatók olyan fogalmi és szervezeti elemek, melyek vizsgálatával szervezeti előnyök érhetők el (lásd 10. sz. táblázat).

A vizsgálat során bebizonyosodott, hogy az általános politikai, gazdasági, technológiai és biztonsági szituáció hatásai tetten érhetők az információ menedzsment szabályozása szintjén. Ezt bizonyítja a kilencvenes évek stratégiai szabályozásánál ismertetett beszerzés-politikai jelenség a kereskedelmi jellegű szolgáltatások felé (COTS, térítéses szolgáltatások) fordulás jelensége. Továbbá felismerhető a stratégiai dokumentum azonnali egységesítése a 9/11 krízist követő időszakban.

A kognitív összefüggések feltárását célzó módszerre vonatkozólag, a kutatás szintén pozitív eredményt hozott, azaz a hasonló tartalmi kérdésekről rendelkező dokumentumok feldolgozása során a belső összefüggések jól feltárhatók a szabályok tételes felfektetésével és összevetésével. Az ehhez szükséges módszer a két párhuzamosan létező direktíva vizsgálatánál bemutatásra került.

A hasznosítható tanulságok fejezetnél felsorolt elemek szabadon bővíthetők. A hasznosítás pontos módja a bevezetőben ismertetett szerint, egy átfogó jellegű kutatásban a szerző szándéka szerint, további vizsgálat tárgyát fogja képezni.

Felhasznált irodalom

[1] Haig Zs.: *Információ – társadalom – biztonság*. NKE Szolgáltató Kft., 2015

[2] Négyesi I.: Az információ szerepe a katonai-vezetői információs rendszerekben. *Hadtudományi Szemle*, II 1 (2009) 119–123.

[3] Munk S.: Katonai informatika a XXI. században. Zrínyi Kiadó, 2007.

[4] Munk S.: Az információ, mint a katonai vezetés erőforrása. (Nyilvántartás, szabványosítás). *Hadtudományi Tájékoztató*, VII 2 (1998) 5–25.

[5] Brzezinski, Z.: Egy új típusú hegemónia. *História*, XXIII 4 (2001) 15–17.

[6] Munk S.: A Katonai Informatika az Egyesült Államok haderejének alap- és műveleti doktrínáiban. *Hadtudományi Szemle*, IV 2 (2011) 1–12.

[7] Négyesi I.: A csapatvezetés automatizálásának egyes tapasztalatai az USA fegyveres erőinél az 1950-es évek közepétől az MN REVA Szolgálat szemszögéből. *Hadtudományi Szemle*, VII 4 (2014) 33–41.

[8] Hangya G.: A biztonságpolitika hatása a haditechnikára. *Hadtudomány*, XII 4 (202) 11

[9] Varga G.: Stratégiai koncepciók a kezdetektől Lisszabonig. *Nemzet és biztonság*, III 9 (2010) 16-25

[10] Kimberly A.*: U.S GDP by Year Compared to Debt, Recessions and Major Events*. http://useconomy.about.com/od/GDP-by-Year/a/US-GDP-History.htm (Megnyitás dátuma: 2015.11.29.)

[11] *Timeline of Computer History\Computers*. http://www.computerhistory.org/timeline/computers/ (Megnyitás dátuma: 2015.11.29.)

[12] *Timeline of Computer History\Networking &The Web*. http://www.computerhistory.org/timeline/networking-the-web/ (Megnyitás dátuma: 2015.11.29.)

[13] *The WHTE HOUSE\presidents*. https://www.whitehouse.gov/1600/Presidents (Megnyitás dátuma: 2015.11.20.)

[14] Michael W.: Bush and Jeltsin declare formal end to cold war. *The New York Times*, 02 02 1992, http://www.nytimes.com/1992/02/02/world/bush-and-yeltsin-declare-formal-end-to-cold-war-agree-to-exchange-visits.html?pagewanted=all (Megnyitás dátuma: 2015. 11. 01.)

[15] Fukuyama, F. F.: *A történelem vége és az utolsó ember*. Európa Könyvkiadó. 2014.

[16] Aspin, L.: Report on the bottom-up review, Secretary of Defense 1993 October, Office of the Secretary of Defense\ Historical Office. http://history.defense.gov/Portals/70/Documents/dod_reforms/Bottom-upReview.pdf (Letöltés dátuma: 2015. 11. 23.)

[17] *Defense Information Management (IM) Program.* (Directive Number DODD 8000.1). US Department of Defense, 1992.10.27.

[18] Munk S.: *Katonai informatika II. Katonai informatikai rendszerek, alkalmazások*. Zrínyi Miklós Nemzetvédelmi Egyetem, 2006. (Egyetemi jegyzet)

[19] Cheney, R.: *Secretary of Defense: Annual Report to the President and the Congress FY1992.* http://history.defense.gov/HistoricalSources/SecretaryofDefenseAnnualReports.aspx (Letöltés dátuma: 2015.11.26)

[20] *DoD Information Resources Management Program.* (Administrative Reissuance, Directive Number 7740.1). US Department of Defense, 1994.

[21] *Under Secretary os Defense (Comptroller)/About Ousd(C)/Ousd(C) History.* http://comptroller.defense.gov/Portals/45/Documents/OUSDC_History/OUSDC_History.pdf (Letöltés dátuma: 2015.11.26.)

[22] *Multiservice Procedures for joint task force information management, FM101-4 MCRP6-23A NWP3-13.1.16 AFTTP(I)3-2.22*. Air Land Sea Application Center 1999.

[23] Négyesi I.: COTS rendszerek alkalmazási lehetőségeinek vizsgálata. *Hadtudományi Szemle*, IV 4 (2011) 111–116.

[24] *Management of DOD Information Resources and Information Technology.* (Directive Number DODD 8000.1). US Department of Defense, 2002.

[25] *Management of DOD Information Resources and Information Technology.* (Directive Number DODD 8000.1). US Department of Defense, 2003.

[26] *Management of DOD Information Enterprise.* (Directive Number DODD 8000.1). US Department of Defense, 2009.

[27] *Global Information Grid.* (Directive Number DODD 8100.1). US Department of Defense, 2002.

[28] *Office of The Secretary of Defense Historical Office*. Key Officials 1947-2014, June 2014. http://www.whs.mil/library/key2004.html (Letöltés dátuma: 2015.11.25.)

[29] *Information Management ARMY KNOWLEDGE MANAGEMENT AND INFORMATION TECHNOLOGY MANAGEMENT.* (Army Regulation 25-1, AR 25-1). Headquarters Department of the Army, 2004.

[30] *Information Management Army Information Technology.* (Army Regulation 25-1, AR 25-1). Headquarters Department of the Army, 2013.

HADMÉRNÖK

XI. Évfolyam 2. szám - 2016. június

Fehér Judit
feherjenator@gmail.com

A RENDŐRSÉGI INFORMATIKAI HÁLÓZATOK INFORMÁCIÓBIZTONSÁGI HÁTTERÉNEK MEGHATÁROZÁSA

Absztrakt

Az információbiztonság helyzetéről készülő felmérés, a biztonság, az irányítás és a kockázatkezelési területek helyzetéről adhat egyszerre objektív és átfogó képet. A hálózat információbiztonsági hátterének meghatározásához, valós értékek eléréséhez meg kell vizsgálni a hálózathoz tartozó dokumentumokat, az informatikai rendszerek és a hálózat lehetséges fenyegetéseit, veszélyhelyzeteit. Mindehhez sérülékenység vizsgálatokat kell lefolytatni, amely párhuzamosan kockázatelemzés elvégzését is feltételezi. A rendőrség egyes informatikai hálózatainak információbiztonsági hátterének vizsgálatai, illetve ezek eredményei valós, gyakorlat orientált információbiztonsági kérdéseket vetnek fel. A feltárt hiányosságokból és tapasztalatokból az informatikai hálózatok információbiztonsági követelményrendszerét lehet megállapítani annak érdekében, hogy a várható biztonsági szintnek és védettségnek az megfeleljen.

A survey about the situation of IT security provides an objective and a comprehensive picture about the situation of security, governance and risk management areas. To determine the network information security background and to the achieve fair values, should be examined documents belonging to the network, the potential threats and the risk positions of information systems and networks, which should be conducted vulnerability assessments with risk analysis. The results of some police information network of information security background investigation raises real practice-oriented information security issues. The identified deficiencies and experiences in the information security requirements of the IT network system can lead to ensure that the expected level of security and protection has been fulfilled.

***Kulcsszavak**: információbiztonság, informatikai irányítás, informatikai kockázatkezelési eljárások ~ information security, information management, information risk management*

BEVEZETÉS

A rendőrségi informatikai rendszereinek és különösen a hálózatainak információbiztonsági kérdéseinek feltárásához több irányú, területileg és időben eltolódó elemzést kell lefolytatni. Elsődlegesen a jelen helyzetből kell kiindulni. A rendőrségi informatikai rendszereken összességében a rendőrségi informatikai hálózatok kerülnek értelmezésre. A rendszerek információbiztonságának vizsgálatához az adminisztratív oldalról megközelítve dokumentumelemzéseket kell lefolytatni, mely során mintavételezéssel kerül meghatározásra az egyes rendőrségi informatikai hálózatok biztonsági helyzete, melyet a rendszer egészére ki lehet vetíteni. A valós értékek eléréséhez meg kell vizsgálni, a mintavételezés során kiemelt informatikai hálózatok lehetséges fenyegetéseit, veszélyhelyzeteit, melyhez dokumentum elemzéseket az adminisztratív területen, a fizikai területen pedig sérülékenység vizsgálatokat kell lefolytatni kockázat elemzéssel. Ezen eredmények a valós gyakorlat orientált információbiztonsági kérdéseket veti fel, mely alapján a hiányosságokból és tapasztalatokból a követelményrendszerét lehetne a kiemelt rendőrségi informatikai hálózatoknak megállapítani. Mindezt annak érdekében, hogy a várható biztonsági szintnek és védettségnek megfeleljenek rendszer szinten. Viszont jelen vizsgálat csak adminisztratív területre szorítkozva az információbiztonsági dokumentum elemzések eredményeit fogja feltárni, a fizikai vizsgálattal egybekötött teljes információbiztonsági hátteret, azok eszközrendszerét, a sérülékenység elemzés és kockázat elemzés eredményeit nem tárja fel.

Az információbiztonsági dokumentumok vizsgálata kiterjesztésre került mind a haza szakmai ajánlásokra, mind a nemzetközi ajánlásokra. Alapvető információbiztonsági dokumentumként kerül használatra a Rendőrségi Ideiglenes Informatikai Biztonsági Szabályzata, és az ISO/IEC 27001:2013 „A” melléklet 10.6 fejezete, a hálózatbiztonsági követelmények tekintetében.

A rendőrségi informatikai hálózatok információbiztonsági helyzetvizsgálata során a fenti dokumentumok átfogó elemzése került lefolytatásra. A dokumentumok szakterületi vonatkozásában az informatikai hálózatok információbiztonságával kapcsolatos rendelkezések köre térben és időben kerülnek szűkítésre. Időbeli vonatkozásában csak és kizárólag a jelen szakirányítási időszakban 2010-óta született és a rendőrségi informatikai hálózatok információbiztonságával kapcsolatos dokumentumok feldolgozására koncentrálódik. Pontosan ezen szempontrendszer miatt a fent említett két dokumentum analízisének célja felkutatni azon pontokat, ahol ráutaló szakmai meghatározásokat találhatunk a rendőrségi informatikai hálózatok információbiztonsági helyzetére vonatkozóan.

A vizsgálat területe korlátozásra került a Nagytávolságú és helyi hálózatok biztonsági osztályba sorolásának állapotában, helyzet felmérésében, a szükséges intézkedések meglétében, az érvényben lévő előírások alkalmazhatóságában, fizikai megvalósíthatóságában. Az elemzés nem terjed ki a minősített hálózatokra, és a kritikus infrastruktúra elemekre.

A vizsgálati pontok fogalmi szintjei:

- információbiztonsági helyzet felmérés,
- biztonsági osztályba sorolás vizsgálata,
- intézkedések megléte, kockázat kelezési eljárások
- előírások alkalmazhatósága,
- fizikai megvalósíthatósága.

A fenti pontok és az azokat övező utalások, a kiemelt informatikai hálózatok információbiztonság vizsgálati eredményei a rendőrségi informatikai hálózatok információbiztonsági helyzetének hátterét mutatják meg.

Ezek alapján a mintavételezésnek megfelelően kiválasztásra került a két legnagyobb terület a rendőrségi hálózatbiztonság területén:

- a rendőrség nagytávolságú informatikai hálózata,
- a rendőrség lokális (helyi) informatikai hálózata.

A RENDŐRSÉG NAGYTÁVOLSÁGÚ INFORMATIKAI HÁLÓZATA - KOMMUNIKÁCIÓS HÁLÓZAT HELYZETVIZSGÁLATA

Az elemzés első lépésében kijelölésre került a rendőrség nagytávolságú informatikai hálózata, azon belül a kommunikációs hálózatot. A vizsgálat szempontjai:

- információbiztonsági helyzet felmérés, a rendszer összetétele, a rendszer kapcsolatai, a rendszerek összekapcsolódásai,
- biztonsági osztályba sorolás, sérülékenység elemzés, kockázat kezelés
- specifikus előírások, előírások alkalmazhatósága,
- fizikai megvalósíthatóság, fizikai védelem.

A rendőrségi hálózatok megkülönböztetése:

- a nagytávolságú-,
- a helyi-,
- a minősített-,
- a zártcélú-,
- a nyíltcélú hálózat,
- a kritikus infrastruktúra.

A vizsgálati szempontrendszert szűkített spektrumának vizsgálatában a nagytávolságú hálózatokon belül elkülönítésre kerül speciális területként a kommunikációs hálózat.
Első elemzési pont a helyzet felmérés. A jelenlegi országos kommunikációs hálózat, az 1994-ben az ORFK és a BM Adatfeldolgozó Hivatal közös beruházásában üzembe helyezett zárt rendszerű X.25-ös táv-adatátviteli hálózat. A rendszer a megyei rendőr-főkapitányságok, és a budapesti kerületi kapitányságok részére biztosít hozzáférést a központi adatbázisokhoz. A városi kapitányságok modemes kapcsolattal a megyei főkapitányságokon keresztül érik el az X.25-ös hálózatot. A rendszerhez hozzáférésük van a BM, az ORFK és a BRFK központi szerveinek, valamint a közigazgatási hivataloknak és a határőrségi igazgatóságoknak.
Az X.25-ös hálózat mintegy 6 000 végponttal rendelkezik, pont-pont hierarchiájú kapcsolat van RIK és a megyei főkapitányságok között.

Második pontként a biztonsági osztályba sorolást vizsgálata következett. Az ORFK szakmai képviseletével történő egyezetések kerültek a vizsgálat érdekében lefolytatásra, továbbá a Nemzeti Elektronikus Információbiztonsági Hatósággal a rendőrségi nagytávolságú informatika hálózat biztonsági osztályba sorolásának tekintetében. Egyértelmű megállapítást nyert, hogy nem került besorolásba, a besorolás körülményei így nem voltak vizsgálhatóak. A biztonsági osztályba sorolás hiányosságának vizsgálata során arra hiányosságra is fény derült, hogy nem lelhetőek fel sem intézkedések írásos formában, sem kockázat kezelési eljárások. A kutatás kiterjedt a sérülékenység elemzési vizsgálatok eredményeire is, de nem voltak fellelhetőek egyik irattárban sem.

Harmadik pontként az előírások alkalmazhatóságát tesztelésre került sorra. A dokumentum vizsgálatokból egyértelműen kiderült, hogy általános érvényű utalásokat lelhetőek fel a rendőrség Ideiglenes Informatikai Biztonsági Szabályzatában, viszont konkrétumokat nem fogalmazott meg, így azok alkalmazhatóságát nem lehetett vizsgálni. Ezen hiányosság abból következett, hogy a biztonsági osztályba sorolás nem történt meg, így specifikusan előírásokat nem lehetett megfogalmazni.

Negyedik pontként a fizikai megvalósíthatóság tekintetében a kommunikációs hálózatot a külvilágtól kívülről és az egyes szervezetek egymás között tűzfalakkal védik. A kábelezés fizikai védelmében viszont hézagokat lehetett felfedezni, sajnos a védelem nem megoldott, ezt kábelezési rajzok támasztották alá. Ez s egyértelmű eredményterméke volt az előírások hiányosságának.

A RENDŐRSÉG LOKÁLIS (HELYI) INFORMATIKAI HÁLÓZATAINAK HELYZETVIZSGÁLATA

A vizsgálat második lépésében kijelölésre került a lokális helyi informatika hálózatok analízise. A szempontrendszerében az előző vizsgálati elemeket figyelembe véve a nagyobb speciális területről haladva a kisebb terület felé volt az elsődleges. A cél a lokális hálózatok elemzésénél a közös használati szempontok helyett az egyéni szempontokat kerültek előtérbe.

Valamennyi kapitányság rendelkezik számítógépes hálózattal, amelyek lehetővé tették rendkívül sok, a rendőrségi szakmai munkát támogató alkalmazás fejlesztését és elterjesztését. A vizsgálat alapját képezték az ORFK szakmai dokumentumai.

Első pontként a helyzet vizsgálat során megállapítást nyert, hogy a lokális hálózatok többnyire NetWare 3.x, kisebb részben NetWare 4.x operációs rendszerre épülnek. Valamennyi hálózat jellemzője, hogy független információs 'szigetekként' működve, helyi alkalmazásokat szolgálnak ki, egymással –vagy egy központi informatikai rendszerrel - kommunikálni, adatot cserélni nem tudnak.

Kivételt képez ez alól a Teve utcai RIK, ahol a hierarchikus szoftvergerinc kiépítésének köszönhetően egységes és integrált informatikai infrastruktúráról beszélhetünk.

A lokális informatikai hálózatok munkaállomásai vegyesen 386, 486, illetve Pentium alapú PC-k. A korábbi évek informatikai beruházásainak nagy része ezeknek a személyi számítógépeknek amortizációs cseréjére irányult.

Második pontként a biztonsági osztályba sorolás vizsgálata során, a nagytávolságú informatikai hálózat részekre bontása után a helyi hálózatok kategorizálása, biztonsági osztály besorolás nem történt meg.

Harmadik pontként az intézkedések megléte során, fellelhető volt a NISZ mint KEKKH jogutódjának irattárában hálózat kábelezési rajzokat, melyek minősített iratok, így azokat a kutatás során nem lehetett felhasználni. Tehát intézkedések megfogalmazása nem volt fellelhető, így kockázat kezelési eljárásokat sem voltak.

Negyedik pontként az előírások alkalmazhatóság során kizárólagosan, a rendőrségi informatikai hálózatának információbiztonságát szavatoló előírást, utasítást információbiztonsági intézkedések az irattárban nem voltak fellelhetők. Csak általános érvényű utalásokat lehetett találni a rendőrség Ideiglenes Informatikai Biztonsági Szabályzatában, ezért azok alkalmazhatóságát nem lehetett vizsgálni.

Ötödik pontként az információbiztonsági fizikai megvalósíthatósága sok helyen (lokálisan) nem megoldott. A hálózatot a külvilágtól kívülről és az egyes szervezetek egymás között tűzfalakkal védik. A kábelezés fizikai védelme nem megoldott.

Az ORFK szakmai képviseletével továbbá a Nemzeti Elektronikus Információbiztonsági Hatósággal szakmai konzultációk kerültek lefolytatásra a rendőrségi helyi informatika hálózatainak biztonsági osztályba sorolásának tekintetében. Egyértelmű megállapítást nyert, hogy nem kerültek besorolásba, a besorolás körülményei így nem voltak vizsgálhatóak. Ezen hiányosság egy olyan láncolatot vont maga után, mely során nem keletkeztek sem intézkedések, sem előírások így fizikai megvalósulásuk nem volt vizsgálható.

DOKUMENTUM KUTATÁS

A fent megnevezett témaköröket magába foglaló dokumentumok értelmezhető szinten utalásokat tartalmaztak a vizsgálatban érintett rendőrségi informatikai hálózatoknak információbiztonságával kapcsolatosan. Viszont az adminisztratív intézkedések hiánya fizikai intézkedések hiányához vezetett. Annak érdekében, hogy ezen hiányosságokat meg lehessen határozni, tovább kell a fent vizsgált dokumentumok tartalmát és alapjait meghatározó alapozó dokumentumok között kutatni.

Ezek alapján a tovább elemezve, szempontrendszerét meghatározva, elkülönítésre kerül egymástól a stratégiai szempontból fontos normatívák és a szakmai informatikai tárgyú dokumentációk. Ezek alapján a dokumentumok körében éles határ rajzolódik ki a rendőrségi informatikai hálózatok információbiztonsága fölötti szakirányítói szinten keletkezett dokumentumok, a vizsgált rendőrségi informatikai hálózatok információbiztonsági intézkedéseit meghatározó dokumentumok, azokat befolyásoló szakmai dokumentumok között.

A dokumentum kutatás első lépése olyan normatívákat felkutatása, amelyek a rendészeti informatika témakörben érinthetik a vizsgálat témáját. Az alábbi törvényeket és törvényerejű rendeletekben kerültek megvizsgálásra az információ védelem területi vonatkozásai és a hozzákapcsolódó adatvédelemi vonatkozásokat kutatva:

- 2009. évi CLV. tv a minősített adat védelméről,[1]
- 2000. évi IV. törvény az információ biztonságáról szóló, Brüsszelben, 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről,[2]
- 218/2011. a minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól, [3]
- 161/2010. Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, [4]
- 92/2010. Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól, [5]
- 90/2010. Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről, [6]
- Az adatvédelemmel, és az információ védelemmel kapcsolatos normatívák körében:
- 2010. évi CLVII. tv. a nemzeti adatvagyonról, [7]
- 38/2011. Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról, [8]
- 2011. évi CXCVI. tv. a nemzeti vagyonról, [9]
- 2011. évi CXII. tv az információs önrendelkezési jogról és az információszabadságról, [10]
- 2010. évi CLXXXV. tv. a médiaszolgáltatásokról és a tömegkommunikációról, [11]
- 2003. évi C. tv. az elektronikus hírközlésről [12]
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról [13]
- 65/2013. (III.8.) Kormányrendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtási rendeleteként [14]
- a 301/2013. (VII. 29.) Korm. rendelet „a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról” [15]
- 233/2013. (VI. 30.) Korm. rendelet „az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak,

valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről [16]
- 36/2013. (VII. 17.) BM rendelet „a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról" [17]
- 77/2013. (XII. 19.) NFM rendelet az „állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről [18]

A második lépcsőfok, az ágazati szintű informatikai védelmet meghatározó normatívák áttekintése. Ezek közül az alábbiak kerülnek kiemelésre:
- 1277/2010. Korm. határozat a kormányzati informatika konszolidációjához szükséges intézkedésekről, [19]
- 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiájáról, [20]
- 21/2011. BM utasítás a Belügyminisztérium Informatikai Biztonság Politikájáról, [21]
- 94/2009. HM utasítása a honvédelmi tárca információbiztonság politikájáról, [22]
- 8/2009. KHEM utasítás a Közlekedési Hírközlési és Energiaügyi Minisztérium Információbiztonsági Szabályzatáról. [23]

A fent megvizsgált dokumentációk ugyan érintik az informatikai hálózat információbiztonság tárgykörét, összefüggésbe hozhatóak a rendőrséggel, de egyértelműen egyik sem rendelkezik semmilyen meghatározással egyáltalán a rendőrségi informatikai hálózat információbiztonságának követelményrendszerire vonatkozó meghatározásokkal. Viszont mindegyik jól használható a fent feltárt hiányosságok pótlására.

Viszont más szemszögből tekintve a rendőrségi informatikai hálózatok információbiztonsági kérdésire, az elemzett dokumentumokban ha a rendőrséget a Belügyminisztérium ágazati szervezeteként beazonosítjuk, konkrét utalásokat találhatunk a hálózat biztonság területén. Például a 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiája dokumentum IV. Stratégiai fejlesztési irányok 1. Hálózatfejlesztési politika alfejezete élesen megfogalmazza „Törekedni kell a korszerű, virtuális technológiák alkalmazására, melyeket megfelelő adatfeldolgozó hálózat kiépítésével kell alátámasztani. Az informatikai szolgáltatásokat központosított és integrált rendszerekkel kell biztosítani." Mindemellett kitér a fizikai védelmi eszközrendszer létesítésére is „a szervezetek informatikai hálózatán határtűzfalakat kell létesítenie. Ki kell jelölnie a szervezete informatikai hálózatának határát, azon belül minden informatikai védelmet magának kell ellátnia. Olyan egyenszilárdságú hálózatvédelmi eszközöket és saját tulajdonú védelmi eljárásokat kell alkalmaznia, amelyek garantálják a szervezet informatikai hálózatán forgalmazott, tárolt adatok biztonságát."

A fizikai biztonságra nagy hangsúlyt fektetve kiemeli, hogy a „ BM-nek és ágazati szervének szervertermeit az ott tárolt adatok, rendszerek minősítési szintjének megfelelő biztonsági fokozatba kell sorolni és a vonatkozó szabályok szerinti fizikai védelmet kell biztosítani. A biztonsági rés csökkentése és az üzembiztonság növelése érdekében az amortizációs cserék segítségével el kell érni, hogy az informatikai eszközpark egyetlen eleme se legyen 6 évesnél idősebb." [24, 14.o.] Ezen intézkedések körének megjelenése nem volt tapasztalható az első vizsgálat során górcső alá vett dokumentumokban.

A 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiája dokumentum célzottan előírja a dokumentációs rendszer felállítását és kezelését, mely szerint „a BM és ágazati szervei informatikai hálózatának védelme érdekében az informatikai szakterületre kell koncentrálni az elektronikus adatok archiválását, szervezetenként központilag rendezett

címtárak létrehozatalát, kezelését, az informatikai rendszerekhez való hozzáférés nyilvántartás vezetését, az elektronikus és papír alapú másolás, továbbá nyomtatási folyamatok naplózását." [25, 15.o.]

Az elvonatkoztatás alapjait tekintve a helyi hálózatok tekintetében is találunk konkrét meghatározásokat: „a helyi hálózati infrastruktúra konszolidációja során közel 4000 db új UTP CAT5e hálózati végpont kerül létesítésre (a meglévő 5000 db felújítása mellett). A szerverparkok helyi hálózathoz csatlakozása gigabit Ethernet felületen kerül majd biztosításra, az aktív eszközök homogenizálásával és teljes körű cseréjével." [25, 15.o.]

A fenti eredmények tudatában - mely már jól hasznosítható a rendőrségi információbiztonsági dokumentációk továbbfejlesztésében -, át kell tekinteni, azokat a szakmai előírásokat, amelyek alapján a további kutatások lefolytatásra kerülhet és a korábban meghatározott pontokra pontos képet lehet alkotni. Sajnos a fent nevezett időkorlátban nem keletkezett további olyan szakmai irányt mutató anyag mellyel a vizsgálatot a hálózatok információbiztonsági területén lehetett volna folytatni. Ezért a fent említett dokumentumok szakmai forrásai kerülnek felkutatásra, annak érdekében, hogy javaslatot lehessen megfogalmazni az egyéb hiányosságok pótlására. Egyértelmű be lehetett azonosítani azokat nemzetközi és hazai szabványokat, melyeket a rendőrségi informatikai hálózatának biztonsági helyzeti vizsgálatára alkalmazni lehet. Ezek közül az alábbiak kerülnek felhasználásra:

- 2012. évi törvénytervezet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről, [26]
- 25. számú Ajánlása Magyar Informatikai Biztonsági Ajánlások (MIBA), [27]
- 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK), [28]
- 25/1-3. kötet Az Informatikai Biztonság Irányításának Vizsgálata (IBIV), [29]
- 25/1-1. kötet Informatikai Biztonság Irányítási Rendszer (IBIR), [30]
- 25/2. Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS). [31]

A nemzetközi szabványok közül:

- ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványok, [32]
- ISO/IEC 27001:2005. [33]
- továbbá a ISO/IEC 27001:2013[34]

Az alkalmazhatóságuk szempontjából röviden összefoglalásra kerülnek a szabványok fontossága, amelyek a vizsgálat során figyelembe vételre kerültek:

A Miniszterelnöki Hivatal Elektronikuskormányzat-központ megrendelésére elkészült a Magyar Informatikai Biztonsági Ajánlások (MIBA) című ajánlássorozat. A MIBA fő célja, hogy biztonságos informatikai rendszerek kialakítását és fenntartását segítse elő. A nemzetközi szabványokhoz és ajánlásokhoz igazodva a MIBA három fő részből áll:

A Magyar Informatikai Biztonsági Keretrendszer (MIBIK) [35] szervezeti szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBIK a biztonságos informatikai rendszerek irányításáért, menedzseléséért felelős vezetőknek, illetve a szervezet egészére vonatkozó követelmények teljesülését értékelő szakembereknek szól.

Részét képezi az Informatikai Biztonsági Iránymutató Kis Szervezetek Számára (IBIX) [36], ami olyan szervezeteknek nyújt segítséget biztonságos informatikai rendszereik kialakításához, amelyek nem rendelkeznek jelentősebb informatikai rendszerrel, illetve ehhez elkülönült informatikai személyzettel.

A MIBIK az ISO/IEC 27001:2005, ISO/IEC 27002:2005 [37]és az ISO/IEC TR 13335 [38] nemzetközi szabványokon, valamint az irányadó EU és NATO szabályozáson alapul. A MIBIK része az Informatikai Biztonsági Irányítási Rendszer (IBIR)1, amely a szervezet informatikai biztonságának tervezésére, üzemeltetésére, ellenőrzésére és javítására vonatkozik. A MIBIK további részei az Informatikai Biztonság Irányítási Követelményei

(IBIK), amely az informatikai biztonság kezelésének hatékonyabbá tételéhez nyújt segítséget, lehetőséget teremtve a követelmények és feladatok szakmailag egységes kezelésére, illetve az Informatikai Biztonsági Irányításának Vizsgálata (IBIV), amely az informatikai biztonság ellenőrzéséhez ad módszertani segítséget.

A Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS) [39] technológiai szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBÉTS célközönsége az informatikai rendszer kialakításáért, fejlesztéséért felelős vezetők, valamint az informatikai termékek és rendszerek biztonsági értékelését és tanúsítását végző szakemberek köre."[40, 5.o.]

Az informatikai biztonság kérdésével számos szabvány és ajánlás foglakozik. Gyakran hivatkoznak e területen az ITIL1-re [41] és a COBIT2-ra [42]. Az ITIL, „Az informatikaszolgáltatás módszertana" egy az informatika, mint szolgáltatás egészére kiterjedő, nemzetközileg széles körben elfogadott dokumentum. Az ITIL-ben a biztonságirányítás, bár önálló folyamat, amennyire csak lehetséges, integrálódik a többi folyamatba. Az ITIL Biztonságirányítás (Security Management) kötete a BS7799 [43] szabványt használja hivatkozásként, amikor a létező ITIL folyamatokat bővíti a biztonságirányítással. A COBIT az információrendszer ellenőrök egy nemzetközileg is ismert és elfogadott, az informatikai rendszerek szervezéséhez, és különösen az ellenőrzéséhez szükséges irányelveket tartalmazó dokumentum. A biztonság kérdésére nagy hangsúlyt fektet, de részleteiben nem foglalkozik a kérdéssel.

Az ISO/IEC 15408 szabvány (Common Criteria) [44] elsősorban technikai jellegű, főleg az informatikai termékek gyártóinak ad támogatást. Nagyon részletes és megbízható követelményeket, eljárásokat biztosít az informatikai eszközök biztonsági minősítésére. Nem tartalmaz ugyanakkor megfelelően, részletesen kidolgozott követelményeket, az informatikai rendszereket üzemeltető, felhasználó szervezetek számára.

Az informatikai biztonság területén egyre többen használják az ISO/IEC TR 13335 – Guidelines for the Management of Information Security (GMITS) [45] műszaki beszámoló. Az ISO/IEC TR 13335 nem szabvány, annak ellenére, hogy a Nemzetközi Szabványosítási Szervezet és a Nemzetközi Elektrotechnikai Bizottság szabványsorozatának részeként került kiadásra, de „Technical Report"-ként, ami ebben az esetben a megoldási lehetőségek, leírását jelenti, és ezt csak akkor vizsgálják felül, ha az abban foglaltak már nem érvényesek, vagy már nincsenek használatban. Az ISO/IEC TR 13335 öt részből áll:

1. Az informatikai biztonság koncepciója és modellje (Concepts and models for Information Security),
2. Az informatikai biztonság irányítása és tervezése (Managing and planning Information Security),
3. Az informatikai biztonság irányításának megoldásai (Techniques for the Management of Information Security),
4. A védelmi eljárások kiválasztása (Selection of Safeguards),
5. Hálózatbiztonsági megoldások (Safeguards for External Connections).

„Az ISO/IEC 27002:2013 szabvány nem csak azért kiemelt fontosságú, mert a teljes szervezetre vonatkozó, az összes rendszerelem csoportot átölelő informatikai biztonsági követelményeket és védelmi intézkedéseket tartalmazza, de a különböző nemzeti dokumentumok közül ez vált nemzetközi szabvánnyá, és emellett a „de facto" nemzetközi szabvánnyá vált ITIL is ezt használja hivatkozási alapként. Az ISO/IEC 27002 szabványt – bár kritikák is érik – a világ, és különösen az Európai Unió mind több országában fogadják el a különböző szervezetek informatikai rendszerük biztonságának alapjaként. Ezért a jelen követelményeknek ez a nemzetközi szabvány képezze az alapját, az ISO/IEC TR 13335

szabvány, továbbá a NATO (Security within the North Atlantic Treaty Organisation (NATO) – C-M(2002)49) és az Európai Unió (Európai Unió Tanácsának Biztonsági Szabályzata (2001/264/EK) releváns szabályozásai figyelembe vételével."[46., 32.o.]

A dokumentum elemzések a rendőrségi informatikai hálózatok információbiztonságának és védelmének tárgykörében a fenti struktúrában utalások sem közvetlenül sem közvetve nem voltak fellelhetőek.

ÖSSZEGZÉS

Az általam lefolytatott vizsgálat célja a rendőrségi informatikai hálózatai információbiztonsági hátterének feltárása volt.

Az elemzés alá vett informatikai hálózatok információbiztonsági hátterének kutatási eredményei alapján meg lehetett határozni azon rendőrségi informatikai hálózatok információbiztonsági helyzetét.

A dokumentumok vizsgálatával cél volt azon pontokat felkutatni, ahol ráutaló szakmai meghatározásokat találhatunk a rendőrségi informatikai hálózatok információbiztonsági helyzetére vonatkozóan. A kijelölt témaköröket magába foglaló dokumentumok értelmezhető szinten utalásokat tartalmaztak a vizsgálatban érintett rendőrségi informatikai hálózatoknak információbiztonságával kapcsolatosan.

Tekintettel a fentiekre, az elvégzett vizsgálat több irányú, területileg és időben eltolódó elemzéseket jelentett. Az analízisek a rendőrségi informatikai hálózatának nagyságára való tekintettel kerültek végrehajtásra. Elsődlegesen a jelen helyzet elemzése volt a kiindulópont. Ez az elemzés mind a releváns haza szakmai ajánlások, mind a nemzetközi ajánlások figyelembe vételével történt meg. Alapvető dokumentumként került felhasználásra a Rendőrségi Ideiglenes Informatikai Biztonsági Szabályzata, és az ISO/IEC 27001:2005 „A" melléklet 10.6 fejezete, a hálózat információbiztonsági követelmények elemzésekor.

A vizsgálat területe a mintavételezés eredményeképpen korlátozásra került a nagytávolságú és helyi hálózatok biztonsági osztályba sorolásának állapotában, helyzet felmérésében, a szükséges intézkedések meglétében, az érvényben lévő előírások alkalmazhatóságában, fizikai megvalósíthatóságában. Ennek okán a vizsgálat nem terjedt ki a minősített hálózatokra, a zártcélú és nyílt hálózatokra, továbbá a kritikus infrastruktúra elemekre. A kutatási pontok fogalmi szinten kerültek meghatározásra, úgy, mint helyzet felmérés, biztonsági osztályba sorolás vizsgálata, intézkedések megléte, előírások alkalmazhatósága, fizikai megvalósíthatósága.

19 olyan törvény és törvényerejű rendelet került vizsgálat és elemzés alá az információ védelem területi vonatkozásait és a hozzákapcsolódó adatvédelemi vonatkozásokat kutatva, amelyek során a rendőrségi informatikai hálózatának információbiztonsági hátterének kutatása folyt.

Miután ez nem vezetett eredményre így tovább folytatva további 5, az ágazati szintű informatikai védelmet meghatározó normatíva került áttekintésre. Ezek már érintették az informatikai hálózat információbiztonság tárgykörét, összefüggésbe voltak hozhatóak a rendőrséggel. Továbbá pontos meghatározásokat tartalmaztak a hálózat információbiztonsági szintjének emelésére, amely segítséget nyújthat a rendőrségi informatikai hálózat információbiztonságának követelményrendszerinek körvonalazásához. Így a kutatási kört szakmai forrásokra történő bővítésével, 8 nemzetközi és hazai szabványt került beazonosításra.

Az elméleti vizsgálódás mellet a vizsgálatban a gyakorlati megvalósulás is helyt kapott a rendőrségi nagytávolságú informatikai hálózata és kommunikációs hálózatának leírásai. A , helyzetvizsgálat keretében, egyértelmű megállapítást nyert, hogy nem került besorolásba, a besorolás körülményei így nem voltak vizsgálhatóak.

A kutatás során áttekintésre került a rendőrségi lokális (helyi) informatikai hálózatainak leírásait, helyzetvizsgálat keretében, mely során egyértelmű megállapítást nyert, hogy nem került besorolásba, a besorolás körülményei így nem voltak vizsgálhatóak.

Összegezve a fentieket az információbiztonság a stratégiai dokumentumokban előírt követelményekhez képest elmaradottnak tekinthető, mind az adminisztráció, mind az információvédelmi intézkedések területén. Kellő mélységű szabályozottság hiányában nem volt megállapítható a rendőrségi informatikai hálózatnak besorolási szintje. Nem volt fellelhető olyan dokumentáció, mely utalást tett volna a biztonsági besorolására, vagy annak információbiztonsági helyzetére, kockázat elemzésre, kockázat kezelésre, eljárásokra, intézkedésekre. Ez egy olyan sorozatos hiányosságot vont maga után, amely láncolatot épített fel az információbiztonsági előírások, intézkedések, eljárások és fizikai megvalósíthatóságuk nélkülözhetetlenségüknek a bizonyítására. Az egyes vizsgálati pontok által felfedezett hiányosságok ok-okozatot bizonyítottak a következő vizsgálati pontok közötti eredményekben. Viszont szakmai normatívákban egyértelmű utalások és meghatározások voltak beazonosíthatóak, és a rendőrségi informatikai hálózatok információbiztonsági szintjének fejlesztésére használhatóak, feldolgozhatóak. Ezen normatívák segítésével a dokumentációk olyan szintre fejleszthetőek melyek segítségével meghatározhatóak a a rendőrségi informatikai hálózatok a biztonsági osztályba sorolása. Mind emellett a besorolás körülményeinek bővítésével olyan intézkedések és eljárások kidolgozását helyezik kilátásába, melyek az információbiztonsági kockázatok csökkentését vonnák maguk után.

Konklúzió: a vizsgálat tárgyát képező rendszerek információbiztonsága, a biztonsági osztály általi besorolás eredményeképpen meghatározott intézkedések és eljárások láncolati felfűzésének összessége. Mely láncolat megszakadása egyértelmű ok okozatok eredményeit képezik le. Ezek az ok okozati összefüggések az informatikai információbiztonság fenyegetettségét vonják maguk után.

Felhasznált irodalom

[1] 2009. évi CLV. tv a minősített adat védelméről,

[2] 000. évi IV. törvény az információ biztonságáról szóló, Brüsszelben, 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről,

[3] 218/2011. a minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól,

[4] 161/2010. Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól,

[5] 92/2010. Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól,

[6] 90/2010. Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről,

[7] 2010. évi CLVII. tv. a nemzeti adatvagyonról,

[8] 38/2011. Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról,

[9] 2011. évi CXCVI. tv. a nemzeti vagyonról,

[10] 2011. évi CXII. tv az információs önrendelkezési jogról és az információszabadságról,

[11] 2010. évi CLXXXV. tv. a médiaszolgáltatásokról és a tömegkommunikációról,

[12] 2003. évi C. tv. az elektronikus hírközlésről.

[13] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[14] 65/2013. (III.8.) Kormányrendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtási rendeleteként

[15] a 301/2013. (VII. 29.) Korm. rendelet „a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról”

[16] 233/2013. (VI. 30.) Korm. rendelet „az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről

[17] 36/2013. (VII. 17.) BM rendelet „a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról”

[18] 77/2013. (XII. 19.) NFM rendelet az „állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről

[19] 1277/2010. Korm. határozat a kormányzati informatika konszolidációjához szükséges intézkedésekről,

[20] 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiájáról,

[21] 21/2011. BM utasítás a Belügyminisztérium Informatikai Biztonság Politikájáról,

[22] 94/2009. HM utasítása a honvédelmi tárca információbiztonság politikájáról,

[23] 8/2009. KHEM utasítás a Közlekedési Hírközlési és Energiaügyi Minisztérium Információbiztonsági Szabályzatáról.

[24] 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiájáról 14.o.

[25] 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiájáról 15.o.

[26] 2012. évi törvénytervezet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről,

[27] 25. számú Ajánlása Magyar Informatikai Biztonsági Ajánlások (MIBA),

[28] 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK),

[29] 25/1-3. kötet Az Informatikai Biztonság Irányításának Vizsgálata (IBIV),

[30] 25/1-1. kötet Informatikai Biztonság Irányítási Rendszer (IBIR),

[31] 25/2. Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS).

[32] ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványok,

[33] ISO/IEC 27001:2005. szabvány

[34] ISO/IEC 27001:2013. szabvány

[35] Magyar Informatikai Biztonsági Keretrendszer (MIBIK)

[36] Informatikai Biztonsági Iránymutató Kis Szervezetek Számára (IBIX)

[37] ISO/IEC 27002:2005. szabvány

[38] ISO/IEC TR 13335. szabvány

[39] Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS)

[40] 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK) pp. 5-7. 2008.

[41] Information Technology Infrastructure Library (ITIL)

[42] Control Objectives for Information and Related Technology (COBIT)

[43] BS7799

[44] ISO/IEC 15408 (Common Criteria)

[45] ISO/IEC TR 13335 – Guidelines for the Management of Information Security (GMITS)

[46] Dr. Ködmön István, Információbiztonság az ISO27001 tükrében, Hétpecsétes Történetek, Hétpecsét Információbiztonsági Egyesület, Budapest, 2008. pp.39.

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Nagy Dániel
nagy.daniel@operculum.hu

MODERNIZÁLÁS A NATO INFORMATIKAI RENDSZEREIBEN

Absztrakt

A NATO informatikai rendszere, akárcsak bármely információs rendszer, időközönként átalakításra, modernizálásra szorul. Nem csak azért, hogy az új kihívásokat is teljesíteni tudja, hanem azért is, hogy a normál működés a kor színvonalán elvárt minőségben teljesülhessen. 2015-2020 között a NATO hatalmas informatikai megújítási projekten megy keresztül, amely azt célozza, hogy a szolgáltatások egy jól menedzselhető és hatékony privát felhőbe kerüljenek.

NATO's IT systems needs to be updated and modified from time to time, just like any other IT system. The updates enable these systems not only to withstand the challenges of the future, but fulfil today's requirements at an adequate level as well. Between 2015 and 2020 NATO is undergoing an enormous renewal project. The objective of this huge work is to transfer some services into a well manageable and efficient private-cloud.

Kulcsszavak: *NATO, felhőkoncepció ~ NATO, cloud conception*

BEVEZETÉS

Napjaink hadserege elképzelhetetlen modern információ technológiai (IT) eszközök nélkül. Az információs eszközök civil és katonai területen végbement térhódításának köszönhetően a szárazföldi-, tengeri-, légi- és kozmikus hadszíntér mellett létrejött egy új hadszíntér, amelyet információs hadszíntérnek nevezünk.[1] Ezen a hadszíntéren az információ megszerzése, birtoklása és hatékony felhasználása a cél. Mindezek szorosan hozzájárulnak a más hadszíntereken elérhető eredményekhez, sőt kapcsot jelentenek közöttük, és a civil szféra között is. A katonai információs eszközök azonban nem csak harctéri események irányítása illetve annak előkészítése érdekében jönnek létre, hanem attól függetlenül, folyamatosan léteznek, hiszen elengedhetetlenek a hadsereg, illetve a hadseregek szövetségeinek földrajzi korlátokon és országhatárokon átívelő menedzselésére.

KOMMUNIKÁCIÓS RENDSZEREK A NATO-BAN

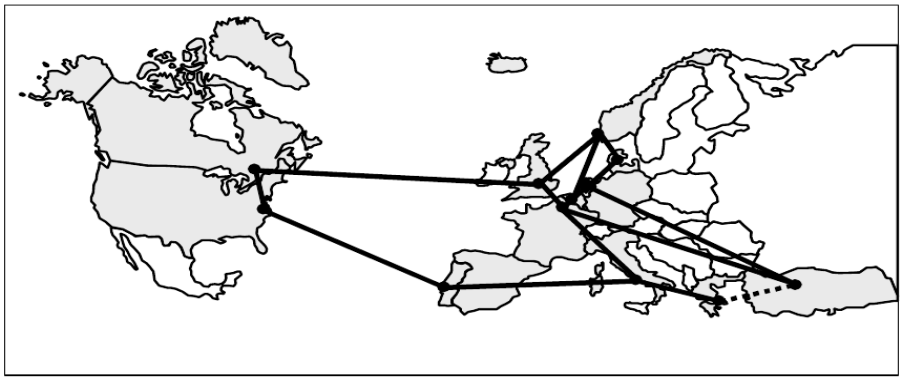
Dr. Munk Sándor ezredes 2006-ban elkészítette Katonai informatika II. című egyetemi jegyzetét [2], amelyben mélyreható részletességgel mutatta be a NATO és tagállamainak katonai

informatikai rendszereit. A mű jó áttekintéssel szolgál a katonai információs eszközök helyzetéről, valamint annak szerepéről 2006-ig.

A NATO legmagasabb értelmezésben NATO C3 rendszerként hivatkozik az informatikai rendszerére, azonban ez a híradással és kommunikációval kapcsolatos eszközökön túlmenően jelentését tekintve "híradó és informatikai rendszerek, érzékelő (szenzor) és riasztási eszközök, navigációs és azonosító rendszerek és ezek létesítményeinek összessége, beleértve NATO szinten egyeztetett eljárásokat, szolgáltatásokat, valamint közös finanszírozású, illetve az ezekkel kapcsolatban álló többnemzetiségű, együttműködő, vagy nemzeti erőforrásokat amelyek szükségesek a NATO C3 funkciók megvalósításához."[2] Fontos kiemelni, hogy ezek a rendszerek a kezdetekben egymástól elszigetelt, majd összekapcsolt, de semmiképp sem kezdetektől fogva centralizált hálózatként elképzelt infrastruktúrák voltak.

Az első újragondolás 1990-ben kezdődött meg. Ebben az időszakban az informatika egyfajta átmeneti időszakban létezett. Túl volt már a kezdeti, a mainframek[1] által jellemzett időszakon, de a mai értelmezésű, hálózatalapú kor, az internet és más hálózatok kezdeti formája miatt még nem jött el. Később a gépek teljesítményének fejlődése lehetővé tette, hogy viszonylag összetett feladatokat futtassanak asztali gépek, így számítási kapacitás miatt már csak speciális esetekben kellett „nagygépek” szolgáltatásait igénybe venni. Az hálózatok összetettsége, és az internet tehát mai szemmel még gyerekcipőben járt, így a rendszerek összekapcsolása sem volt annyira összetett feladat, mint napjainkban.

A NATO különböző rendszereinek egy rendszerbe történő integrálása 1996-ban merült fel [2]. Munk professzor írása szerint ez a tervezet már sok olyan hálózatos alapvetést tartalmazott, amely a ma hálózataiban sincsen másképpen. A rendszert felosztották hálózati erőforrás-tartományra, illetve felhasználói erőforrás-tartományra. A felhasználók, amelyek lehetnek helyhez kötöttek (statikus) vagy mozgók (mobilok), a hálózati erőforrás-tartományban érhettek el szolgáltatásokat illetve adatokat. A kommunikáció egyfelől egy vonalkapcsolt megvalósítás, amely a NATO Alaphálózatra, a nemzeti védelmi hálózatokra, valamint a közös digitális átviteli infrastruktúrára épül. Másfelől egy modernebb csomagkapcsolt megvalósítás NATO Kezdeti Adatátviteli Szolgáltatás[2] néven. Ez utóbbit tizenkét legalább Class II minősítésű kapcsolóközpont működteti, amelyek biztonságos összeköttetést valósítanak meg a tagállamok között.



1. ábra A NIDTS csomópontjai a világban [2]

Kilencvenes évekre jellemző dinamikus informatikai fejlődés, illetve a délszláv válság hatására új felhasználói igények jelentek meg. Létrejött a NATO Általános Kommunikációs

[1] mainframe: Nagygép. A személyi számítógépnél lényegesen nagyobb teljesítményű és rendelkezésre állású számítógép, amelyet intézmények használnak valamilyen szempontból kritikus alkalmazások futtatására.

[2] NATO Kezdeti Adatátviteli Szolgáltatás (NATO Initial Data Transfer Service – NIDTS)

Rendszere (NATO General Communication System, NGCS), amely a kor hálózatára jellemző módon, ISDN[3] alapon nyújtott elsősorban vonalkapcsolt, illetve csomagkapcsolt összeköttetést. Ez már egy szolgáltatás alapú rendszer, amely azt (is) jelenti, hogy a hálózathoz kapcsolódó felhasználók ezen keresztül más hálózatok szolgáltatásait is elérhetik, amely így egyetlen hálózatnak látszik a felhasználó szemszögéből.

A ma telekommunikációs gyakorlatában a vonalkapcsolt hálózatokat csak nagyon speciális esetekben használják. A katonai alkalmazás sem indokolja a mai technológiai szinten a vonalkapcsolt hálózat megtartását, így az NCI[4] a hálózat lecserélésére írt ki tendert 2014. február 25-én, az alábbi tartalommal:

„[...] A projekt célja a jelenlegi elsősorban vonalkapcsolt NATO Általános Kommunikációs Rendszer lecserélése egy teljes mértékben Internet Protocol (IP) alapú hálózattal. A jelenlegi nyílt hangátviteli rendszer helyére - amely automata alközpont alapú[5] -, voice over IP (VoIP) kerül.[6] A modernizált NGCS támogatni fogja a felkészülést az IP alapú kommunikációs szolgáltatásokra, amely jelentősen megnövelt kapacitást, teljesítményt és szolgáltatási minőséget jelent minden statikus és mobil NATO felhasználó számára.[...]”[3]

TÖRTÉNELMI KITEKINTÉS

Sok, az egész világot átformáló technológiai fejlesztés kezdi életciklusát katonai fejlesztésként. Nem ritka, hogy a civil ipar aztán továbbfejleszti a technológiát abban az esetben, ha a katonai vívmánynak gazdasági vonatkozása van a civil életben. Gondolhatunk itt a nukleáris energia felhasználásra csakúgy, mint a globális helymeghatározásra. Az informatika sajátos pozíciója furcsa helyzetet alakított ki ebben a kérdésben. A számítógépek, a mobilkommunikáció, az internet, a hely-alapú szolgáltatások olyan mértékben váltak életünk részévé, hogy a világ meghatározó iparága lett az, amely ezeket a fejlesztéseket szolgáltatja. Nincs az a katonai fejlesztés, amely fel vehetné a versenyt azoknak a cégeknek a tapasztalataival, akik milliárdok számára gyártanak mobiltelefont, hálózzák be a világot bázisállomások építésével vagy éppen optikai kábeleket húznak tízezer kilométer szám a tengerek, óceánok alatt. A leírtak nem csak a technikára, hanem best practice-ekre[7], folyamatokra, paradigmákra is igaz.

Az egyik ilyen talán már paradigmának is nevezhető, de lényegét tekintve műszaki megvalósítás a felhőszolgáltatás[8]. Annak megértéséhez, hogy mi a felhőszolgáltatás, illetve miként kerül a lentebb részletezett módon a NATO látókörébe, tekintsük át röviden a számítástechnika történelmének egy szűk szeletét.

A számítógépek hőskorában, a személyi számítógépek megjelenése előtt, 1960-1970-es évek körül, a számítógépek igen drágák voltak, ezért kevés is volt belőlük intézményenként

---

[3] ISDN: Integrated Services Digital Network, digitális szolgáltatásokat is nyújtani képes szolgáltatás, illetve annak hálózata.

[4] NATO Communications and Information (NCI) Agency: NATO Kommunikációs és Információs Ügynökség. 2012. július 1-én alakult, az alábbi szervezetek összevonásával: NATO Consultation, Command and Control Agency (NC3A), NATO ACCS Management Agency (NACMA), NATO Communication and Information Systems Services Agency (NCSA), ALTBMD Programme Office valamint a NATO HQ ICTM egyes részei. (https://www.ncia.nato.int)

[5] eredeti szövegben: Private Automatic Branch Exchange (PABX)

[6] VoIP: Voice Over Internet Protocol, IP alapú hálózaton történő hangátvitel szolgáltatás.

[7] best practice: Legjobb gyakorlat, valamilyen tevékenység hosszas művelése folyamán felgyúlt, a praktikumba illeszthető tapasztalat.

[8] felhőszolgáltatás: Gyakran angolul hivatkoznak rá, cloud service-ként.

néhány. Ezekhez a nagygépekhez[4] terminálokon keresztül volt lehetséges kapcsolódni, ami azt jelentette, hogy a felhasználók egy „buta számítógép” segítségével adták be az adatokat a nagyszámítógépnek végrehajtásra, illetve ezen a terminálon keresztül tekintették meg az eredményt. Egy nagygéphez több terminál is csatlakozhatott és akár időosztásban a nagygép egyszerre több terminál által beadott programot is futtathatott. A hetvenes évek végére megjelentek, a nyolcvanas években pedig egyértelműen meghódították a világot a személyi számítógépek. Ezek lényegesen kisebbek, olcsóbbak, egyszóval elérhetőbbek lettek mint a nagyszámítógépek, és nem utolsó sorban a félvezető-technika fejlődésével hamar tekintélyes számítási teljesítményt nyújtottak a kis dobozban. Ez a tendencia oda vezetett, hogy a nagyszámítógépek kezdtek eltűnni, mert a feladatok túlnyomó részét személyi számítógépen is el lehetett végezni. Egyre kevesebb olyan feladat került elő, amihez valóban egy személyi számítógép teljesítményét sokszorosan meghaladó kapacitásra volt szükség. A világra ha nem is izoláltan, de egymás működésére kevéssé utalt számítógépek jellemezték az otthonokban és az intézményekben egyaránt. Otthon mindenki a saját gépén futtatott szövegszerkesztőt, az intézményekben pedig asztali gépükön futtatták a tervezőprogramot vagy a szimulációt a mérnökök.

A helyzeten az internet bámulatos fejlődése változtatott, amikor szükségessé váltak olyan gépek, amelyek költséghatékonyan és elsősorban megbízhatóan kezelnek olyan adatokat, amelyeket sokan akarnak elérni. Gondoljunk a web térhódítására vagy ez e-kereskedelemhez kapcsolódó szolgáltatásokra és fizetésekre. Napjainkban a mobil-kommunikáció és mobil-számítástechnika fejlődését éljük meg. Ma már nem azért fordulunk az interneten keresztül elérhető szolgáltatásokhoz, mert a zsebünkben elférő számítógép ne lenne képes számítási teljesítményével szolgálatunkra lenni, hanem azért, mert az internet térhódítása a számunkra érdekes adatok súlypontját a saját gépünkön kívül helyezte, illetve egyszerűen így kényelmesebb és nem utolsó sorban biztonságosabb. Nem azért használjuk például a Google Docs szolgáltatását, mert a személyi számítógépünknek nehezére esne egy szövegszerkesztőt futtatni, hanem azért, mert így ugyanazt a dokumentumot akár egyszerre többen is szerkeszthetik, azonnal mindenhol elérhető, illetve az asztali, vagy zsebben hordott számítógép háttértáránál nagyságrendekkel biztonságosabb környezetben tárolódik a fájlunk. Ma tehát az adatok tárolása és azokhoz kapcsolódó szolgáltatások erőteljesen tolódnak át cégek által üzemeltetett nagyteljesítményű szerverparkokba. Ezt a jelenséget, illetve szolgáltatást hívják felhőalapú szolgáltatásoknak.

Az alábbiakban ismertetett projekt a NATO rendszerének privát felhő[9] szolgáltatásba történő áthelyezését irányozza elő. A dokumentumból kiolvasható, hogy a NATO éppen azon indíttatásból és céllal döntött a felhő alapú megoldás mellett, ami miatt a civil életben is nagy teret hódít magának ez a megvalósítás.

A NATO ELSŐ LÉPÉSE A FELHŐSZOLGÁLTATÁSOK FELÉ

„A NATO első lépése a felhőszolgáltatások felé: áttekintés és üzleti hajtóerő” címmel adott ki az NCI Ügynökség 2014. augusztus 31-i keltezéssel egy cikket[5], amelyben részletezi a címben előrevetített felvetést. Az alábbiakban ennek a cikknek általam fontosnak, és a fentebb leírtak tükrében érdekesnek talált olvasatát közlöm.

[9] privát felhő: Olyan felhőszolgáltatás, amelyben a felhőt használó vállalkozás (vagy személy) üzemelteti magát a felhőszolgáltatást is. Katonai rendszerek érzékenysége miatt ezek nem bízhatók harmadik félre, maga a hadsereg kell, hogy létrehozza és fenntartsa a felhőszolgáltatást.

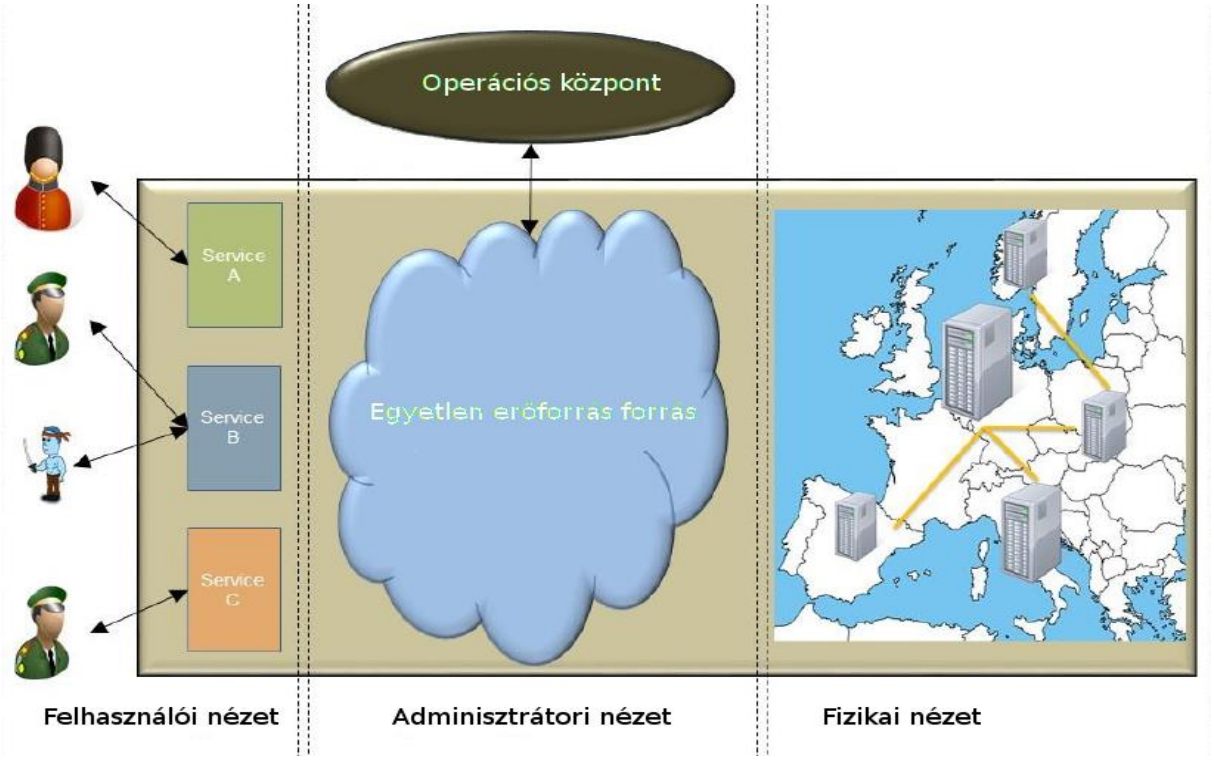
Miután 2012-ben az NCI rendelkezésébe és felelősségébe kerültek a NATO informatikai erőforrásai, a kezdeti tanulmányok arra irányultak, hogy megállapítsák, miként használják ezen erőforrásokat, mik lehetnek a problémák, és mit lehet tenni annak érdekében, hogy ezeket a problémákat megszüntessék. A tanulmány egyik eredménye azt lett, hogy a NATO erőforrásait lényegesen nagyobb ráfordítással üzemeltetik, mint az indokolt volt. Ezt követően meghirdetésre került az IT Modernizációs (ITM) program, amelynek célja a legtöbb erőforrás lecserélése, modernizálása és az azokat üzemeltető szükséges munkaerő csökkentése. Az IT Modernizáció program teljes egészében átalakítja a NATO által nyújtott szolgáltatások módját. A jelenleg lokálisan nyújtott szolgáltatásokat leváltják globálisan összefogott módon nyújtott szolgáltatások. Ez a NATO első lépése a felhőalapú szolgáltatás irányába.

Írásom első felében Munk professzor munkája alapján röviden bemutattam, miként fejlődött a NATO informatikai rendszere az idők során. Az NCI tanulmányban olvasottak megerősítik ezt, kitérnek arra, hogy a NATO rendszerei a mindenkori igényekre választ adva, lépésről-lépésre fejlődtek a mai szintre. A fejlesztéseket különféle nemzetek menedzselték, különféle igények alapján és különféle forrásokra alapozva. A források és a fejlesztési projektek szerteágazott volta oda vezetett, hogy a jelen infrastruktúrájában egyebek mellett nagy eltérések mutatkoznak a technikai megoldásokban, az IT szolgáltatások menedzsmentjében és a szolgáltatási szintek definíciójában. A problémát súlyosbítja, hogy az egyes szituációk felmerülésekor azokat nem egészében, a rendszerben betöltött szerepével együtt vizsgálták, hanem izoláltan, arra lokális megoldást keresve. Tették ezt azért, hogy az implementációs rizikót a függőségek számával együtt csökkentsék. Annak ellenére, hogy egyes helyeken történtek lépések a helyzet javítására, a mai helyzetet az jellemzi, hogy sok esetben változatos műszaki megoldások találhatók, akár még telephelyen belül is. Ennek eredményeként az infrastruktúra lokális fókuszú, heterogén, nehéz, költséges fenntartani és rugalmatlan. Sok helyen különféle hardverrel, szoftverrel, szolgáltatásokkal és folyamatokkal találkozunk.

A lokális fókuszú megközelítés egyik hatása, hogy a hardver egy bizonyos szolgáltatáshoz kötött, és kihasználtsága alacsony. A 2012 augusztusában készült felmérés átlagosan 9% hardver kihasználtságot mutatott, de ugyanakkor rámutatott arra is, hogy a szabad kapacitást nem lehet más, esetleg erőforrás híján lévő szolgáltatások támogatására fordítani. Történik mindez elavuló hardver- és szoftvereszközökkel, amelyek üzemeltetése költséges. A felmérés szerint a hardverek 65%-a már lejárt támogatású. A felvázolt helyzet azt is jelenti, hogy vészhelyreállítás is csak lokális módon tud megtörténni, azaz a mentések telephelyen belül vannak, a helyszínek nem tudják egymás támogatni ebben a tekintetben. Komoly katasztrófa esemény bekövetkeztekor (pl. szerverterem-tűz) nem világos, hogy a telephely hogyan és mennyi idő alatt tudja visszaállítani működőképességét. Harmadrészt a jelenlegi helyzet az információbiztonság területén is kérdéseket állít, hiszen a sokféle szoftver, sokféle verziójának naprakészségét és megfelelő védelmi szintjét garantálni problémás.

Az IT Modernizáció program zászlójára tehát a felhő-alapú szolgáltatást írták. Lássuk, milyen válaszokkal szolgál a fenti kérdésekre ez a megoldás. Alapvetően a rendszert úgy kell átalakítani, hogy az gyakorlatilag, globálisan egy vállalkozásnak látszódjon, amely a különféle telephelyek és felhasználók számára szolgáltatásokat nyújt. A központi menedzsment egyik eredménye lesz, hogy a költségek is központosítottan kezelhetőek és követhetők, így nagyobb teret adva az optimalizálásnak. Az egyik legfontosabb tényező az erőforrások elosztottságának biztosítása. A múlt gyakorlatában a telephelyek a legrosszabb forgatókönyv szerint becsülték meg az erőforrásigényeiket, arra még biztonsági tartalékot is húzva. Többek között ez vezettet a jelenlegi 9%-os átlagos kihasználtsághoz. A fennmaradó több mint 90% kapacitással nem lehet mit kezdeni, még akkor sem, ha létezik olyan telephely, amely éppen erőforrás szűkében van valamilyen oknál fogva. A felhő alapú szolgáltatás drámaian képes növelni az

erőforrás kihasználtságát. Nem csak arról van szó, hogy a váratlan terhelés csúcsokat más, kevéssé kihasznált szerverek átvehetik, hanem arról, hogy az egész rendszert egy új szemléletben lehet tervezni. A legtöbb lokális rendszer kapacitás kihasználtsága soha nem lehet optimális, ha másért nem azért, mert az emberek általában 8 órát dolgoznak egy nap. 24 órában 16-ból a rendszer lényegesen alacsonyabb terheléssel fut. Ha egy globális szolgáltatás a terhelés megosztására képes, akkor a terhelést például az időzónák figyelembevételével lehet és kell kialakítani. Így az Egyesült Államok és, Európa egyes részei használhatják ugyanazt a rendszert, úgy, hogy annak kapacitását nem kettejük összegére, hanem a legnagyobb terhelést jelentő régióra kell méretezni. A rendszer 24 órában közel teljes kihasználtsággal működhet azáltal, hogy mindig más régiót szolgál ki. Ezt a modellt használja minden globális szolgáltató, mint az Amazon vagy a Google, hiszen biztosítani tudják, hogy a mindenkori erőforrásigény csak töredéke annak, amit az összes felhasználó összege jelentene.



2. ábra A felhőszolgáltatás három nézete [5] (Magyarra átdolgozta a szerző)

A felhasználót általában nem érdekli, hogy hol van az a szerver, amelynek szolgáltatását igénybe veszi, illetve milyen műszaki háttéren keresztül jut hozzá. Ő az asztali számítógépével, a hálózaton keresztül bejelentkezik a felhőbe, amely aztán kiszolgálja. Hasonlóképpen, a felhasználókkal és szolgáltatásokkal foglalkozó adminisztrátorok sem kell, hogy ismerjék az infrastrukturális részleteket, ők jogosultságokat osztanak, hozzáféréseket intéznek, illetve jelzik, ha erőforrás problémát látnak. Mindez azért válik lehetővé, mert a háttérben egy robusztus, rugalmas, bővíthető, globálisan elosztott rendszer nyújt egy átfogó infrastruktúrát.

Az átalakítás magában foglalja a NATO Parancsnoki Struktúrát (NCS)[10] az NHQ-t[11] és NATO ügynökségeket. Információbiztonság tekintetében három szintről beszélhetünk: NS[12]

[10] NCS - NATO Command Structure

[11] NHQ - NATO HQ - NATO Főparancsnokság

[12] NS - NATO Secret - titkos NATO hálózat

azaz titkosított, NR[13] azaz korlátozott hozzáférésű, valamint a publikus mindenki számára elérhető rendszereket. További felosztás lehetséges a rendszerek felhasználás módja tekintetében: A műveleti hálózat (ON)[14], amely NS rendszerszintig nyújt szolgáltatásokat, illetve a védett üzleti hálózat (PBN)[15,] amely pedig az NR szintig, beleértve az internet hozzáférést is. Az internet elérése egy külön projekt keretében kerül megvalósításra, amelyet PIA[16] átjárónak neveznek. A PBN az a hálózat, amely összekapcsolja, és egy hálózattá forrasztja a sokféle NU[17] és NR tartományokat, amely így lényegesen javítja az információ-cserét. Ez a hálózat jelent csatlakozási pontot az NS rendszerekkel is.

A felhőszolgáltatások körül kérdőjelek sorakozhatnak azonban azok rendelkezésre állását, biztonságát és bizalmasságát illetően. Egy publikus felhő felhasználónak nem csak a felhőszolgáltatást nyújtóban (például Gmail szolgáltatás esetében a Google-ben) kell megbíznia, hanem az infrastruktúrában is, amely számára lehetővé teszik a szolgáltatás elérését és használatát. Ezek olyan kérdések, amelyek katonai alkalmazások tekintetében csak a privát felhőszolgáltatás alkalmazását teszik lehetővé minden NU besorolási szint fölé eső információ és szolgáltatás tekintetében. Mindez azt is jelenti, hogy a NATO számára a felhőszolgáltatások, és elsősorban azok publikus oldalainak kihasználása problémás. Ahogyan írtam nem csak magára a felhőszolgáltatást nyújtó szerverparkra és annak üzemeltetésére kell gondolni, hanem az elérést lehetővé tevő infrastruktúrára is. A Földünket behálózó és lefedő vezetékes és vezeték nélküli hálózat döbbenetes mértékben fejlődött az utóbbi években, ezek használata katonai kommunikáció tekintetében is nagy jelentőségű. Ha információbiztonsági tekintetben használatuk alkalmassá is teszik őket titkosított kommunikációra, rendelkezésre állásuk, változó kapacitásuk már vetnek fel kételyeket. Mindezek ellenére a NATO számára sem lesz más út, mint a publikus infrastruktúrák és szolgáltatások katonai alkalmazhatóságát megtalálni. A NCI tanulmánya szerint ez 3-8 év alatt fog végbe menni.

Itt meg kell említeni egy új koncepciót, a hibrid felhő lehetőségét. Ebben az esetben a kiépített privát felhő rendszer mellett, bizonyos feladatokra publikus felhőszolgáltatások is igénybe vehetők. Ennek a megoldásnak óriási a jelentősége olyan helyzetekben, amikor nemzetközi kommunikációban a kommunikáció azonos besorolású szinten kell, hogy megvalósuljon. Az afganisztáni műveletek során a NATO nyújtott sok olyan szolgáltatást, amelyet aztán a tagállamok használtak. A NATO közösen végezte el ezeket a beruházásokat és fejlesztéseket, ami azt is jelentette, hogy ezeket a beruházásokat és fejlesztéseket a tagállamoknak nem kellett egyenként megvalósítania. Ez a felhő ügynök[18] koncepció. A jövő rendszereiben a NATO felhő ügynökként közvetíthet szolgáltatásokat ezen szolgáltatásokat lehetővé tevő államok és cégek között, legyen az NATO-n belüli vagy NATO-n kívüli. A koncepció valamennyire hasonlatos a nagy cégek és azok beszállítóinak viszonyára. Független attól, hogy hány száz vagy ezer, ismert vagy ismeretlen beszállítóval operál egy autógyártó, a márka nyújt garanciát a jármű minőségének egészére. Ezt a koncepciót még részletezni és fejleszteni kell, de az internet fejlődését és egyáltalán az infokommunikáció fejlődésének irányát tekintetbe véve ez nem csak lehetséges, de szükséges irány is.

[13] NR - NATO Restriced - korlátozott hozzáférésű NATO hálózat

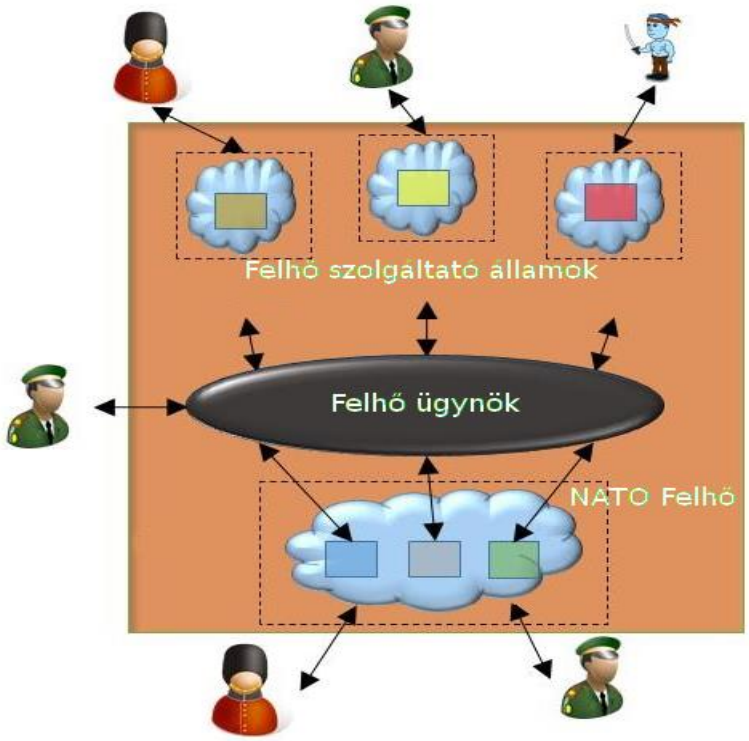
[14] ON - Operational Network – Műveleti hálózat

[15] PBN - Protected Business Network

[16] PIA - Public Internet Access, publikus internet elérés

[17] NU - NATO Unclassified, nem titkos, mindenki számára szabad hozzáférésű dokumentum

[18] angolban: cloud broker



3. ábra A felhő ügynök koncepcióját szemléltető ábra [5] (Magyarra átdolgozta a szerző)

A technikai megvalósítással kapcsolatban elmondható, hogy három adatközpontot (EDC) hoznak létre[19], valamint a különféle helyszínekre alap- és kiemelt[20] csomópontok kerülnek. Az alap csomópontok lokálisan csak minimális tároló illetve számítási kapacitást nyújtanak, feladatuk elsősorban a felhőhöz való szinkronizálás, míg a kiemelt szerverek ennél magasabb kapacitást nyújtanak a lokális felhasználásoknak, rugalmassági okokból, illetve azoknak az alkalmazásoknak, amelyek még nem alkalmasak az új architektúra kezelésére. Ilyenformán a vészhelyreállítás központilag kerül kezelésre, minden adatot három külön fizikai területen tárolva. A három adatközpont Monsban, Brüsszelben illetve az olaszországi Lago Patriában kerül telepítésre. A rendszer központja (OpsCen)[21] Monsban lesz, illetve egy másik, tartalékként szolgáló még meg nem határozott helyszínen a Benelux államokban. Ez említett három adatközpont már meglévő NATO csomópontok modernizálásával jön létre. A három adatközpont látja el az összes NATO felhőszolgáltatást és végzi a mentéseket. Minden mentés mindhárom csomópontra tükrözve lesz, így katasztrófa esetben a visszaállás biztonságos és kiszámítható módon fog történni.

A számítások szerint a projekt végére a jelenlegi szolgáltatások 80%-a felhő-alapúvá válik, a maradék 20% nem alkalmas arra, hogy ilyen módon működjön. Ezek az alkalmazások továbbra is lokális módon működnek majd. Egy későbbi fázisban a cél a 100%-os felhő-alapú megvalósítás.

Bár az így átalakított rendszer jelentős megtakarítást hoz majd az üzemeltetési költségek tekintetében, a hajtóereje mégsem elsősorban gazdasági alapú. A cikk kiemeli, hogy a NATO rendszerei már elavultak, így azok cseréje időszerű, sőt azokra már források is vannak. Így az

[19] Enterpsire Data Centres (EDC)
[20] Standard Node (SN), Enhanced Node (EN)
[21] OpsCen: Operations Centre műveleti központ

IT Modernizációs projekt nem igényel új forrásokat, hanem a jelenlegiek ésszerűbb és korszerűbb kihasználást célozza. Másfelől a jelenlegi IT rendszerek fenntartására egyszerűen túl sok munkaerőt kell alkalmazni, ami nem fenntartható.

A projekt 2015-ben indult és ötéves átfutással terveztek. Négy lépésben történik a megvalósítás, amelyet hullámoknak neveznek. Először létrehoznak a három adatközpontból kettőt, illetve az operációs központot és tartalék állomását. Lecserélik a hardvert azokon a csomópontokon, amelyeknek erre a legnagyobb szükségük van. A tenderkiírás 2014-ben történt, ennek feldolgozása és a szerződések elkészülte után, 2016 elején kezdődhet meg az implementáció. Ilyenformán a két első adatközpont 2017 elejére készül el. Ezután a csomópontok lecserélése történik, olyan sorrendben, ahogyan azok elavultsága azt diktálja. Az ezt követő hullámok egy-egy évesek lesznek, és folyamatosan megtörténik a helyszínek felhőbe integrálása. A harmadik adatközpontot a harmadik hullámban alakítják ki 2016 végén. A teljes projekt lezárását 2020-ra tervezték.

ÖSSZEGZÉS

A felhő alapú szolgáltatások az informatika legújabb kori vívmányai közé sorolhatók, amelyek különösen a mobil eszközök térhódításával hatalmas ütemben fejlődnek. Írásom első felében röviden vázoltam a NATO informatikai rendszereit. Ezt követően egy kis történelmi kitérővel rávilágítottam azokhoz a mérföldkövekhez, amelyek a szerver-kliens alapú architektúrát az elmúlt évtizedekben formálták. Az utolsó fejezetben pedig egy nemrégiben az NCI által publikált ambiciózus tervet ismertettem, amely a NATO információs rendszerét célozza privát felhőbe helyezni 2020-ig bezárólag.

A NCI által kiadott cikk legnagyobb tanulsága meglátásom szerint, hogy a katonai és civil infokommunikációs rendszerek napjainkban nem csak a használt technikai eszközök terén mutatnak erős konvergenciát, hanem a hadsereg illetve esetünkben a NATO olyan koncepció használatát veszi át, amely a civil életben már bizonyított és bevált. A hadsereg és a civil szféra kommunikáció és az informatikai rendszerekkel szembeni elvárásai túlnyomó részt megegyeznek, a civil szféra azonban, a felhasználók hatalmas számát tekintve gyakorlati, tapasztalati előnyben van. A NATO által indított ITM projekt informatikai szemmel, helyesebben azoknak a cégóriásoknak a szemével nézve, akik ezen projektet megvalósítják, „csak” egy nagy, üzleti rendszer megvalósítását jelenti a hadsereg, mint megbízó speciális igényeinek figyelembe vételével.

Felhasznált irodalom

[1] Haig Zs., Kovács L., Ványa L., Vass S.: Elektronikai hadviselés. NKE, Budapest, (2014)

[2] Dr. Munk Sándor: KATONAI INFORMATIKA II. Katonai informatikai rendszerek, alkalmazások. ZMNE jegyzet, Budapest, (2006).

[3] NCI Agency: Notification of Intent to Call for Bids (IFB-CO-13735-NCI), (2014).

[4] Wikipedia: Mainframe computer. Wikipedia [Online] http://en.wikipedia.org/wiki/Mainframe_computer (2015.01.05.)

[5] Peter J. Lenk: NATO’s First Step to the Cloud: Overview and Business Drivers https://www.ncia.nato.int/it-modernization/PublishingImages/Pages/default/WP1%20-%20One%20Small%20Step.pdf (2016.05.05.)

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Sági Gábor
gabor.sagi@yahoo.com

MEGVÉDHETŐEK-E A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK?

Absztrakt

A kritikus informatikai infrastruktúrák egyre nagyobb szerepet töltenek be mindennapi életünkben. Az újonnan felmerült igények megvalósítása miatt az infrastruktúrák komplexitása, integráltsága egyre nagyobb méreteket ölt. A kor követelményeinek való megfelelés érdekében a korábban zárt hálózatok fokozatosan megnyíltak először csak az adott vállalt belső informatikai hálózata felé, később - sok esetben - az internet felé is. Az architektúra nyílttá válása, a komplexitás növekedése magával hozta az infrastruktúrák fenyegetettségének növekedését és újszerű támadási technikák kialakulását, alkalmazhatóságát is. Napjainkban a legjelentősebb kihívást az olyan – sok esetben hosszabb előkészítést és végrehajtást igénylő – támadások jelentik, amelyek célzottan egy információs infrastruktúra, vállalat, kormányzati szerv ellen irányul. A megfelelő védelem kialakítása nehezíti, hogy sok esetben a támadás a korábbi tapasztalatoktól, ismerté vált eseménysorozattól eltérő módon kerül végrehajtásra, azaz nem ismert a fenyegetés karakterisztikája, és így a jelenlegi védelmi megoldások nem vagy csak korlátozottan alkalmasak ezen események észlelésére, kezelésére. A szerző a cikkben bemutatja, hogy információbiztonsági szempontból milyen nehézségeket hozott az informatikai infrastruktúrák fejlődése, milyen támadási vektorokkal kell számolni a védelem kialakítása során, illetve milyen nehézségekkel kell számolni, milyen kockázatot jelenthet egy képzett támadó, milyen veszélyt hordozhatnak a védelemre hivatott műszaki megoldások.

Critical information infrastructures play an increasingly important role in our daily lives. Due to the implementation of the new needs the infrastructures are becoming more complex, integrate. In order to meet the requirements of the nowadays, the previously closed networks gradually opened for the first time only to the internal network of a company's information technology, in many cases even later into the Internet. The increase in complexity brought increase of threats of infrastructures and appear new attack techniques. Today, the biggest challenge is - in many cases a longer preparation and implementation require - are the attacks that are directed specifically to an information infrastructure of company, government agency against. Developing good protection is complicated by the fact that in many cases the attack is carried out without past experience or known events, different way, ie not known to the threat characteristics, and so the current security solutions are not only limited use of these events to detect, defend. The author of the article shows from information security point of view,

what kind of difficulties for the development of the IT infrastructure, which attack vector can be expected in the development of protection, and what problems have been encountered, which kind of risks are carried by a skilled attacker, what kind of risks are carried by the protection of technical solutions.

Kulcsszavak: *kritikus információs infrastruktúrák védelme, fenyegetések, védelmi nehézségek ~- critical information infrastructure protection, threats, protection difficulties*

BEVEZETÉS

Az információs rendszerek használatának széles körű elterjedése, az információs rendszereket használók igényeinek változása, az információs rendszerekkel szemben támasztott – a korábbi funkcióktól eltérő igények szükségessé tettek új típusú rendszerek kifejlesztését, meglévő rendszerek továbbfejlesztését, amelyek a kor követelményeinek megfelelőin ki tudják szolgálni a megrendelők, felhasználók igényeit. Megnőtt az igény a rendszerek integrációjára, távolról történő menedzselésére, újfajta architektúrák (pl.: internet, web2, mobil eszközök, cloud) használatára, újfajta szolgáltatások (pl. mobil alkalmazások, netbank, BYOD, smart home, smart city, Internet of Things, vezető nélküli autó) igénybevételére. Az új szolgáltatások ugyanakkor korábban nem tapasztalt módon növelték az rendszerek komplexitását, s az egymással együttműködő rendszerek sebezhetőségét, illetve jelentősen nőtt a motiváció az információs infrastruktúrákból való információszerzésre, a rendszer működésének zavarására.

Az információs társadalom zavartalan működésének megbontására irányuló támadások tényleges célpontjai a kritikus infrastruktúrák - hiszen ezek adják működésének alapját -, azonban az ellenük irányuló információalapú támadások és fenyegetések a különböző szintű és fontosságú infokommunikációs rendszereket érintik. Ezek a rendszerek mára a fenyegetések stratégiai célpontjaivá váltak.[1]

Számos olyan kritikus infrastruktúránk van, amely sérülékeny információs (informatikai) rendszereket használ. Ezáltal a kritikus infrastruktúrák egyik legkritikusabb része maga az infrastruktúrát irányító, vagy az azt ellenőrző és vezérlő információs rendszer. [2]

Mind a hazai, mind a nemzetközi szakirodalomban számos szerző foglalkozik az információs infrastruktúrák védelmi kérdéseivel. Hazai vonatkozásban kiemelkedő a 2014-ben megjelent „Kritikus infrastruktúrák és kritikus információs infrastruktúrák” című tanulmány, amely részletesen taglalja a kritikus információs infrastruktúrák helyét szerepét a mindennapi életben, az infrastruktúrák támadási vektorait, valamint a lehetséges védelmi megoldásokat. A tanulmány részletesen bemutatja a kritikus információs infrastruktúrák civil és katonai vonatkozásait, valamint bemutatja a környező országok, az Egyesült Államok, Európai Unió és a NATO kritikus infrastruktúrákkal kapcsolatos tevékenységét, a tevékenységben résztvevő szervezetek szerepét, szabályozói környezetet. Ugyanakkor az elmúlt évben számos új fenyegetettség forrás, illetve védelmi megoldás látott napvilágot, amelyek lassan mindennapjaink részévé vállnak. A hazai szakirodalomban kevés cikk foglalkozik továbbá a már széles körben elterjedt védelmi megoldások, illetve a régi és az új védelmi megoldások hordozta kockázatokkal.

Jelen írás kívánja felhívni a figyelmet arra, hogy a jelenleg alkalmazott információvédelmi megoldások milyen kockázatokat hordoznak, az új védelmi elgondolások bevezetése során milyen új kockázatokkal kell számolni, illetve milyen nehézségekkel kell számolni a védelem működtetése során.

KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELME

Kritikus információ rendszerek, információk védelmének elve

Az információnak a tudásalapú információs társadalomban kitüntetett szerepe van. Az információs társadalom működése az információk és az az információs rendszerek támadásán keresztül jelentősen befolyásolható, károsítható, hatékonysága csökkenthető.[3]

A kritikus információs rendszerek megbízható működése, az információs rendszerekben kezelt információk a szervezetek számára a legfőbb értékek egyike, a hosszabb távon fenntartható fejlődés egyik legfontosabb alapja. Hatékonyan és biztonságosan működő

információs rendszer nélkül egy szervezet sem képes ellátni feladatát, nem képes megfelelni a tulajdonosi, irányító és szabályzói elvárásoknak.

A szervezet információs rendszerekkel szembeni folyamatosan növekvő kitettségének hatására az információs rendszerek és az azokban kezelt információk, a rendszerek által irányított folyamatok egyre kiemeltebb szerepet töltenek be a szervezet életében, olyannyira, hogy napjainkban számos ágazatban megfelelő szinten működő információs rendszerek nélkül elképzelhetetlen a működés. A kitettség növekedése magával hozta az igényt, hogy a szervezet által üzemeltetett, igénybe vett rendszereket egyre magasabb színvonalon kell védeni a nem kívánt, nem várt eseményekkel szemben.

A belső elvárások mellett ugyanakkor „társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme” [4]. Ahol:

- Bizalmasság: az adat tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
- Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség) és a származás megtörténtének bizonyosságát (letagadhatatlanság) is, illetve a rendszerelem tulajdonsága, amely arra vonatkozik, hogy a rendszerelem rendeltetésének megfelelően használható.
- Rendelkezésre állás: az adat, illetve az informatikai rendszer elemeinek tulajdonsága, amely arra vonatkozik, hogy az arra jogosultak által a szükséges időben és időtartamra használható.

A bizalmasság (ang.: confidentiality), a sértetlenség (ang.: integrity) és a rendelkezésre állás (ang.: availability) hármasát szokták az angol kezdőbetűik alapján CIA-elvnek nevezni. [5]

A hazai szabályozásban, illetve nemzetközi szabványokban a hitelesség és a letagadhatatlanság nem minden esetben jelenik meg különálló követelményként, hanem része a sértetlenség követelményének.

A fentiek alapján a biztonság a rendszer olyan – az érintett számára kielégítő – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. [6]

A kockázatarányos védelem kialakítása során figyelembe kell venni a kezelt információk minősítését. Az adatminősítés jelenlegi rendjét figyelembe véve, a komplex információbiztonság szempontjából – a tárolt adatok minősítésétől függően – a vállalatoknál, intézményeknél, kormányzati és védelmi célú szervezeteknél biztonsági osztályokat kell kialakítani. [7]

Fontos megjegyezni azonban, hogy a kritikus információs infrastruktúrák védelmét szorosan koordinálni kell magával a kritikus infrastruktúrák védelemmel. [8]

Információs infrastruktúrák kialakulásának sajátosságai információbiztonsági aspektusból

A szervezetek megalakulása során ritkán adatik meg, hogy egy szervezet már induláskor tudatosan alakítsa ki információs rendszerét, információbiztonsági megoldásait. Ennek oka részben, hogy a szervezet indításakor – értelemszerűen – nem lehetnek meg azok a tervek, amelyek a szervezett hosszú távú céljait, feladatait tartalmaznák, s amelyből tervezetten ki lehet alakítani egy egységes információs rendszert, továbbá egy induló vállalkozás esetén általában nincsenek meg az egységes információs rendszer kialakításához szükséges emberi

és pénzügyi erőforrások sem. A szervezet fejlődése során jellemzően – főleg a kezdeti időben - egy adott feladatnak megfelelő alkalmazás kerül kiválasztásra, kifejlesztésre, az új rendszer általában nem kerül integrálásra a meglévő rendszerekkel. Az új rendszer tervezése során legtöbbször nem ismertek a hosszabb távú elképzelések, így csak később – az új igények megjelenésekor – válik láthatóvá, hogy szükség lehet különféle rendszerarchitektúrára épülő rendszerek összekapcsolása.

Másrészről a szervezet informatikai rendszerei számának növekedésével párhuzamosan nő az szervezett informatikai kitettsége, amely biztonságtudatos vállalati szemlélet esetén magával hozhatja a kockázatarányos védelem kialakítását. A kezdeti kezdetleges megoldásokat - a szervezet fejlődése során - felváltják a komplex – több szintű - védelmi megoldások, amelyek bevezetése általában magával hozza az üzleti folyamatok változását, így bevezetésük nem minden esetben könnyű feladat.

A több évtizede működő szervezetek esetén az adott pillanatban érvényes igény, szükséglet határozta meg, hogy mely folyamatok kerülnek információs rendszerekkel támogatásra, s jellemzően az adott időszak információbiztonsági technológiákat alkalmazva vagy – fenyegetettségek felismerésének és a jövőbeli elvárások ismeretének hiányába – mindenféle védelmi megoldás nélkül. A kezdeti időkben elsősorban a rendelkezésre állás volt a cél, kevesebb hangsúlyt helyeztek a bizalmasság, sértetlenség megőrzésére – ez a felfogás mai napig megtalálható – bár egyre kisebb mértékben - a különböző ipari irányító, mérési, stb. rendszereknél és sok esetben, az irodai környezetben is.

Ezen fejlődési utat járják be többek között a SCADA, PLC és egyéb ipari tevékenységet támogató informatikai rendszerek is. Információbiztonsági szempontból különösen aggasztó ezen rendszerekben alkalmazott technológiák védelmi megoldások gyengesége, védelmi mechanizmusok szinte teljes körű hiánya. Jelentős kockázatot hordoz, hogy ezen rendszerek közötti kommunikáció sok esetben nem titkos csatornán történik, mivel a fel nem ismert fenyegetések, a korábban nem ismert üzleti célok miatt az adatok titkosítása nem volt cél a protokollok fejlesztése során. Az egyedi megoldások miatt széles körben elterjedt a modem-es, hagyományos soros porton történő távoli rendszer elérés, de maga az master-slave architektúra is hordoz kockázatokat. [9]. Az ilyen rendszerekre is jellemző, hogy a kezdetben szeparált rendszer, összekötésre került a vállalat belső informatikai hálózatával, majd az internettel, s közben nem biztos, hogy kialakításra kerültek a megfelelő védelmi megoldások az infrastruktúra védelmének biztosítására.

A szélesebb körben elterjedt – nem speciális célra fejlesztett – rendszerek (pl.: ügyviteli-, banki-, vállalatirányítási-, pénzügyi rendszerek), vállalati belső információs rendszerek esetén a szervezetek a fenyegetettség érzetük alapján, illetve a szabályozói környezet szigorítása miatt vezették be védelmi megoldásaikat. A szervezet méretétől és az uralkodó információbiztonsági trendektől függően bevezetésre kerültek különféle egymással együttműködő, egymás működését támogató védelmi megoldások, többek között az IDM, IPS, IDS, DLP rendszerek, de fontos szerepet kaptak a különféle tűzfal és egyéb határvédelmi megoldások is.

A mobil eszközük elterjedése, a felhő alapú szolgáltatások igénybevétele azonban az eddigiektől eltérő, új szemléletet követelnek a biztonsági szakemberektől is, hiszen az addig jól körülbástyázott rendszerek hirtelen nyílttá váltak és a hatékonyságra törekvő üzleti igény lényegesen megelőzte ezen technológiák védelmét biztosító rendszerek kifejlesztését. Mobil eszközök védelmét biztosító MDM vagy EMM rendszerek még mindig nincsenek széles körben elterjedve, illetve a felhő alapú szolgáltatások esetén sem sikerült a biztonsági szakemberek számára megnyugtató védelmi megoldást találni.

Az informatikai rendszerek elterjedésével párhuzamosan alakultak ki az egyes rendszerekkel szemben megfogalmazott védelmi követelmények, amelyek segítettek a biztonsági szakembereknek megfelelő védelmi szint kialakításában. Később született meg a

felismerés, hogy hatékony információ védelem alapfeltétele - a különféle védelmi intézkedéseken túl - a megfelelő információ biztonsági irányítási rendszer működtetése (IBIR). Ma már természetesnek mondható, hogy egy szervezet rendelkezik az információbiztonsági irányítási rendszer területén külső, akkreditált tanúsítvánnyal (pl.: ISO 27001).

Információs infrastruktúrák fenyegetésének forrásai

Az információs infrastruktúrák megfelelő szintű működését számos külső és szervezeten belüli veszély fenyegeti. A támadások származhatnak egyes személyektől, jogosulatlan felhasználóktól, csoportoktól, terroristáktól valamint különböző nemzeti szervezetektől külföldi hírszerző szolgálatoktól, katonai szervezetetektől. Szakértők véleménye szerint a rendszerbetörések nagy többségében, mintegy 70–90%-ban belső munkatárs, vagy volt munkatárs is közreműködik. [10] Az információbiztonsági tevékenység része ezen fenyegetések kockázatainak csökkentése, a bekövetkezett esemény mielőbbi felismerése, hatékony kezelése, normál üzembe történő visszaállás megkönnyítése.

A fenyegetések eredete szempontjából megkülönböztethetünk emberi közreműködés nélküli (természeti eredetű) vagy közvetlen emberi közreműködés eredetű fenyegetéseket. Természeti eredetű fenyegetésnek tekintem azon fenyegetéseket, amelyeket kialakulását közvetlenül az ember nem tudja érdemben befolyásolni. Természeti jellegű fenyegetés az emberi tevékenység okozta természeti jelenségek (pl. erdőkivágások miatti árvíz, lokális időjárási események), az éghajlatváltozás és az időjárás szélsőségessé válása miatt kialakult fenyegetések, mivel ezen fenyegetések hosszú távú emberi tevékenységek következményei és befolyásolásukra rövid távon csak kis mértékben képes az emberiség, viselkedésük megegyezik a természeti jelenségek karakterisztikájával illetve ezen fenyegetések elleni védőintézkedések megegyeznek a természeti eredetű fenyegetések elleni védelmi intézkedésekkel.

Emberi tevékenység okozta fenyegetések közé sorolom azon fenyegetéseket, amelyeket közvetlen emberi tevékenység okoz, függetlenül attól, hogy annak mi a szándéka és oka. Az információs rendszer biztonságát lehet gondatlanul vagy szándékosan veszélyeztetni. A gondatlan veszélyeztetés elsősorban nem megfelelő szaktudásból, a biztonságtudatosság hiányából vagy a tevékenység következményeinek nem megfelelő felméréséből származik. Szándékos tevékenységek közé sorolandó azon tevékenységek, amelyek során egy személy vagy egy csoport célja az adott informatikai rendszer működésének megzavarása, a rendszerben tárolt információk kompromittálása (módosítása, törlése, információ megszerzése).

A belső veszélyeket elsősorban a saját alkalmazottak, munkatársak okozzák, akik a biztonsági rendszabályok be nem tartásával, képzetlenségükkel, hanyagságukkal, illetve vélt vagy valós sérelmeik megtorlásaként veszélyeztetik az adott szervezet, intézmény, vállalat stb. infokommunikációs rendszereit. Ezek a veszélyek, amennyiben felfedésükre és elhárításukra nem helyeznek hangsúlyt, komoly biztonsági problémák forrásai is lehetnek.

A külső veszélyek közé mindazon fenyegetések tartoznak, amelyek valamilyen külső forrásból származnak, és a támadás célja anyagi- politikai-, gazdasági- vagy katonai előnyszerzés. E támadásokat általában az információs technológiához kiválóan értők hajtják végre. E támadók köre az infokommunikációs rendszerek elterjedésével és fejlődésével egyenes arányban napról-napra növekszik és bővül. [1]

Az informatikai rendszerek tervezési, megvalósítási hibáiból adódó fenyegetések emberi tevékenység okozta fenyegetések közé soroltam, mivel közvetve véletlen vagy szándékos emberi tevékenység okozza a fenyegetést, illetve a fenyegetés kihasználásához is sokszor emberi tevékenység szükséges.

Az alábbi táblázatban összefoglaltam – a teljesség igénye nélkül - a leggyakoribb fenyegetéseket:

Természeti eredetű	Emberi közreműködés eredetű	
	gondatlan	szándékos
földrengés, árvíz, időjárás (pl.: vihar), kozmikus tevékenység (pl. napkitörés)	szoftverhiba, üzemeltetési folyamat megsértése, rossz döntés, ipari-, közlekedési-, nukleáris baleset	terrorizmus, hacking, bosszú, szabotázs, külső- vagy belső fegyveres konfliktus, információs hadviselés

1. táblázat Tipikus fenyegetések

A fenyegetés bekövetkezésének lehetséges hatása

A fenyegetés hathat közvetlen az infrastruktúra elemére vagy az infrastruktúra működését támogató egyéb – például információs – infrastruktúra elemre. Egy információ biztonsági esemény hatása azonban túlmutathat az információs infrastruktúra határain (pl. tartós áramszünet, szolgáltatás szünetelése miatti társadalmi, gazdasági hatás).

Az esemény hatását, kiterjedését többféle szempontból lehet csoportosítani.

Területi hatás alapján megkülönböztethetünk lokális, regionális, országos vagy akár több országon átívelő is eseményt. Jellemzően a kiterjedtség határozza meg, hogy az esemény kezelésében milyen szintű erőforrások bevonása szükséges. Jellemzően minél nagyobb a területi határ, annál nagyobb egy esetleges incidens bekövetkezésből adódó hatás, és annál komplexebb a védekezés.

Gazdasági hatás alapján az esemény bekövetkezésének közvetlen, illetve közvetett pénzügyi (gazdaság) hatás alapján lehet csoportosítani az eseményt. Alapvetően két fő csoportot lehet kialakítani: az esemény hatása az adott szervezeten belül kezelhető vagy az esemény kihatással van az adott megye, régió, ország gazdaságára. A szervezeten belül kezelhető hatás szélsőséges esetben akár a szervezet megszűnését is jelentheti.

Időbeli hatás: amely megmutatja, hogy az adott infrastruktúra vagy egyes elemének vesztesége mennyi ideig fejti ki komoly hatását (azonnal, 24–48 óra, egy hét, hosszabb időtartam). [8]

Ugyanakkor sok esetben nem a területi, gazdasági hatás határozza meg a támadás hatékonyságát, hatását. Az elmúlt néhány évben napvilágra került számos olyan célzott támadás, amelynek célja egy jól irányzott tevékenység elvégzése és amelyek egy kormányzati szerv, szervezet vagy egymással kapcsolatban álló szervezetek ellen irányultak:

- Az első dokumentált kibertámadást 1997-ben egy Sri Lankai terrorszervezet követtel el, [3] amelyet számos egyéb (pl.: Észtország, Grúzia elleni) kibertámadás követett.
- a Stuxnet 2010. júniusi felfedezése volt az első olyan széles körben nyilvánosságra került biztonsági esemény, amely vélhetően kormányzati támogatással, vélhetően egy konkrét célpontra irányult és mellesleg rávilágított arra, hogy a SCADA rendszerek informatikai védelme nem megfelelő. A támadás célja vélhetően az iráni atomprogram késleltetése volt a natanzi centrifugáinák és bushehri atomerőmű berendezéseinek támadásán keresztül. A Stuxnet amellett, hogy talán a legismertebb malware, nagyon kifinomult technikát használ(t) működése során. A malware egyes szakértői vélemények alapján 2-3 évig működött észrevétlenül, hozzávetőlegesen 100 ezer (egyes vélemények szerint 150 ezer) számítógépet fertőzött meg a világon, készítőiről bizonyíthatóan a ma napig nem derült ki, hogy kik voltak [11].
- vélhetően a Stuxnet fejlesztője, vagy a forráskódot ismerő személy készítette a magyar Crysys Lab által 2011-ben felfedezett Doqut [12], amely vezérlőrendszerekkel kapcsolatos információszerzésre lett vélhetően készítve és

ellentétben a Stuxnettel – az előzetes vizsgálatok alapján – nem tartalmaz romboló jellegű kódot.
- Európában az első – 2012. decemberében – nyilvánosságra hozott célzott kibertámadás a német 50 Hz elleni támadás volt, ami ugyan nem érintette a tényleges szolgáltatást, de több órára lebénította a cég informatikai rendszerét és rávilágított az informatikai rendszerek védelem fontosságára az M2M (machine to machine) rendszerek vonatkozásában [13].
- 2012-es felfedezésekor a legszofisztikáltabb káros program [14] Flame volt. A megfertőzött hozzávetőlegesen 1000 számítógépet fertőzött meg Közel-Keleten. A támadás célpontjai között oktatási, egészségügyi, kormányzati intézmények is voltak és a program gyakorlatilag bármilyen forrásból, csatornáról képes volt adatot lopni.
- Ugyanakkor 2014-ben is több 10 millió esetben történ például bankkártya vagy személyes adat lopás csak az Egyesült Államokban [15].

A támadások jellemzően a kibertérben maradnak, azaz közvetlen fizikai pusztító hatásuk nincs a fizikai környezetre. Ez alól kivételt képeznek az irányító rendszerek elleni támadások, amelyek – a különféle érzékelők, a technológiai folyamatok manipulánsán keresztül – sikeresen akadályozták a technológiai folyamatokat, illetve akár komoly fizikai pusztítással járó incidenst is okozhattak volna.

A támadásoknak azonban van egy közös tulajdonságuk: nem lehetett minden kétséget kizáróan bizonyítani, hogy kik voltak az elkövetők. Közvetlen bizonyítékok, szakértői vélekedések alapján azonban mindig volt feltételezett elkövető. Az egyetlen ismertté vált ítélet az orosz-észt konfliktus után született, ahol a 20 éves egyetemista 850 fontnyi büntetést kapott. [16]

Biztonsági esemény előre jelezhetősége

Az információs rendszerek globális jellegéből adódóan e rendszerek bárhonnan, bármikor elérhetők, és az információtechnológia vívmányait ellenük fordítva támadhatók. [1]

Az incidensek bekövetkezését minden esetben valamilyen eseménysorozat előzi meg. A támadó a támadás sikeres végrehajtásának érdekében számos tevékenység közül választhat. Ezen tevékenységek egy része a megtámadott számára nem észrevehető (pl.: publikus információ források elemzése), más része látható lehet, ugyanakkor megfelelő védelem hiányában nem biztos, hogy látható, a látható jelekből pedig nem biztos, hogy felfedezhetőek a támadás nyomai. Sok esetben az utólagos vizsgálat során derül ki, hogy jobban szervezett védelmi megoldással a támadási kísérlet felfedezhető lett volna.

Meghatározott események sorozata utalhat egy incidens várható bekövetkezésére, de nem feltétlenül jelenti azt, hogy a biztonsági esemény be is következik, illetve, hogy az esemény biztonsági eseménnyé válik-e. Ilyen események lehetnek például az elektronikus – pl.: elektronikus levélben beküldött káros kódok, amelyek megfertőzhetik a számítógépet és ott adatot gyűjthetnek vagy egyéb káros tevékenységet végezhetnek, de ilyen esemény lehet sikertelen bejelentkezések után egy sikeres, vagy akár egy IP cím lekérdezése is.

Az információ biztonsági incidens megelőző esemény sorozat definiáltságától függően megkülönböztethetünk:
- előre jól definiált eseménysorozat követő incidens: az eseményt egy időben, viselkedésében előre jól definiálható eseménysorozat előzi meg, amelyet a jelző, figyelmeztető rendszerek nagy biztonsággal jelezni fognak. Ezen eseménytípusok esetén jól tervezhetőek a különféle védelmi megoldások, legyenek azok fizikai, logikai vagy folyamati jellegűek. A korszerű információs technológiáknak köszönhetően számos olyan figyelmeztető mechanizmus került bevezetésre, ami képes előre jelezni az egyes infrastruktúra elemek várható fizikai hibáit, és ezzel

jelentős mértékben tudja támogatni a rendszereket üzemeltető szervezeteket. A kiforrott információbiztonsági védelmi megoldásoknak köszönhetően sok lehetőség van automatikus beavatkozásra is. Ilyen védelmi lehetőségek lehetnek hálózati forgalom átirányítások, vírus eltávolítás egy állományból, IDS rendszer jelzése, beavatkozása, riasztás küldése központi monitoring, riasztási rendszernek, DDoS védelem.

- nem vagy gyengén definiált eseménysorozatot követő incidens: ez eseményt nem előzi meg olyan – időben behatárolható - konkrét ismert eseménysorozat, tevékenység, amely egyértelműen előre jelzi a bekövetkezendő incidenst. Az időben elhúzódó és a jelző rendszerek által - az időbeni elhúzódás miatt - nem érzékelt eseménysorozatot is ebbe a kategóriába soroltam, mivel ilyen események felismerése is csak korlátozottan alkalmasak a jelenlegi védelmi megoldások. Definíció szerint ebbe a csoportba tartoznak továbbá azon eseményeket is, amelyek észlelése nem vagy csak hosszú idejű tevékenység után történik meg. Ezen csoportba jellemzően az információs rendszert érintő támadások tartoznak, amelyek előkészítése jellemzően hosszabb ideig tart és komolyabb erőforrást, szaktudást igényel. Ezen támadások elleni védekezés nehézkes, a jelenlegi információbiztonsági védelmi rendszerekkel szinte lehetetlen.

Vizsgálva a különböző veszély típusokat könnyen belátható, hogy a természeti katasztrófák elleni felkészülés többnyire gondos tervezéssel biztosítható, és ezáltal a kár bekövetkezése jó eséllyel a lehetőségekhez képest a legkisebbre csökkenthető. A mégis bekövetkező eseményeknél a kárelhárítás – elsősorban itt is a jó tervezhetőség miatt – gyorsan és hatékonyan véghezvihető.[5]

Az emberi közreműködés eredetű fenyegetések jelentős részének bekövetkezési valószínűsége – hasonlóan a természeti eredetű fenyegetésekhez – gondos tervezéssel, előre definiált eljárásokkal, megfelelő képzéssel jelentős mértékben csökkenthető. A kárelhárítás az esemény nagyságától függően hatékonyan végrehajtható. Ugyanakkor a védekezés a szándékos károkozás, illetve nem ismert támadási technika (pl. nulladik napi sérülékenység) kihasználása esetén jelentős nehézséget okozhat.

Szándékos emberi tevékenységből fakadó fenyegetések nagymértékben függenek a támadó fél szakmai tudásától, motivációjától, illetve a rendszer védelmi képességeitől. A napvilágra került sikeres kritikus infrastruktúrákkal szembeni támadások szinte mindegyikéről elmondható, hogy a támadás előre jól megtervezett módon, korábban nem ismert technikákkal történt, a támadók kihasználták a támadott rendszerek nulladik napi (0-day) sérülékenységeit és azon keresztül bejutva az információs rendszerbe végezték tevékenységüket. Jól jellemzi a támadások kifinomultságát, hogy például a Stuxnet az atomreaktornak csak a dúsító berendezéseit (centrifugákat) támadta, magát az erőművet nem, a Flame számos különböző modullal rendelkezik (kb. 20 megabájt méretben) és a vezérlő szerver parancsára képes volt magát eltávolítani a fertőzött rendszerből, a Doqu pedig célirányosan csak releváns információt gyűjtött.

Az előző fejezetekben említett és vélhetően még számos egyéb fertőzés további közös jellemzője, hogy a fejlesztés során kiemelt figyelmet fordítottak arra, hogy a káros tevékenységek minél hosszabb ideig – akár évekig is – rejtve maradjanak.

Az információs rendszerek „intézményesített” védelme

A fenyegetés eredetétől, illetve méretétől függetlenül léteznek olyan eljárások, védelmi mechanizmusok, amelyek jelentősen tudják csökkenteni az információbiztonsági incidens bekövetkezésének valószínűségét, segíteni tudnak az esemény bekövetkezésének korai felismerésében, az incidens bekövetkezése esetén az információs infrastruktúrák

működésének zavarásából eredő károk csökkentésében, illetve segítenek az elvárt működés mihamarabbi visszaállításában.

Hatékony információvédelmi rendszer kialakítását sok esetben jogszabályok írják elő, követelik meg. A hazai szabályozásban a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény alapozta meg a kritikus infrastruktúrák védelemének rendszerét. A törvény végrehajtásának érdekében számos kormányrendelet született, ugyanakkor kormányrendeletek kiadása még sok ágazat esetén nem történt meg, így az infrastruktúrák kijelölése több ágazatban nem kezdődött el.

A kritikus információs infrastruktúrák információvédelem alapjait a hazai szabályozási rendszerben az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, illetve a végrehajtására kiadott 77/2013. NFM. rendelet, majd a rendeletet hatályon kívül helyező, de tartalmában közel megegyező 41/2015. BM. rendelet alapozta meg. A kormányrendelet konkrét követelménylistát tartalmaz, figyelembe veszi az informatikai rendszer kieséséből, az informatikai rendszerben kezelt adatok bizalmasságának, sértetlenségének, rendelkezésre állásának elvesztése esetén bekövetkező közvetlen, közvetett kár nagyságát, társadalmi-, politikai hatását. A fentebb említett rendelet mellet számos olyan követelményrendszer létezik, amely szintén használhatóak az információvédelmi rendszerének kialakításában: például ISO/IEC 27002, NIST 800-53, BSI IT-Grundschutz-Kataloge, stb.

Fontos kiemelni azonban, hogy a védelem kialakításának kockázatarányosnak kell lennie, azaz a védelmi költség nem haladhatja meg a lehetséges kár maximális értékét, illetve a védelmi tevékenységek aránytalanul nem csökkenthetik a rendszer használhatóságát. Ezen egyensúly megtalálása sok esetben nem könnyű feladat.

A szervezeten belül kialakított információvédelmi képességének nagymértékben függnek továbbá a szervezett információbiztonsági érettségétől, a munkavállalók, szerződéses partnerek biztonság tudatától, illetve az alkalmazott konkrét fizikai, logikai védelmi megoldásoktól.

Mindazonáltal egy szervezet működtetheti a legfejlettebb információvédelmi rendszert, ha a szervezet dolgozói nem rendelkeznek megfelelő ismeretekkel, biztonság tudattal, a bevezetett védelmi megoldásokat nem tudják hatékonyan használni, akkor az információvédelem nem tud, nem képes hatékonyan működni.

Információs infrastruktúrák védelmének nehézségei

Az információs infrastruktúrák működtetése során egyre nehezebb biztosítani az infrastruktúra elemek megfelelő szintű védelmét, biztonságos – elfogadható szintű - működését az egyre komplexebb rendszerek, az integrált elemek sokszínűsége, az egyre nagyobb hatékonyságra való törekvés, valamint a pénzügyi és technikai korlátok miatt.

Az információs infrastruktúrák komplexitásának növekedésével párhuzamosan jelentős mértékben nőtt az egyes elemek sérülékenységéből adódó eredendő kockázat, az integrációknak köszönhetően az addig védettnek és zártnak hitt rendszerek biztonsági szempontból védtelenné válhatnak. A hiányosságokat jól mutatja, hogy például az elmúlt években is több esetben külső partneren keresztül sikerült kritikus információs infrastruktúra védelmi rendszerin áthatolni és ott jogosulatlan műveletet végezni.

Sok esetben nem biztosított a kritikus információs infrastruktúra kiszolgálását biztosító infrastruktúra védelme. Nem megfelelő a közműellátás, illetve nagyon sérülékenyek a telephelyek közötti kommunikációs csatornák: hiányzó tartalék közmű hálózatok, könnyen hozzáférhető hálózati kábelek. Ugyanakkor számos egyéb tényező veszélyezteti a biztonságos működést.

Motivációs – emberi - tényezők

Az informatikai rendszerekben kezelt adatok biztonsága a különböző rendszerelemeken megvalósított védelemtől függ, ezért a védelmi rendszer kialakításánál mindenkor számításba kell venni az embert, amely az egész védelmi rendszerben a legnagyobb bizonytalansági tényezőt jelenti. [17] Az emberi tényező több szempontból is biztonsági kockázatnak mondható, a felhasználók tudatlansága, szakképzetlensége, valamint az ezekből adódó emberi mulasztások aggasztó hatással vannak az informatikai biztonságra, de nem szabad megfeledkezni az emberi segítőkészség, befolyásolhatóság és naivság kihasználhatóságáról sem [18]. Különösen jelentős a kockázat, ha a munkavállaló tudásánál, képességénél magasabb szintű jogosultsággal rendelkezik az adott rendszerben. A nem kellő tudatosság, az adminisztratív szabályok hiánya sok esetben biztosít lehetőséget az emberi viselkedés támadó általi befolyásolására, azaz social engineering-re.

Az emberi tényező megjelenhet a támadó oldalon is. A támadónak a céljainak elérésére számos lehetőség kínálkozik. Minél komolyabb a támadó szándéka, annál szerteágazóbb eszközöket használhat információszerzésre, a támadás kivitelezésére. A támadás hatékonysága jelentősen javulhat, ha a támadó speciális szaktudással rendelkezik, vagy olyan csoport tagja, amely érdemi információval rendelkezik a cél rendszerről, illetve megfelelő erőforrást tud biztosítani a támadás megtervezéséhez végrehajtásához. Ilyen csoportok lehetnek hektivisták, de akár egy állam (vagy annak titkosszolgálatának) dolgozói. Fontos megemlíteni azt a tényt is, hogy a biztonsági incidensek legtöbbjét a vállalat belső munkatársai követik el, vagy legalábbis belső alkalmazottak segítsége, közreműködése is szükséges a sikeres támadás végrehajtásához [19]. A támadó szaktudása, lehetőségei és a támadás sikerességének esélye alapján a támadót az alábbi főbb csoportok egyikébe lehet besorolni:

- script kiddie, lamer, noob: olyan informatikában kevésbé jártas személy, aki mások által készített megoldásokat használ, nem képes újításokra, szofisztikált támadások végrehajtására. Információit hasonló tudással rendelkező társaitól szerez, velük oszt meg. Széles körű ismeret hiánya miatt igazán komoly károkat nem tudnak okozni, célja inkább a figyelemfelhívás. Az általános védelmi megoldások általában hatékony védelmet nyújtanak ellenük, ugyanakkor az ismert sebezhetőségek javításának hiánya nagymértékben növelhetik a támadás sikerességének esélyét.
- egyéni, kis szervezettségű támadók (hacker, cracker): több szintje létezik, jellemzően elegendően magas szintű informatikai, információ biztonsági tudással rendelkezik ahhoz, hogy önállóan vagy csoportosan meg tudjanak tervezni és végre tudjanak hajtani egyedi támadást. Általában nem rendelkeznek korlátlan erőforrással, így a támadás bár jól tervezett lehet, de nem szofisztikált. Célok között lehet a pénzszerzés, információszerzés, károkozás, de lehet, hogy csak szociális, társadalmi, ideológiai, vallási ok miatti figyelemfelkeltés. Nem megfelelően kialakított és üzemeltetett információ védelmi rendszer hiányosságait kihasználva komoly károkozásra képesek. Védekezés megfelelően kialakított és üzemeltetett információvédelmi rendszerrel lehetséges, amelynek része a többszintű védelem (pl.: intelligens tűzfalak, DLP, IPS, IDS megoldások), biztonsági monitorozás, naplóelemzés is.
- „hivatásos támadók”: általában szervezetekhez – nagyvállalatokhoz, kormányokhoz, terrorszervezetekhez, jelentősebb társadalmi csoportokhoz köthető személyek, akik megfelelő anyagi hátteret, akár titkosszolgálati úton szerzett, gyártóktól, fejlesztőktől ellopott információt kapnak a „megrendelőktől” a támadás sikeres végrehajtásának érdekében. Munkájuk során fontos, hogy észrevétlenek maradjanak, felfedésük ne történjen meg. Ez alól kivétel, amikor a támadó kiléte szándékosan nem mered rejtve (pl.: terrorszervezetek). Mélyreható ismeretük és megfelelő háttér miatt a védekezés

ellenük nehéz. A támadások során a rendelkezésre álló eszközök széles spektrumát alkalmazzák. Támadási módszerek a social engineeringtől, nem ismert sebezhetőségeken át, új támadási technikák kialakításáig terjedhet. A támadások nehezen felismerhetőek, nem egy esetben éveken keresztül maradt rejtve a támadó tevékenysége. A támadás jelentős költsége (Stuxnet esetén 10 és 50 millió dollár közötti összeg) miatt ezen támadási forma nem elterjedt, és csak akkor „éri meg", ha a sikeres támadásnak komoly pénzügyi, politikai hozadéka van (például Stuxnet).

Műszaki kockázatok

Napjainkban használt védelmi megoldások – néhány kivételtől eltekintve – nem képesek olyan eseménysorozatokat, jelsorozatokat felismerni, amelyek korábban nem lettek az adott rendszerben megadva. A rendszerek tanulása múltbéli események elemzésének eredményeként, manuális úton – frissítések által – kerül be a rendszerbe, nem tanulással.

Ugyanakkor az elmúlt időszakban ismertté vált incidensek rávilágítottak arra, hogy az információ védelemre hivatott megoldások magukban is jelentős kockázatot hordoznak, amivel az információbiztonsági szakma nem vagy csak kevésbé számolt:

- a biztonságosnak hitt biztonsági rendszerek belátnak mindenhova, azaz bizonyos körülmények között bármilyen műveletet el tudnak végezni a kritikus információs infrastruktúrában, így a biztonsági rendszerek sérülékenységei fokozott veszélyt jelentenek,
- a széles körben elterjedt szignatúra alapú megoldások nem képesek követni a támadások során alkalmazott folyamatosan változó technikákat,
- a biztonság szavatolására hivatott rendszerek is számos hibát, sérülékenységet tartalmaznak,
- a felvásárlásoknak köszönhetően jelentősen csökkent a védelmi megoldásokat szállító vállalatok száma, ami sok esetben hasonló biztonsági megközelítést jelent a különféle termékeikben, megkönnyítve az integrációt és az üzemeltetést, de csökkentve a rendszer védelmi képességét,
- az egymástól függetlennek tűnő megoldások sok esetben hasonló alapokon működnek, így párhuzamos használatuk sem hozza meg az elvárt eredményt, ezzel hamis biztonságérzetet nyújtanak a szakemberek és a döntéshozók számára,
- a különböző szállítók által készített megoldások mindenki számára elérhetőek, így lehetőség van az egyes védelmi megoldások gyenge pontjainak megkeresésére,
- költséghatékonyság miatt a szervezetek általában nem használnak ugyanarra a feladatra több szállítótól is beszerzett terméket,
- a termékek fejlesztése során a kormányzati, titkosszolgálati szervek nyomására backdoorok kerülnek a rendszerekbe, amelyekről előbb-utóbb információt szerez a hacker társadalom is,
- hosszabb távon komoly kockázatot jelent a nem hazai, EU-n belül készített védelmi rendszerek, technológiák használata. A jelenleg baráti országok viszonya változhat, ami magában hordozhatja a fenyegetés jelentős növekedését,
- pozitív kockázatként jelent meg, hogy az elmúlt időszak eseményei következtében a biztonsági megoldást szállító cégek, kutató laborok egyre nagyobb figyelmet fordítanak saját nemzetük által használt rendszerek védelmére, ami rövid távon is jelentősen javíthatja biztonságunkat.

Ezen kockázatok meglétét bizonyítja, az elmúlt időszakban napvilágra került lehallgatási ügyek (többek között NSA – winchester firmware manipuláció, titkosszolgálati lehallgatások), számos kiemelt, magas kockázatú sérülékenység biztonsági megoldásokban

(például SSL, SYMANTEC Endpoint Protection, CISCO ASA sérülékenység [20]), illetve a korábban említett káros kódok éveken keresztül tartó észrevétlen működése is.

Hatékony információvédelem megteremtésének lehetőségei

A védelmet, mint tevékenységet modellezve egy egyszerűsített helyzetet képzeljünk el, amelyben a támadókat és a védőket egyszerűsítéssel egy-egy személy, a védő és a támadó testesíti meg. A támadó az egyik oldalról támad, és ez a támadás mindig valamilyen, a támadás végső célját képező értékre, a védett értékre irányul. A támadás legtöbbször nem közvetlenül éri a védett értéket, hanem a körülményektől függő támadási útvonalon zajlik le, amelyen különböző természetes vagy művi védelmi akadályokat kell legyőzni. A másik oldalon a védő a védett értéket védi, vagyis a támadásokat igyekszik megakadályozni, elhárítani. Mivel a védő és a támadó egymás szándékairól, módszereiről semmilyen információval nem rendelkezik, ezért elmondhatjuk, hogy mindkét fél egymástól független és egymás számára ismeretlen stratégiával igyekszik megvalósítani támadási, illetve védelmi szándékait. [21]

Az előző fejezetekben említett okok és kockázatok miatt nyilvánvaló, hogy a jelenleg széles körben alkalmazott védelmi megoldások nem vagy csak részben jelentenek megoldást megfelelő információbiztonság kialakításához. Fokozott figyelmet kell fordítani a korábbi években - a biztonságos rendszerfejlesztés érdekében megfogalmazott - alapelvek betartására, ugyanakkor az új kihívások egyben újszerű gondolkodásmódot, újszerű megoldásokat is követelnek az információbiztonság területén tevékenykedő vállalatoktól, szakemberektől.

Másrészről pedig fokozott figyelmet kell fordítani az információs rendszer tervezésére, a fejlesztési, tesztelési feladatok magasabb színvonalú, biztonságos üzletmenetet garantáló végrehajtására. Egy rendszer vagy szolgáltatás gyorsabb bevezetése nem járhat a rendszer implementációs idejének csökkentésével.

Újszerű gondolkodás részeként lehetséges megoldásként látom az eddig alkalmazott technológiák kiegészítését, olyam védelmi rendszerekkel, amelynek működési paraméterei részben vagy egészben egyediek, a támadó számára nehezen vagy egyáltalán nem megismerhetőek.

Napjainkban rendelkezésre álló nagy számítási kapacitásnak köszönhetően már széles körben elterjedtek azok a megoldások is, amelyek a felhasználó, rendszer viselkedésében vagy a hálózati adatforgalomban bekövetkező szokatlan tevékenységet vizsgálják.

Részleges megoldást jelenthet a – nem feltétlenül publikus - felhő alapú technológia, amely segítségével a világ számos pontjáról lehet gyűjteni az információbiztonsági szempontból releváns információkat, a begyűjtött információkat rövid idő alatt fel lehet dolgozni és el lehet küldeni a szolgáltatást igénybe vevő szervezeteknek, így a hatékony információ megosztás segíthet az incidens megelőzésében, kezelésében. Ugyanakkor számos szakmai vita zajlik a felhő alapú szolgáltatások biztonságával kapcsolatban, aminek következtében a különböző hatóságok sem ajánlják, támogatják a publikus felhő alapú szolgáltatások igénybevételét.

A kutatások során előtérbe kerülhet a mesterséges intelligencia alapú technológiák alkalmazási lehetőségeinek vizsgálata, alkalmazása. [3] Várhatóan jelentős előrelépést fog jelenteni a tanuló rendszerek szélesebb körű elterjedése, függetlenül attól, hogy az helyi vagy felhőszolgáltatás alapú védelmi megoldásban kerül kialakításra. Ugyanakkor a tanuló rendszerek sem fognak tudni teljes védelmet biztosítani, mivel a tanulási folyamat manipulálható, illetve az incidensek felismerésére a mai rendszerekben figyelt paraméterek széles körű kiterjesztésére lenne szükség, amelyhez jelenleg még nincs elegendő számítási kapacitás és a vizsgálat, rendszer fenntartásának költsége már nem biztos, hogy

kockázatarányos. A tanulásra képes rendszerek – jó definiált esetekben – akár képesek lehetnek önálló döntésre, beavatkozásra is.

A fejlődés ezen lehetséges útjai azonban számos új kockázatot hordoznak, amelynek feltérképezése még nem történt meg teljes körűen, a kockázatok kezelésére ma még nincsenek meg a válaszok. Várhatóan azonban az újszerű technológiák szélesebb elterjedése ki fogja kényszeríteni ezen kockázatok részletes feltárását, valamint az ügyfelek, hatóságok számára megfelelő megoldás biztosítását.

Megítélésem szerint igazi áttörést és megoldást a korábban lefektetett tervezési, fejlesztési alapelvek figyelembe vétele mellett, a jelenlegi alkalmazott védelmi megoldások az új technológiákkal történő hatékony ötvözése, valamint a tudásmegosztás hozhat.

ÖSSZEGZÉS

A kritikus infrastruktúrák és kritikus információs infrastruktúrák megfelelő szintű védelme elengedhetetlen a társadalom, a gazdaság, a védelmi szektor működéséhez. A kritikus infrastruktúrák működése manapság szinte elképzelhetetlen hatékony informatikai támogatás nélkül. Az infrastruktúrák fejlődésével párhuzamosan kerültek új informatikai támogató rendszerek bevezetésre, kerültek a meglévő rendszerek integrálásra. A fenyegetettségek felismerése magával hozta az infrastruktúrát védeni hivatott védelmi megoldások bevezetését. Meghatározása kerültek a rendszerekkel szemben támasztott fizikai, logikai követelmények és kialakultak az információbiztonsági irányítási rendszerek.

Az informatikai rendszerek komplexitása, sokszínűsége ugyanakkor magával hozta az emberi és technikai fenyegetettségek jelentős növekedését, amelyre az információ biztonsági szakma csak részben tudott válaszolni.

Az információs rendszerek és az azokban tárolt információk egyre nagyobb értéket képviselnek, így a rendszerek működésének zavarására, valamint az információk megszerzésére is egyre nagyobb a motiváció. Nem egy információbiztonsági incidens mögött vélhetően állami szereplők állnak, aminek bizonyítása ugyan nehézkes, de a támadás célja és a támadáshoz felhasznált anyagi-, emberi erőforrások valószínűsítik a támadó hátterét.

Ugyanakkor az elmúlt időszak eseményei rávilágítottak arra is, hogy nem csak közvetlenül az emberi tényező jelent komoly kockázatot, hanem a védelem biztosítására hivatott rendszerek is. A jelenleg széles körben elterjedt védelmi eszközök csak akkor tudják hatékonyan ellátni feladataikat, ha a támadás karakterisztikája ismert, azaz korábban sikerült azonosítani egy biztonsági incidens előzményeit. Számos esetben azonban – a rendelkezésre álló erőforrások miatt – megjelennek olyan tevékenységek, amelyek nem utalnak támadásra, így a védelmi rendszerek nem jeleznek, sokszor akár több éven keresztül sem.

Az újszerű megoldások – hasonlóan a korábbi évekhez – várhatóan nem fognak önmagukban megoldást hozni a folyamatosan növekvő kockázatok elviselhető mértékű szintre csökkentésében.

Hatékony információvédelem kialakításához újfajta technikai megoldások bevezetése, új gondolkodásmód szükséges, amely magával hozhatja az elmúlt években megjelent korszerűnek tekinthető információvédelmi megoldások integrációját, a már széles körben alkalmazott megoldásokkal. Új szerepet kaphat a felhő alapú szolgáltatás, a viselkedés alapú esemény felismerés, illetve a mesterséges intelligencia is a hatékony védelem megteremtésében.

Felhasznált irodalom

[1] Haig Zsolt: Az információs társadalmat fenyegető információalapú-veszélyforrások:

http://www.zmne.hu/kulso/mhtt/hadtudomany/2007/3/2007_3_4.html (letöltve: 2015.szeptember 3.)

[2] Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van II.: Célok és teendők http://www.hadmernok.hu/2011_1_kovacs_sipos.pdf (letöltve: 2015.szeptember 3.)

[3] Haig Zsolt – Kovács László: Fenyegetés a cybertérből http://www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf (letöltve: 2015.szeptember 6.)

[4] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény

[5] Muha Lajos: A MAGYAR KÖZTÁRSASÁG KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁINAK VÉDELME Doktori (PhD) értekezés Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem 2007.

[6] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008

[7] Haig Zsolt – Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák tanulmány 2012 http://uni-nke.hu/downloads/konyvtar/kovasz/kritikus_infrastrukturak.pdf (letöltve: 2015. július 10.)

[8] Haig Zsolt, Hajnal Béla, Kovács László, Muha Lajos, Sik Zoltán Nádor: A kritikus információs infrastruktúrák meghatározásának módszertana 2009. http://www.cert-hungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf (letöltve 2015. július 10.)

[9] Eric J. Byres - Matthew Franz - Darrin Miller: The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems http://www.ida.liu.se/labs/rtslab/iisw04/camready/SCADA-Attack-Trees-Final.pdf (letöltve: 2014.03.10.)

[10] Haig Zsolt: Számítógép-hálózatok hadviselés rendszere az információs műveletekben. http://uni-nke.hu/downloads/bsz/bszemle2006/1/06_Haig_Zsolt.pdf (letöltve 2015. július 10.)

[11] Nicolas Falliere, Liam O Murchu, and Eric Chien: W32.Stuxnet Dossier https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (letöltve: 2015.04.30)

[12] Steven Cherry: Sons of Stuxnet http://spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet (letöltve: 2015.04.30)

[13] Pelle Neroth: Germany's 50Hertz hit by cyber attack in European first http://eandt.theiet.org/blog/blogpost.cfm?threadid=49719&catid=390 (letöltve: 2015.04.30)

[14] sKyWIper Analysis Team: A complex malware for targeted attacks http://www.crysys.hu/skywiper/skywiper.pdf (letöltve: 2015.04.30)

[15] Bill Hardekopf:The Big Data Breaches of 2014 http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/ (letöltve: 2015.04.30)

[16] Estonia fines man for 'cyber war' http://news.bbc.co.uk/2/hi/technology/7208511.stm (letöltve: 2015.09.10)

[17]Muha Lajos – Krasznay Csaba Az elektronikus információs rendszerek biztonságának menedzselése https://opac.uni-nke.hu/webview?infile=&sobj=9696&source=webvd&cgimime=application.pdf (letöltve: 2014.03.10.)

[18] Thapar, 2007 Thapar, A. (2007): Social Engineering - An attack vector most intricate to tackle!, http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf letöltve: 2015. március 10)

[19] Oroszi Eszter: Social Engineering Az emberi erőforrás, mint az információbiztonság kritikus tényezője http://krasznay.hu/presentation/diploma_oroszi.pdf (letöltve: 2015.03.20)

[20] Kormányzati Eseménykezelő Központ (GOV CERT Magyarország) sérülékenységek: http://tech.cert-hungary.hu/taxonomy/term/22 (letöltve: 2015.05.04)

[21] Muha Lajos: Az informatikai biztonság meghatározása (3.3. fejezet), In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2004., ISBN:963 9313

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Som Zoltán - Papp Gergely Zoltán
som.zoltan.kdi@office.uni-nke.hu - papp.gergely.kdi@office.uni-nke.hu

TUDÁSFEJLESZTÉS A KIBERBŰNÜLDÖZÉSBEN – LEHETŐSÉGEK ÉS KIHÍVÁSOK

Absztrakt

Napjainkban az infokommunikációs eszközök széles körben elterjedtek, a hétköznapi élet minden területén jelen vannak. Ezek az eszközeink értéket képviselnek, mint ahogy értéket képviselnek azon adatok, információk is, amelyek ezen eszközökön tárolódnak. Sok esetben maga az információ megszerzése a cél, a tároló eszköztől függetlenül, vagy fordítva. Fel van-e készítve a felhasználók arra, hogy milyen módon óvhatják meg adataikat? Legalább ennyire fontos, hogy fel vannak-e készítve a nyomozati szervek, hogy az új társadalmi változásokra, tendenciákra reagáljanak? Ezen logika mentén három fő érdekcsoportot különböztethetünk meg. Az első az állampolgárok köre, akik információs rendszereket és eszközöket használnak. A második fő csoport, akik információs rendszerekkel kapcsolatos visszaéléseket követnek el, eszközök vagy információk megszerzésében érdekeltek. A harmadik csoportot pedig a nyomozati szervek alkotják, akik a meglévő eszközparkkal, saját vagy külső erőforrásból próbálják fenntartani a rendet. A külső erőforrások vonatkozásában az igazságügyi szakértőkre gondolunk elsősorban, akik szakmai és műszaki felkészültségükkel képesek a nyomozati szervek munkáját segíteni. Mélyebben és összefüggéseiben vizsgálva a kérdést, ezen folyamatok kihatással lehetnek az e-szolgáltatások elterjedésére, az e-befogadására, a teljes IKT szegmensre és a GPD-re is. Így az infokommunikációs folyamatokból eredő változások feladatokat indukálnak számos területen, mind a kormányzati, a szolgáltatói, a bűnüldözői és a nyomozati tevékenységet folytató szervezeteknél egyaránt.

The use of various info-communication tools are widely spread, they are present in all areas of our every-day lives. These tools represent values to us, just as various data and information stored on them do. In numerous cases the goal is to acquire information with no special regard to the storage device or it might even be the other way around. Are users adequately prepared to be able to protect their data? Are they familiar with the right methods to do so? Just as importantly, are investigative bodies prepared to react to tendencies and changes of this new society? Following this logic, there are three major interest groups. The first one being the citizens using IT systems and tools. The second major group consists of those who are interested in acquiring information or equipment for which they abuse IT systems. And the investigative bodies make up the third group who try to maintain order using instruments they already own, utilizing their personal resources or some external ones. By external resources, we primarily mean judicial experts who are well prepared both professionally and technically

speaking and thus would be able to aid the work of investigative bodies. Reviewing the question at hand in context and more deeply, it becomes visible that these processes may affect the spreading of e-services, e-acceptance, and the ICT segment as a whole or even the GDP. As a result, changes in info-communication processes induce objectives to be set by service providers and bodies engaged in both governmental activities as well as law enforcement and investigation.

Kulcsszavak: *információbiztonság, informatikai bűnesetek, informatikai szakértő, információbiztonsági és tudatossági oktatás, e-befogadás, e-közigazgatás ~ information security, IT crime, IT expert, information security education and awareness, e-acceptance, e-(public) administration*

INFORMÁCIÓS RENDSZEREK NAPJAINKBAN

Az Európai Unió EU2020 programjának része, hogy polgárai minél több szolgáltatást vehessenek igénybe elektronikusan, ehhez pedig minden szükséges feltétel, például a szélessávú internetelérés lehetősége is rendelkezésre álljon.[1] Ezzel összhangban van a Nemzeti Infokommunikációs Stratégia 2014-2020, a technológiai változások és lehetőségek gyors kiszélesedése azonban más megközelítést igényel az állampolgárok részéről is. Felkészítéseket kell tartani tudatossági képzésekkel, ismeretterjesztő anyagokkal annak érdekében, hogy a gyors változásokkal járó kockázatokat csökkenteni lehessen, az állampolgárok megfelelő kompetenciával, rendelkezzenek, megfelelő tudatossági szinten legyenek saját adataik védelme érdekében.[2] Az állampolgárok általános csoportján kívül azonban számos más halmaz és érdekeltségi kör mentén is lehet csoportokat definiálni.

Az Európai Unió és Magyarország Kormányának, 2020-ig előirányzott stratégiai tervei [3], [4] további, nagymértékű fejlődést terveznek az elektronikus szolgáltatások, az IKT szektor és az e-közigazgatási szolgáltatások területén is. Ilyen nagyságú és gyorsaságú fejlődésre és változásra fel kell készíteni az érintetteket, az állampolgárokat, a közigazgatásban dolgozókat, megfelelő információbiztonsági szintet kell elérni.[5], [6]

Hétköznapi életünk minden területén jelen vannak és nélkülözhetetlenné váltak az információs rendszerek, különös tekintettel arra, hogy minden további közműszolgáltatás, szállítás, stb. is ezen rendszerek összehangolt irányítása mellett valósul meg.[7] A felhasználók jelentős része könnyen megtéveszthető, sokan a közvetlen környezetünkben napi szinten használt eszközök működési elvével sincsenek tisztában (például okostelefon, világítás, egyéb elektronikus vezérlésű rendszerek). Ennek egyik oka az, hogy a rendszer szállítója jellemzően el is rejti a „motorháztető alatt” annak elemeit, mivel a kezelőnek, felhasználónak elegendő bizonyos gombokat megnyomnia, nem szükséges ismernie a háttérben zajló folyamatokat. Ebből következik, hogy nem is érdemes ezen ismereteket oktatni (hiszen a technika fejlődésével mindez folyamatosan változik), sokkal inkább egy általános biztonságtudatossági magatartás és gondolkodás kialakítására, fejlesztésére van szükség, leginkább ezzel készíthető fel az állampolgár a lehetséges veszélyekre.

LOKÁLIS ÉS NEMZETKÖZI ESEMÉNYEK

Jól példázza a változó trendeket a 2007-es Észtországi kiberháború és 2010-es Iráni atomprogram[8] elleni támadás is.[9] Észtország esetében megmutatja, hogy mélyen, elemi folyamatokban vannak jelen az információs rendszerek, amelyek elleni célzott támadás rövid időn belül képes megbénítani a normál hétköznapi folyamatokat, akár egy egész ország életét. Az iráni atomprogram elleni Stuxnet vírustámadás pedig jó példa arra, hogy rendszereink összetettsége olyan méreteket öltött, amely már nehezen követhető. Strukturáltsága olyan bonyolult, hogy csupán más rendszerek segítségével vagyunk képesek működésüket fenntartani.

Léteznek szervezett bűnözői csoportok, amelyek fő profiljuk mellett alkalmanként más területeken is próbálkoznak, a meglévő adataikból próbálnak minél nagyobb profitra szert tenni. Az internetes feketepiacon minden adatnak értéke, ára van. Megadott összegekért cserél gazdát egy e-mail cím adatbázis, vagy bankkártya adatok, stb. minden pénzzé tehető. Általában véve igaz, hogy olyan gyorsan változik a technológia, amelyet rendkívül nehéz

szabályozási keretek között kezelni. A teljesség igénye nélkül jó példa erre a bitcoin [11] fizetési megoldás, vagy a Tor projekt [12], amely teljes anonimitást garantál.[13] Azonban az internet rendkívül polarizáló ereje révén, ezen eszközök is többféle célra, így illegális tevékenységre is alkalmasak.

A kiberteret [14], az Ibtv[15] alapján értelmezve könnyen belátható, hogy olyan globális hálózatot használunk, amelyben a potenciális fenyegetettség és támadások szempontjából szinte csak logikailag értelmezhető a magyar vagy más kibertér. A globális kibertér kifejezés jól reprezentálja, hogy nincsenek országhatárok, a visszaélési lehetőségek átlépik azokat. Egyetlen globális kibertér van, ahol természetesen vannak földrajzi eltérések, de ezek nem értelmezhetőek túl szigorúan. A Budapesten megalkotott – és számos további EU tagország által ratifikált –, a kiberbűnözés visszaszorításáról szóló egyezmény kereteit napjainkra túlhaladta az informatika világa. A kapcsolódó jogsértések is teljesen megváltoztak, így szükségszerű a terület újraszabályozása és folyamatos monitorozása. A tudomány fejlődési ütemét tekintve bizonyos, hogy az internetalapú digitális gazdaság a hazai fejlődés fontos tényezője lesz a következő években.[16] Az információs rendszerek polarizáló hatása figyelhető meg.

Összegezve egy olyan koordináta rendszerben képzelhetjük el az információs rendszereket, a globális kiberteret, amelynek az abszcisszáján az érdekeltségi motiváció található (azaz nemzetállamok, bűnszervezetek, ipari vállalatok, egészen a lakossági felhasználásig megtalálhatóak), míg az ordinátán az adott tevékenység pénzügyi hatása ábrázolható. Így talán a „legkisebbnek" tekinthető okostelefon és az ahhoz köthető adateltulajdonítás, valamint az ipari kémkedés reprezentálására egyaránt alkalmas a rendszer.

ÁLTALÁNOS GYAKORLAT ÉS TUDATOSSÁGI SZINT

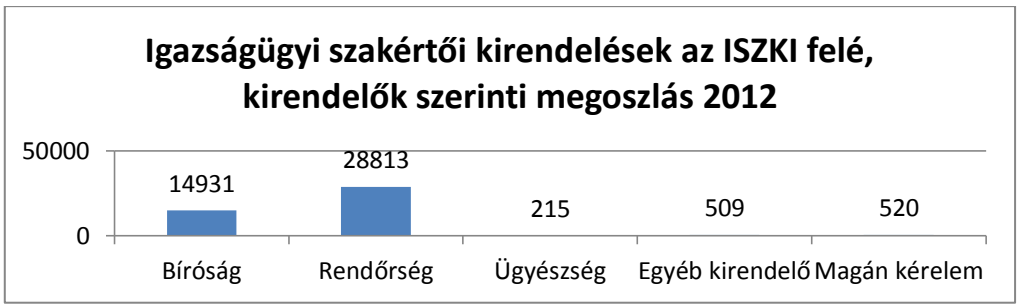
Az információs rendszerek széles körben elterjedtek, további növekedésük prognosztizálható. A nemzetközi és hazai kutatások, események mind azt mutatják, hogy az információra és az információs rendszerek feletti befolyásra napjainkban már komoly figyelmet kell fordítani, kiterjesztve az említett rendszerek működésének garantálására, a benne lévő információk védelmére, annak bizalmasságára, sértetlenségére és a rendelkezésre állására [17]. A globális kibertér eseményeire számos példát lehet felsorolni.[18] A közigazgatás kiszolgáltatottsága jelentős, mivel „…tény, hogy közigazgatás megszervezése a mai világban informatikai számítástechnikai eszközök nélkül nem lehetséges" [19]. A kibertudatosság [20] szinten tartása, növelése, a szervezeti egyenszilárdság megteremtése érdekében komoly lépéseket kell tenni. Ezen lépéssorozat egyike a Nemzet Közszolgálati Egyetemen elindult EIV képzés [21] is, amelynek reális eredményeit várhatóan csak évek múlva lehet kimutatni majd. Ennek oka feltételezhetően az, hogy a szervezeti egyenszilárdság megteremtése kultúra kérdése is, azaz nem lehetséges csak tisztán szabályozással gyors és tartós sikereket elérni.

Az is megállapítható, hogy alapszintű biztonságtudatos magatartással az ilyen visszaélések túlnyomó része megelőzhető lenne a virtuális térben [22]. Kutatások azt is igazolják, hogy a tudatos magatartást jelentősen befolyásolja az informatikai eszközökkel, rendszerekkel kapcsolatos felhasználói attitűd [23]. A jelenlegi információbiztonsági szint további, mélyebb elemzésre szorul, mivel a kutatások alapján valószínűsíthető, hogy a tudás sok esetben

megvan, de a gyakorlatba, a hétköznapokba nem minden esetben épült még be. [24] Magyarország ettől függetlenül jól áll szabályozás és alapok tekintetében az EU-n belül.[25] Nem várható el széles társadalmi rétegektől, hogy a technológia minden részletét ismerjék. Az ilyen jellegű visszaélések és nyomozati tevékenység ellátására, támogatására lett létrehozva a szakértői rendszer. Az általános gyakorlat természetesen valamilyen optimumra törekszik. Azaz a kisebb büntetési tételű vagy kisebb anyagi kárt jelentő ügyekben kisebb mértékben történik meg „energia kifejtés". Míg a 3-5 évnél nagyobb büntetési tételek, életellenes cselekmények esetében sokkal gyakoribb a szakértők bevonása. A szakértői rendszer részletes áttekintése nélkül két fontos dolgot kívánunk kiemelni. Az egyik, hogy a sok apró ügy summázása összességében olyan gazdasági értéket képviselhet, amellyel már érdemes lenne központilag foglalkozni. Ennek érdekében viszont olyan folyamatra, technikai és oktatási modernizációra van szükség, amely révén lehetséges az egyébként kis volumenű esetek kezelése is. A másik, hogy a látszólagosan kis fajsúlyú esetekben jelenleg még nem kezelik az eltűnt adatokat, jellemzően csupán az adathordozó notebook, telefon, stb. eszközökre koncentrálnak a nyomozati tevékenység során.

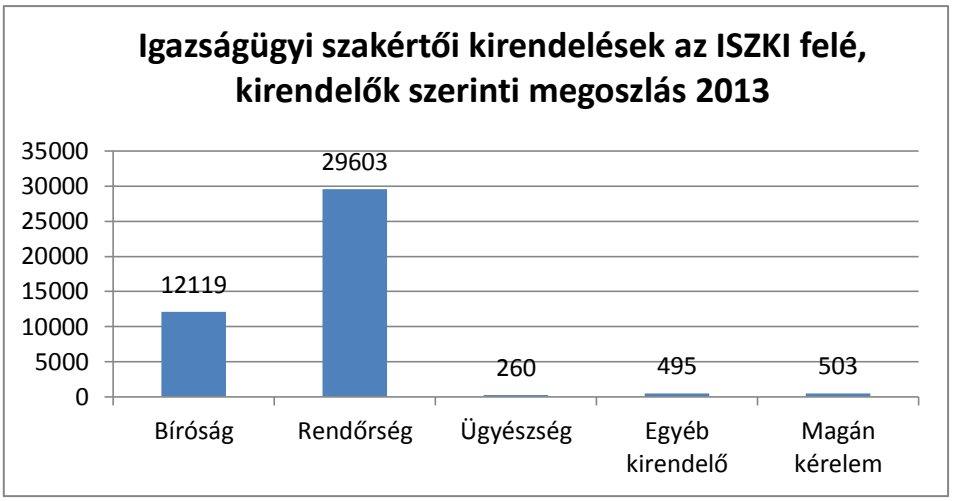
SZAKÉRTŐI KIRENDELÉSEK SZÁMA

Az igazságügyi szakértői rendszer működésének egyik lényege, hogy a tudomány aktuális, legfrissebb állásának megfelelő eredményeket felhasználva lehessen egyes esetekben eljárni, a szakterület legjobbjaitól segítséget kérni. Tekintsük meg a kirendelések számát, amely nem országos összesítés (csak az ISZKI felé érkező kéréseket mutatja), mégis reprezentatívnak tekinthető.[26]



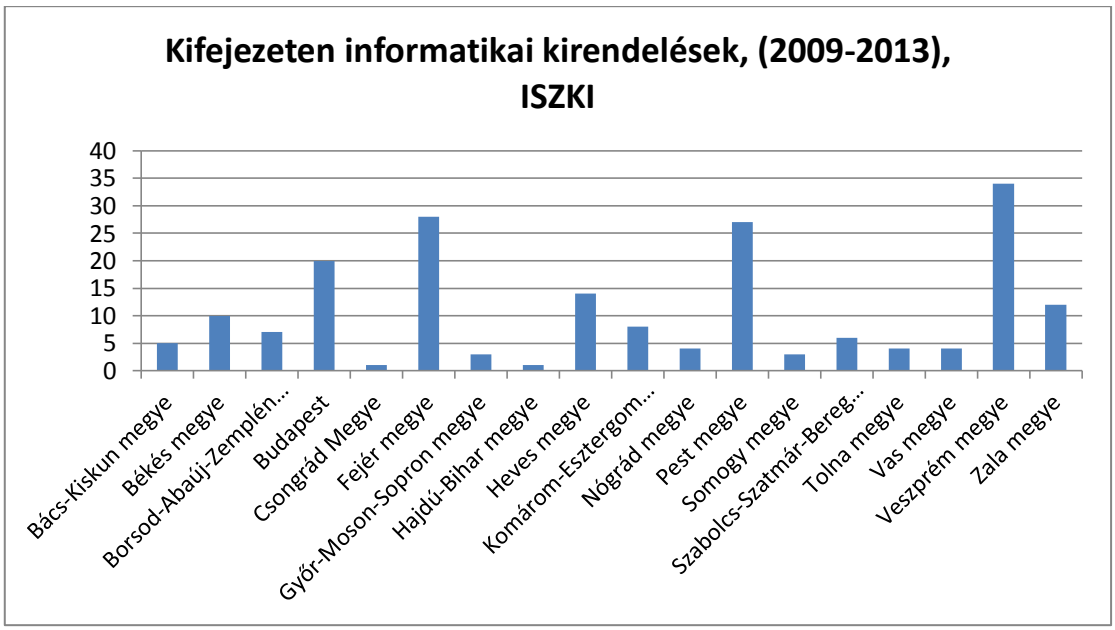
1.ábra Igazságügyi szakértői kirendelések az Igazságügyi Szakértői és Kutató Intézetek felé, 2012-ben[26]

A fenti 1. sz. ábrán az ISZKI felé intézett kirendelések és megkeresések száma figyelhető meg. A 2. sz. ábrán pedig a 2013-as évre vonatkoztatott adatok láthatóak. Látható, hogy nagyságrendi különbségek nincsenek, nagy változások nem tapasztalhatóak.



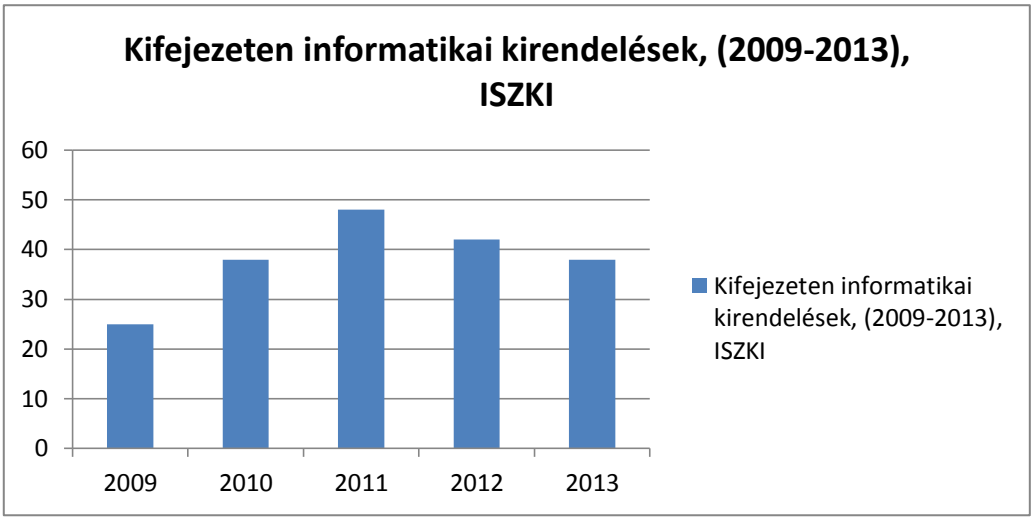
2. ábra Igazságügyi szakértői kirendelések az Igazságügyi Szakértői és Kutató Intézetek felé, 2013-ban [26]

Majd vizsgáljuk meg, a kifejezetten informatika témában történő kirendeléseket is a 2009-2013 intervallumban.



3. ábra Igazságügyi szakértői kirendelések az Igazságügyi Szakértői és Kutató Intézetek felé, informatikai ügyekben 2009-2013, megyénkénti eloszlásban [26]

A 4. ábrán pedig a 2009-2013 közötti, informatikai témában történő esetszámot láthatjuk, kirendelő szerinti bontásban.



4. ábra Igazságügyi szakértői kirendelések az Igazságügyi Szakértői és Kutató Intézetek felé, informatikai ügyekben 2009-2013, évenkénti eloszlásban [26]

Jól láthatóan egészen alacsony számban vannak informatikai kirendelések, felkérések, a teljes számossághoz viszonyítva. Ennek egyik oka lehet, hogy még a nyomozati tevékenységben, kriminalisztikai oktatásban, valamint a felhasznált eszközök tekintetében jelentős fejlesztésre lenne szükség. További oka lehet, hogy sok esetben közvetlenül keresik meg a hatóságok a szakértőket – elsősorban azért, hogy árversenyt indukáljanak. Pedig tudhatjuk, hogy „olcsó húsnak híg a leve", hiszen a jó szakértőnek fent kell tartani az eszközparkot, képeznie kell magát, hogy a kor követelményeinek megfelelve, magas tudományos szinten legyen képes az adott ügyet kivizsgálni.

Fontos tehát, hogy csupán technikai fejlesztés nem hozhat hosszú távú eredményeket. Erre jó példa, hogy „hiába" van rendszám, vagy akár arcfelismerő alkalmazás és rendszer, hiába van letárolva az adott nagy mennyiségű információ az adatbázisban, ha nincs ott a megfelelő szakértelemmel rendelkező humán-erőforrás, amely ezt feldolgozni képes. Tehát minden összetevőre szükség van ahhoz, hogy általánosan fordítani lehessen a jelenlegi tendencián. Az ember, a humán tényező és annak képzése, a képzett munkaerő kapacitása is kiemelten fontos a rendszerben, különös tekintettel arra, hogy az információs technológiák segítségével elkövetett, vagy éppen ennek segítségével felderíthető eseték száma prognosztizálhatóan növekszik. A társadalmi szokások változása miatt elképzelhető, hogy a táblagépek és okostelefonok sok esetben másodlagos célként jelennek meg, elsődlegesen már a rajtuk tárolt adatokon, azok megszerzésén, felhasználásán van a hangsúly. Ezen esetek felderítése technológiai értelemben nem lenne már lehetetlen, sokkal inkább humán-erőforrás függvénye.

MI VÁRHATÓ A JÖVŐBEN?

Az információbiztonság helyzetét vizsgálva Magyarországon láthatóan koncepcionális és szisztematikus munka valósul meg[31],[32], az EU direktívákkal összhangban. Az információbiztonság, annak mérése, az egyéni- és szervezeti tudatossági szint felmérése komoly kihívás, mivel bizonyos esetekben kimutatható, hogy a válaszadók a kérdéseknek akarnak megfelelni.[32] A többi Uniós tagállamhoz hasonlóan Magyarországon is működik az Európai Unió Safer Internet[33] programja, amelyet a Nemzetközi Gyermekmentő Szolgálat karolt fel. Összességében azt feltételezhetnénk, hogy jól állunk – és ez szabályozási szempontból valóban érvényes is –, azonban az tapasztalható, hogy még nem képezi a rutin

részét, nincs beidegződve a biztonságtudatos viselkedés. Bár ismertek az ajánlások, de még nem épültek be a szokásokba.

„Meg nem kerülhető kérdés a felhasználói tudatosság. A tapasztalatok szerint a minden IT újdonságra nyitott, gyakran a biztonsági minimumokat is elkerülő felhasználók zömét a fiatal korosztály adja. Az alap- és középfokú képzésben, majd a szakmai vagy felsőfokú szakirányokban kiemelt szerep hárul az oktatásban közreműködőkre annak érdekében, hogy a ma csak Y generációnak nevezett, néhány év múlva a gazdaság vérkeringésébe bekerülő tömegek személyes és egyéb szenzitív adatokat tudatosan, biztonságosan, készség szinten helyezzenek el, kezeljenek. A jelenleg hiányos, IT biztonság tárgyú oktatási anyagok és oktatói ismeretek pótlására hatékony finanszírozási eszközt kell biztosítania a fenntartónak."[33] Várhatóan növekedni fog azon események száma, amikor például nem csak az okos telefon lesz a célpont, nem csak az adathordozót tulajdonítják el, hanem a rajta lévő adatokkal is megkísérelnek majd visszaélni. Az adott eszközzel kapcsolatos figyelmeztetés akár törvényi kötelezettség is lehetne. „A kormány az Európai Unióban elsőként lépett a hatékonyabb, biztonságosabb, nagyobb tudású, ugyanakkor olcsóbb informatikai rendszer kialakításának, azaz a kormányzati felhőszolgáltatás elindításának útjára." [32] Hozzá kell tenni, hogy ez a tendencia állampolgári szinten is megjelenik. Azaz gyakorlatilag az okostelefon alkalmazások, a közösségi hálózatok, levelezés, mind olyan alkalmazások, amelyek jellemzően a felhőben, valahol a kibertérben találhatóak.

A további, várhatóan újabb platformokon megjelenő jogellenes cselekmények felderítése, szakszerű bizonyítása további kihívást jelent az igazságszolgáltatás valamennyi szereplője számára. A sok esetben felhőben tárolt, fizikai adathordozó lefoglalása nélkül feltárt összefüggések tényadatokkal való alátámasztása, szakvéleményben való objektív és érthető közlése még inkább nélkülözhetetlen lesz az ügyek hatósági szereplői számára. Hogy a jogszabály betűje szerinti kötelezettség teljesítése érdekében szükséges bizonyítási eszköztár és ismeretanyag többlet finanszírozása hogyan oldható meg a kötelezettek oldalán, egyelőre erősen nyitott kérdés.[32] További aggodalomra ad okot, hogy jelenleg sajnos nincs ezen a területen szakértői életpálya modell.

AZ INFORMÁCIÓS TÁRSADALOM GAZDASÁGI VETÜLETEI

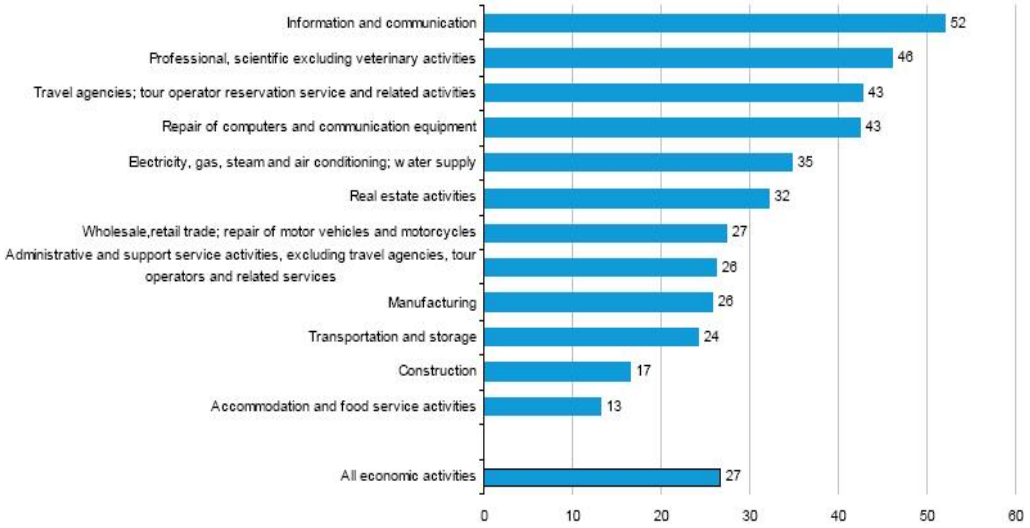
Minden évben, az európai állampolgárok 40%-a (kb. 200 millió fő) vásárol az interneten. Az IKT szektor önmagában majdnem 6%-át reprezentálja az EU GDP-jének és EU IKT szektor és az IKT-hoz kapcsolódó befektetések szállítják hozzávetőleg a felét a termelékenység növekedésének, emellett pedig az internet-gazdaság generálta a 21%-át az EU GDP növekedésének az elmúlt 5 évben. Az ENISA 2012-es jelentése[34] azt mutatja, hogy a kiberbiztonsági incidensek a munkahelyteremtést és a gazdasági növekedést is veszélybe sodorhatják.

Top Threats	Current Trends	Top Emerging Trends					
		Mobile Computing	Social Technology	Critical Infrastr.	Trust Infrastr.	Cloud	Big Data
1. Drive-by exploits	↑	↑	↑	↑		↑	↑
2. Worms/Trojans	↑	↑	↑	↑		→	↑
3. Code Injection	↑	→		↑		↑	
4. Exploit Kits	↑	↑	→	↑			↑
5. Botnets	↑	↑		→		→	
6. Denial of Service	→			→	↑	→	
7. Phishing	→	↑	↑	→			→
8. Compromising Confidential Information	↑	↑		↑	→	↑	↑
9. Rogueware/ Scareware	→		→				
10. Spam	↓		→				→
11. Targeted Attacks	↑		↑	↑	→	↑	→
12. Physical Theft/Loss/Damage	↑	↑	↑	↑	→	→	
13. Identity Theft	↑	↑	↑		→	↑	↑
14. Abuse of Information Leakage	↑	→	↑		→	↑	↑
15. Search Engine Poisoning	→						
16. Rogue Certificates	↑				↑		

Legend: ↓ Declining, → Stable, ↑ Increasing

5. ábra ENISA: Fenyegetettségi térkép 2013 áttekintő [34]

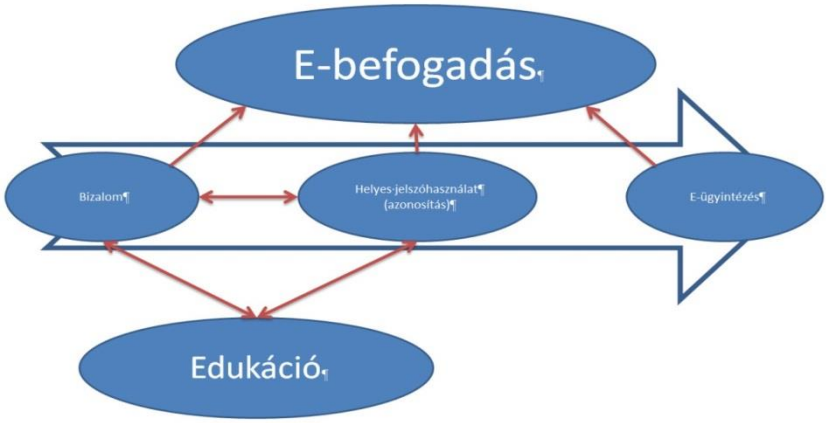
Az 5. sz. ábrán jól látható, hogy szinte minden potenciális támadási-területen minimum stagnálás, mailben irtam de jellemzően emelkedés tapasztalható a kiber bűncselekmények előfordulásában. A stagnáláshoz hozzátartozik, hogy az internetképes eszközök száma növekszik, így a puszta stagnálás is növekedést jelenthet.



6. ábra Az EU GDP és ICT kapcsolata [35]

Éppen ezért kiemelten fontos, hogy erre a nemzetközileg jellemző tendenciára Magyarország, és a hazai bűnüldöző szervek is felkészüljenek. Az igazságügyi szakértők szakmai és műszaki felkészültségükkel képesek a nyomozati szervek munkáját segíteni, mert már számos technikai lehetőség rendelkezésükre áll a tevékenységük támogatására, elegendő ha a számos, nyilvános területen található kamerára gondolunk, vagy a mobiltelefonok nyújtotta lokalizációs és képrögzítési lehetőségre. A megfelelő oktatás segítségével továbbá olyan társadalmi folyamatok is indukálhatóak, amelyek – összhangban a Magyarország

Nemzeti Infokommunikációs Stratégiájával és az EU 2020 célkitűzéseivel – szinergikus folyamatokat indíthatnak el. Mindezek nem csak az e-szolgáltatások elfogadottságát, az e-befogadást, az IKT szektor fejlődését erősíthetik, hanem kimutatható módon a GDP növekedéséhez is jelentős mértékben hozzájárulhatnak. Mindehhez természetesen komplexen látni kell nem csak az egyes folyamatokat, hanem az azok közötti összefüggéseket is.



7. ábra Az ügyfélbizalom, mint feltétel [36]

A FELHASZNÁLÓI BIZALOM ÉS AZ INFORMATIKAI BIZTONSÁG ÖSSZEKAPCSOLÓDÁSA

Ezen szolgáltatások támadása, nem csak és kizárólag anyagi veszteségeket, elmaradt bevételt produkál, hanem hosszú távon az ügyfélbizalom elvesztése révén sokkal komolyabb hatásai lehetnek. Az ügyfélbizalom helyreállítása sokkal költségesebb lehet, mint a prevenciós tevékenység, sőt bizonyos esetekben nem is lehetséges. Ezen a ponton tehát az informatikai biztonság és a felhasználói bizalom között nagyon szoros összefüggés mutatható ki.

Ahogy már említésre került, nem csupán az elkövetéssel érintett tárgy vagyoni értékét szükséges vizsgálni, nem csak az adott esetben érintett információ és információhordozó értékét, hanem az éves szinten summázott érték valószínűleg széles társadalmi mérésekkel összevethető módon befolyásolja azt az ügyfélbizalmat is, amelynek megerősítése és szinten tartása mára a modern gazdaságokban elengedhetetlen feltétel. Mindezeket áttekintve számos területen lehet megfogalmazni tennivalót, kicsit előre tekintve pedig már most láthatóak olyan, jelenleg még nem szabályozott területek, amelyek a technika gyors változásából következőleg olyan módszer kidolgozására sarkalják a szakmában érintetteket, amelyben a törvényi szabályozás gyorsasága összemérhetővé válik a technikai változásokkal. Azaz, ha új, még a törvényekben, eljárásrendekben nem szereplő visszaélési módszerek bukkannak fel, akkor azokat is nagyon gyorsan kezelni lehet, annak nem jelenlegi, hanem várható és összegzett súlya alapján. Így tehát az oktatásnak és a megfelelő eszköz- és humán erőforrásnak a szabályozási területen, a tudatossági képzéseken, az információbiztonsági vezetők rendelkezésre álló forrásaiban, a nyomozati tevékenységet ellátó szervezetek belső- és külső humánerőforrásainak tekintetében is meg kell jelennie. Nem utolsó sorban pedig az igazságügyi szakértő háttérrendszer megerősítésében, hiszen ezek nélkül nem jön létre, nem indulhat be az a szinergikus folyamat, amely révén széles társadalmi rétegekhez jut el a tudás, a tudatosság és nem alakul ki az a széleskörű bizalmi háló sem, támogatva az e-befogadást és erősítve a gazdasági tényezőket.

ÖSSZEGZÉS

Összegezve kijelenthető, hogy a humán faktor, az emberi tényező minden egyes folyamatban jelen van. Azaz nem elegendő és nem lehet megoldás csak a technológia fejlesztése, annak kiválasztása, beüzemelése, működtetése minden esetben humánerőforrást és döntést igényel. Mindehhez pedig olyan magasan képzett, a rendszert jól ismerő személynek kell rendelkezésre állnia, amely átlátja a megfelelő összefüggéseket, megfelelő kapacitással rendelkezik ahhoz, hogy a nagyszámú eseményt – amelyre irányulóan a technika csak elő feldolgozást képes végezni – le tudja kezelni. A tendenciák, nemzetközi és hazai szinten egyaránt jelen vannak, mint ahogy a kibertér képzeletbeli határai is nehezen rajzolhatóak meg. Így az oktatás és a felkészítés területén – amelyek mind a szakembereket, mind pedig széles társadalmi rétegeket érintenek – sok tennivaló van még. A szakértői rendszer vonatkozásában olyan életpályamodellt lenne érdemes kialakítani, amely hatékony támogatást képes nyújtani ahhoz a célhoz, hogy az egyre növekvő információ rendszerekkel összefüggő esetek, visszaélések, ezek terjedése ne öltsön még nagyobb méreteket. Határozott koncepciót kell kialakítani, hogy ne utólag kelljen az e-bizalom visszaállítására, az e-befogadás újra-fejlesztésére horribilis forrásokat elkülöníteni.

Felhasznált irodalom

[1] Europe 2020, A European strategy for smart, sustainable and inclusive growth, http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf, 2016.05.01.

[2] Z. Som: Laws aiding cyber security in the EU. Central and Eastern European eGov Days, 2014.

[3] EU 2020 Programterv az ICT szektorra, http://ec.europa.eu/programmes/horizon2020/en/h2020-section/information-and-communication-technologies, 2016.05.01.

[4] Nemzeti Infokommunikációs Stratégia 2014-2020, http://www.nisz.hu/sites/default/files/u1/nemzeti_infokommunikacios_strategia_2014_2020.pdf, 2016.05.01.

[5] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat, 31. pont a kiberbiztonságról http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf, 2016.05.01.

[6] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat, http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845, 2016.05.01.

[7] Z. Som: Cyber security legislation in the EU in: The information technology as Public Utility. Nispace, 2014.

[8] A. Cserháti: A stuxnet vírus és az iráni atomprogram, http://fizikaiszemle.hu/archivum/fsz1105/CserhatiAndras.pdf, 2016.05.01.

[9] Z. Som: Kibertudatossággal a kiberhadviselés ellen. 13. Robothadviselés konferencia, 2013.

[11] A Bitcoin fizetési eszköz, https://bitcoin.org/hu/, 2016.05.01.

[12] A Tor Projekt, https://www.torproject.org/, 2016.05.01.

[13] P. Sasvári, Z. Som: Az információbiztonság-tudatosság vizsgálata a magyar üzleti- és közszférában. ITBN, 2016.05.01.

[14] [15] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, http://kozlonyok.hu/nkonline/MKPDF/hiteles/MK13069.pdf, 2016.05.01.

[16] Cs. Lente: Mérlegen az informatikai biztonság. ITBN, http://miszk.hu/hir/merlegen-az-informatikai-biztonsag.html, 2016.05.01.

[17] Z. Som: Hitelesítési kérdések a magyar (e-) közigazgatásban. Tavaszi szél konferencia, http://www.kozszov.org.hu/dokumentumok/UMK/UMK_2014_2/20_esemeny_Orszagos_doktorandusz_konf.pdf, 2014.

[18] G. Z. Papp, Z. Som: Jelszóhasználati trendek és az ügyfélbizalom értéke, avagy a jelszó, a bizalom és az e-befogadás és ezek kapcsolata napjainkban. http://www.academia.edu/9393609/Jelsz%C3%B3haszn%C3%A1lati_trendek_%C3%A9s_az_%C3%BCgyf%C3%A9lbizalom_%C3%A9rt%C3%A9ke._A_jelsz%C3%B3_a_bizalom_%C3%A9s_az_e-befogad%C3%A1s_%C3%B6sszef%C3%BCgg%C3%A9sei_napjainkban, 2016.05.01

[19] I. Bukovics: A fenntartható közigazgatás, fenntartható biztonság elmélete. http://docplayer.hu/9743088-Bukovics-istvan-a-fenntarthato-kozigazgatas-fenntarthato-biztonsag-elmelete.html, 2016.05.01.

[20] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus i nformációbiztonságáról, http://kozlonyok.hu/nkonline/MKPDF/hiteles/MK13069.pdf, 2016.05.01.

[21] NKE Elektronikus információbiztonsági vezető szakirányú továbbképzési szak, http://vtki.uni-nke.hu/szakiranyu-tovabbkepzes/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto-szakiranyu-tovabbkepzesi-szak, 2016.05.01.

[22] Z. Som, G. Z. Papp: Információbiztonsági alapok és jelszóhasználati statisztikák. A jelszó, a bizalom és az e-befogadás összefüggései napjainkban. http://www.academia.edu/9393569/Inform%C3%A1ci%C3%B3biztons%C3%A1gi_alapok_%C3%A9s_jelsz%C3%B3haszn%C3%A1lati_statisztik%C3%A1k._A_jelsz%C3%B3_a_bizalom_%C3%A9s_az_e-befogad%C3%A1s_%C3%B6sszef%C3%BCgg%C3%A9sei_napjainkban, 2016.05.01.

[23] J. Reich, Zs. Döme: Közszolgálat a közigazgatásban. ÁROP-2011/1.1.12.

[24] M. Illéssy, A. Nemeslaki, Z. Som: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. Információs társadalom, Társadalomtudományi folyóirat, XIV. évfolyam, 1. szám (p.:52-73) ISSN:1587-8694.

[25] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, http://kozlonyok.hu/nkonline/MKPDF/hiteles/MK13069.pdf, 2016.05.01.

[26] Igazságügyi Szakértői és Kutató Intézetek. Nyilvános, weblapról származó információk, beszámolók, negyedéves jelentések hivatalos 2009-2014. évi adatszolgáltatása alapján saját feldolgozás és elemzés. http://www.iszki.hu/, 2016.05.01.

[27] Digitális Megújulás Cselekvési Terv. Egyszerű Állam: a vállalkozások adminisztratív terheit csökkentő középtávú kormányzati program. Magyary Zoltán Közigazgatás-fejlesztési Program. Magyarország Nemzeti Kiberbiztonsági Stratégiája. Nemzeti Infokommunikációs Stratégia 2014-2020. Ibtv.

[28] Z. Som, G. Z. Papp: Információbiztonsági alapok és jelszóhasználati statisztikák. A jelszó, a bizalom és az e-befogadás összefüggései napjainkban. http://www.academia.edu/9393569/Inform%C3%A1ci%C3%B3biztons%C3%A1gi_alapok_%C3%A9s_jelsz%C3%B3haszn%C3%A1lati_statisztik%C3%A1k._A_jelsz%C3

%B3_a_bizalom_%C3%A9s_az_e-befogad%C3%A1s_%C3%B6sszef%C3%BCgg%C3%A9sei_napjainkban, 2016.05.01.
[29] M. Illéssy, A. Nemeslaki, Z. Som: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. Információs társadalom, Társadalomtudományi folyóirat, XIV. évfolyam, 1. szám (p.:52-73) ISSN:1587-8694.
[30] EU Safer Internet Program, https://saferinternet.hu, 2016.05.01.
[31] Digitális Megújulás Cselekvési Terv. Egyszerű Állam: a vállalkozások adminisztratív terheit csökkentő középtávú kormányzati program. Magyary Zoltán Közigazgatás-fejlesztési Program. Magyarország Nemzeti Kiberbiztonsági Stratégiája. Nemzeti Infokommunikációs Stratégia 2014-2020. Ibtv.
[32] Cs. Lente: Mérlegen az informatikai biztonság. ITBN, http://miszk.hu/hir/merlegen-az-informatikai-biztonsag.html, 2016.05.01
[33] Enisa. Threat Landscape 2013. Overview of current and emerging cyber-threats. 11 December 2013.
[34] Enisa. Threat Landscape 2013. Overview of current and emerging cyber-threats. 11 December 2013.
[35] Eurostat weboldal. Figure 10. http://ec.europa.eu/eurostat/documents/4168041/5947469/KS-QA-10-049-EN.PDF/15c0d269-9f5f-4ab6-aefb-6db976cb22cd , 2016.05.01.
[36] Z. Som: Hitelesítési kérdések a magyar (e-) közigazgatásban. Tavaszi szél konferencia, http://www.kozszov.org.hu/dokumentumok/UMK/UMK_2014_2/20_esemeny_Orszagos_doktorandusz_konf.pdf, 2014.

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Szendi József
j.szendi@yahoo.com

COST OPTIMIZED RADIO COMMUNICATION AT THE FMCG SECTOR SUPPORTING THE OBJECT SECURITY

Abstract

At the FMCG sector the operation management might require a stabile and reliable communication at site. Most cases the company pulls in a mobile telephone asset to cover this task. This case the management of the supply chain, the guards and other workers are using cell phones for communication. In the unlike event of any disaster or accidents this communication line might loose its stable connection. Many cases the workers are not allowed to take in mobile phone to the GMP area, but still must stay contactable. To handle the in-house communication one of the options can be an in-house radio system. This article compares the GSM phone and the in-house radio system helping the decision maker to choose the best solution to cover this task.

Az FMCG szektorban a vezetésnek szüksége lehet stabil és megbízható kommunikációra a telephelyein. A legtöbb esetben a cégek mobil telefon állománnyal kezelik a feladatot. Ennél a megoldásnál az ellátási lánc vezetése az őrség és a dolgozók telefonhívással intézik az üzemeltetést. Egy sajnálatos katasztrófánál vagy balesetnél azonban a kommunikációs csatorna eltűnhet. A legtöbb gyári környezetben a dolgozók amúgy sem használhatnak telefont GMP környezetben, de mégis elérhetőnek kell maradniuk. A belső kommunikáció kezelésére történhet rádió rendszerrel is. A cikk összehasonlítja a GSM telefont és a rádió rendszert segítve a döntéshozót a legjobb megoldás kiválasztásában.

Keywords: *Object safety, Data safety, RF communication at FMCG sites ~ Objektumvédelem, Adatbiztonság, RF kommunikáció FMCG környezetben*

INDUCTION

In-house communication is important due to cost efficiency or Health and Safety purposes at the FMCG (Fast Moving Consumer Goods) sector [1]. FMCG sector uses different kind of manufacturing plants, logistic warehouses, shops and other supply chain elements for its business. Depending on site, the plant might be quiet huge and the site might contain several buildings. Most factories have fence, metal framed windows, boilers – as part of the manufacturing technology – some others might have ammonia based cooling systems built all gears very close to each other. Within this area people should communicate to each other. All of the equipment mentioned above are acting as shield of the communication, managing weak signals in any RF based communication.

As a bundle of contracts, phones might be seen cheap for the Management, so they cover the daily tasks during the manufacturing by cellphones in most cases. If there are overnight maintenance tasks, the phones are also used to handle the in-house communication: like getting permission of suspending the local Fire Alarm System or support many other engineering tasks.

The problem comes if the cellphone supplier's tower is located too far, or the building has several basements. Due to Health and Safety reasons all staff should stay contactable, and none of the Maintenance Engineers should be sent alone to any plant room without any communication device. Losing the connection is a weak point in case of preventing any accidents. The best communication device is essential if we want to reach a better level of in-house security. Nowadays no one is sure about the information safety at site. The company might loose in-house information when using normal cellphones. Actually food and other FMCG manufacturing plants are not as critical like a nuclear plant, but some sales secret might be very sensitive information for the owner. The information is money, even if it is not a classified data [2] by the law.

Internal communication is essential to reach the KPI (Key Production Indicator) [3] goals at an average factory. The old days, daily printed reports where sent around, but nowadays the process efficiency and the speeded customer service expectations require much quicker in-house communication, than a few years before.

Some companies might have tight policies when providing company phones or radios for employees. Actually if the maintenance staff is not allowed so use a mobile at site and even not supplied by any other communication device, might cause absenteeism of work. Basically the local manager and the fire department or the guards cannot reach their staff during working hours. Most cases the serious incident response plan - In Hungary the SKET [4] - describes the minimal required in-house communication protocol.

I specify that an engineering team without communication device is a massive bottleneck within the object security. Shame that the fire alarm procedures and dangerous material recovery actions are effected: such like ammonia or hydrogen recovery or server room cooling safety. Any company having maintenance team without mobile communication device has a high risk of KPI fall. In Hungary traditional service providers like Water or Drain Works are highly affected. In case of fire the maintenance staff is one of the first at site who should actually act. Without the primer action the harm might become much bigger at site in case of technical error.

Actually if the communication protocol is well set up, the data can be logged well and the job can be tracked. This information is handy for the mid management to make action plan to cover minor faults and carry out surveys within the plant. If the minor faults are well managed all faults are handled at a higher level and the payback is a much higher object security as well with less integrity fail.

IN-HOUSE COMMUNICATION ALTERNATIVES

Verbal and written communication

Good option for communication, but the information is slow and not trustable, especially if report comes from the night shift. Actually written report can make a better quality of logging, but still slow and the logging procedure cannot be centralized. Written reports like Survey Reports and Maintenance Sheets are nowadays the standard method of work. Most maintenance task might be handled this way, but in case of any accident paperwork is usually made after the case itself. I specify, that this is a bottleneck of the object security.

Email

Email might work in office to office communication, but at the field, usually at GMP (Good Manufacturing Practice) area normal computers keyboards are not permitted due to hygienic and safety reasons. [5] Due to legal employment and EHS (Environment Health and Safety) [6] specs lone working is not allowed during maintenance procedures at Hungary. Actually one guard and one competent person together in the engineering sector can be even a pair, by the law. Most cases companies are updating the original hand operated plant rooms after a while to semiautomatic type. This plants do not require daily maintenance attendance, only some visits. This case one person is allowed to have regular checks ordered by HR due to the force of reducing costs. I specify that HR should not force lone working, as it is one of the root cause of accidents. In case of any problem the best practice is not the email for communication. Much better way to report a fault is a PDA device or a hand held radio as they are much quicker, well logged and all tasks are human controlled instantly. Basically the guard at the Security Office can log the fault, and the Engineering Manager can call out the contractor to repair the fault. This type of outsourcing can reduce the local costs as special companies can handle special faults quicker.

GSM cellphone

As widely used and well known commercial product [7], the mobile phone is a good solution for communication, if the service provider guaranties the service. Actually the problem is rather data safety and hygiene risk. Most IFS (International Food Standard) [8] regulations do not allow foreign objects at the manufacturing area, and most phones can fall easily into the product. If the company controls the food quality with additives, this information might be handled as special secrets and it is not good, if a competitor uses the mobile phone as a spying tool. GSM cellphone is good gear to reach the customer, but is not the best solution for a factory even widely used everywhere today.

PMR handheld radio

PMR (Personal Mobile Radio) [9] is available on the market at a very reasonable price. The frequency is free to use, but anyone might listen the conversation. Cheap PMR solutions are not safe and reliable for industrial use at all. Actually the power of an average unit is well too weak to support an average sized factory. Also the equipment's lifetime is too short to support a team. We can expect at least 3 years of lifecycle in case of any industrial set up. Actually the PMR radios are available for commercial use are designed really like toys. 3 cell NiCd batteries are unable to handle an output power better than 300 mW. This power is not enough at a noisy field, which is usually full with interference. Licence free PMR solution has no coding in the modulation. Basically anyone picks up the signal might listen the sender as the

modulation is standard narrow FM. The information might go away a few miles in good propagation conditions.

Civil TETRA solution

Civil Tetra system is an industrial solution allowing encryption in communication. Actually a whole bunch of radios are available on the market, and their usage become close to mobile phones. This communication systems are used in 55 countries [10]. It still has a centralized station, but the data is much more isolated and the communication protocol allows to reach just the authorized equipment as seen on Fig1. Even the product has a good quality the communication still relies on the central station.

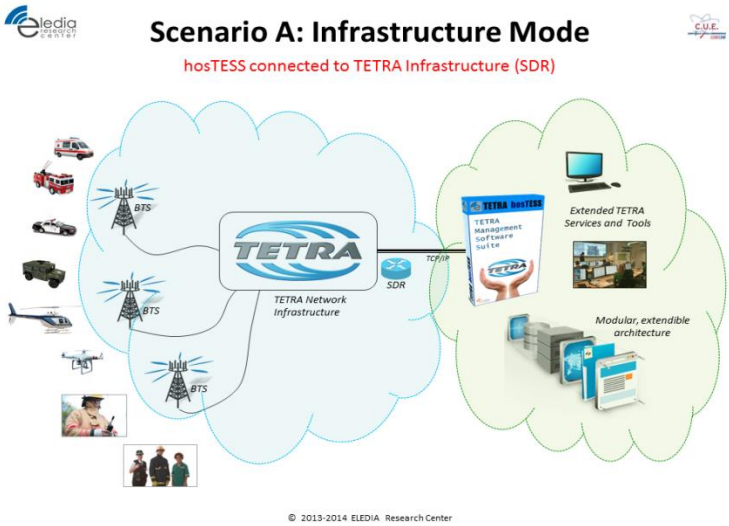


Fig1. Civil Tetra System. source: [10]

Tetra solution is much more secure than free PMR. The radio might be used in local mode and also in distance mode. The second solution requires the centralised station, but the communication can be encrypted meeting TEA2 level as part of the contract. The overall solution the TETRA is an excellent choice for industrial users - such like power stations - but the system is relative pricy for the FMCG sector. As per my research the TEA2 coded communication is available for Private Customers, but the service provider must agree prior to any coding. The communication encryption deepness cannot be the same like used in the public services.

Landline

Landline is still a safe way of communication in meaning of reliability, but the equipment is locked in position. Actually landline wires are easy to reach by unauthorized person. Analog landline is out of date nowadays.

CHOOSING THE BEST SOLUTION FOR AN AVERAGE FACTORY

Engineering Manager usually provides calculation and estimating for the decision maker. The decision maker can believe he/she is in charge, but he/she usually deals with the options already in the forecast plan. If there seems another solution, which is really missed by the decision maker, the forecast plan must be extended. The decision is usually down to cost and payback. Payback could be the customer satisfaction well, but usually the actual costs are compared.

If any payback comes within year it should be invested with no argues, especially if no other policies are affected. If the payback comes in about 3 years, it is still a value. When the company's finance is stable, the solution should be pulled in. If the payback is over 10 years it is not the best option to choose at all.

Some cases to keep the fleet of mobile phones is a bonus for the staff as they can use it for private calls and they stay contactable after working hours. Engineering managers might find the best technical solution, most of the time the cost must be kept as low as possible. Mobile phones are quiet cheap and their service providers can offer a contract for low price if the customer chooses a contract of a bundle. The problem comes if the building is built of metal sheet based panels, which work like a screen, especially if they are well grounded.[11] In case of a well grounded metal frame like commonly used in server rooms as soon as the user enters into the room there is no proper signal. If the people really want to reach someone there they must use a landline or a powerful radio. Actually the cost of the radio system can be about 5 times more compare to a cell phone in a bundle. Actually the radio has several advantages:

- Much more RF power. Even a hand based Vertex Standard VX-231 can reach 5 Watts [12]. This power is enough to cover a 20 floor building including the subbasement also.
- No cost of minutes
- Hand held radios cannot take pictures. Might be handy if client wants to save the know-how. Some factories have a procedure to tape up the cameras on the client's mobile phones due to integrity policies.
- Depending on its frequency it can see trough the iron-concrete structure.
- Civil tetra might use encryption.
- Investigating the data safety

When the management chooses a communication protocol, the security and integrity officer should provide at least a quick description of risks. The know-how is part of the asset such like a part or a product a material or a tool. The easiest way to loose the know-how, if the staff is taking it out from the factory. If they loose a job, they are able to take the know-how with them and next day are able to sell the information for the concurrence. Some other method might be if the camera system is hacked and provides information for someone else. Food manufacturing is mostly not so high-tech, so no point to do it in this way but actually the sales forecast plan is a valuable document for the concurrence. The market is so small, that obviously easier to make some phone calls and have some details from the competitors management as a favour if pre sales data is required.

Actually some of the data is good for the supplier, who wants to sell machinery or some other contractors who might want to cover their fault by making another fault somewhere else within the firm. This situation is very hardly provable. Just like an example in the FMCG sector the cleaners can pressure wash everything including the ceiling and the power switch panels also and then blame the Maintenance staff for bad maintenance. If the fire alarm system is pressure washed it is straight away affect the object security and the root cause could have been easily tracked by a modern PDA solution.

Let's say one of the machine fails due to cheated cleaning procedure. If the maintenance contractor is allowed to make pictures at site, he is able to prove the moisture in the panel, which obviously makes straight forward, that his bill will be paid or at least covered by the Insurance. As soon as is not allowed to make a picture at site, only with the attendance on any technical staff, this picture becomes a valuable data and should be saved and kept as one of the Critical Control Points (CCP). One of the solution is, if there is not allowed to take in smart phones at all. If only authorised people are allowed to take pictures at site, the maintenance procedures are much more controlled. Basically taking out the phones from a factory nowadays can make the staff mourning. HR must have a full understanding about the better Supply Chain integrity without phones otherwise they will not support the idea.

As we can see the communication of the mobile phones are not secure at all. Even the iPhone is easily hacked by the Israeli government [13] the Android has many weak points also. Actually the government might reach the data easily.

CASE STUDY

Infrastructure investigation

Some cases the factory has a basement, which is full with machinery, like air handlers, motors and drivers. They might make additional RF noise. Also if the plant has many buildings the other weak point is the distance. The draft version of the investigation (forecast data only) does not require site attendance. The week points can be estimated by checking the factory layout only. On Fig.2. as a sample project there is map about the biggest yoghurt manufacturers site located at Budapest. The author never been to this site, only Google map was used to provide data to fill the Estimation Sheet. The resolution of the map is limited, but still usable and free of charge. Using AutoCAD we are able to draw draft plan about the layout, which can be seen of Fig.3. The drawing is a simplified map, showing only the required depth of the site for designing.

Fig2. Map for the sample project. Source: (using [14] edited by the Author)

We are able to find the fence on the picture as well. This part, specially the North and West side can be marked as maximal distance from the entrance. The fence should be checked on a regular basis by the Guards. Having good connection is essential for human safety and object safety. Most of the time the Security Office is close to the entrance. The maximal distance is about 300 meters which is not too much for a hand held industrial RF radio, but PMR solution would be too week to cover the communication.

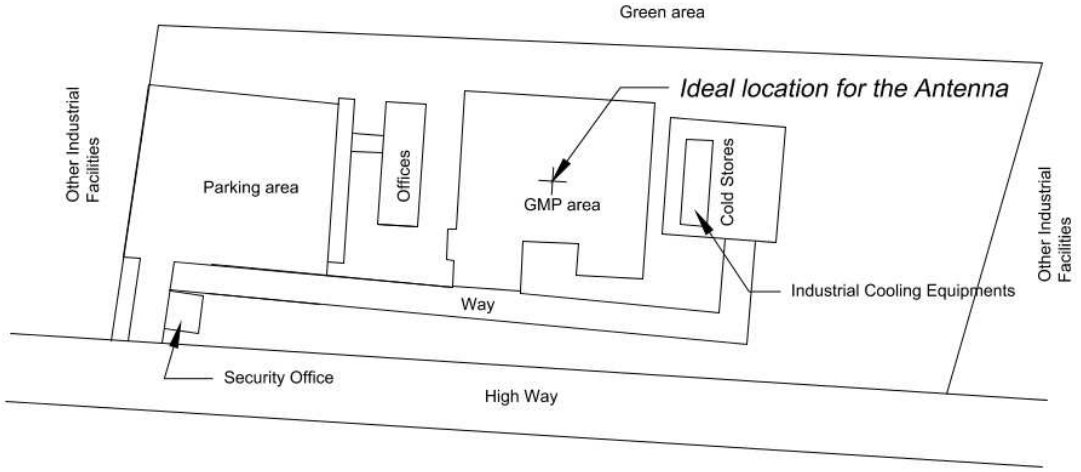


Fig3. Schematics form the plant. Drawn by the Author.

Actually the main building and all the small buildings are acting as shields [11], specially the metal roofs (blue on the picture). Even the main building is much closer to the Security Office the signal strength might be much weaker compared to the fence. If there is a basement, the weakest point might be there.

There is a huge plant room providing cooling energy. This place is mostly very noisy meaning the normal noise and the RF noise as well. In case of maintenance the Engineer should reach the Security Office for Security Officer's permission. The main reason is that most of the time to local fire alarm system or gas detector system should be suspended until the end of the maintenance task.

Install the units

The distance in radio to radio communication as a worst case is at least double distance, than when using a relay station. The relay should be installed to the centre of the plant to as high as possible. One of the best option is an industrial chimney is the architect agrees. Alternatives are the water tower or a standalone beams. If the building has an area which is really screened, like a server room or x-ray room it can be controlled with an extra substation or cover by an extra rule. If everybody agrees that the server room it is not contactable through a radio device, it can be handled as an exception in the policy.

Earthing

Lightning protection equipment is helpful during installation. Prior to any install the lightning protection certificates should be checked or renewed in case of need. During the survey any corrosions on the Earthing cables might show a sign of weak earthing. Lindab based halls are earthed, and they act up as screen for the signal.

Antenna and cabling

To cover an average site 3-4 element Yagi antenna is a good option, especially if vertically installed. The vertical polarisation is better for handheld devices. Most cases the user holds the radio in vertical position. As the Yagi has about 4 dB gain [15] to one direction, the signal is focused to the site. Basically it means that the main station can pick up signal easier from the main direction, and less power is enough for the communication. The station uses coaxial

cables most cases to connect the station to the antenna. The cable must be specified for the used frequency, the impedance must meet with the specs. The cable has more attenuation if narrower. In normal conditions coaxial cables should be shorter than 15 meters, otherwise the most power disappears in the line and not transmitted out. Should the install conditions require longer cabling -as a last result-longer cable might be used, but its diameter should be extended to keep the overall loss below 3dB. [16]

CONCLUSION

Within FMCG sector the in-house RF communication is essential. One of the best and reliable solution is the Civil TETRA, but a shared service of GSM phone and PMR service is a cheaper but still reliable solution. GSM service might be used in this case for office communication. Industrial PMR solution might be used for the in-house services and engineering. In confined spaces, such like industrial tanks, server rooms the landline and the high power PMR might be a good option. The decision is usually made by the management (board) who are comparing the costs and the payback based on the Engineering Managers forecast. Even cost are important the Civil TETRA has an added encryption package which is useful for integrity.

References:

[1] The Telegraph: What is FMCG? Online: https://jobs.telegraph.co.uk/article/what-is-fmcg/ (downloaded: 4/10/2016)

[2] 2009. évi CLV. törvény a minősített adat védelméről Online: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0900155.TV (downloaded: 11/04/2016)

[3] Margaret Rouse: Key performance indicator, www.Techtarget.com Online: http://searchcrm.techtarget.com/definition/key-performance-indicator (downloaded: 14/12/2015)

[4] generisk.hu: SKET, Online: http://www.generisk.hu/sulyos-karesemeny-elharitasi-terv.html (downloaded: 16/12/2015)

[5] ISPE: What is GMP? Online: http://www.ispe.org/gmp-resources/what-is-gmp (downloaded: 02/05/2016)

[6] NAEM: What is EHS? Online: http://www.naem.org/?page=What_is_EHS (downloaded: 03/05/2016)

[7] GSMhistory.com: Who created GSM? Online: http://www.gsmhistory.com/who_created-gsm/ (downloaded: 01/04/2016)

[8] Huszár István: Az IFS rendszer bevezetésének főbb lépései, QHI Online: http://www.qhi.hu/Elelmiszerbiztonsag/IFS/Az%20IFS%20rendszer%20bevezetese.htm (downloaded: 01/04/2016)

[9] Ian Pole: PMR446 Frequencies & Channels Online: http://www.radio-electronics.com/info/pmr-business-land-mobile-radio/pmr446/pmr-446-frequencies-channels-bandwidths.php (downloaded: 05/04/2016)

[10] URL: https://eledia.science.unitn.it/showcase/tetra-hostess/ (downloaded: 05/04/2016)

[11] Az Információs Hadviselés alapjai, ZMNE, Egyetemi Jegyzet, 2000

[12] Vertex Standard, VX230 Series Operating Manual online: http://www.vertexstandard.com/anz/wp-content/uploads/VX-230_OM_USA_EXP_EU_ENG_EC085U104.pdf (downloaded: 05/04/2016)

[13] Tova Cohen: Israeli firm helping FBI to open encrypted iPhone: report, Reuters.com online: http://www.reuters.com/article/us-apple-encryption-cellebrite-idUSKCN0WP17J (Downloaded:12/03/2016)

[14] Danone Plant at Google maps, URL: https://www.google.hu/maps/place/Danone+Tejterm%C3%A9k+Gy%C3%A1rt%C3%B3+%C3%A9s+Forgalmaz%C3%B3+Kft./@47.4876109,19.2005396,16z/data=!4m5!3m4!1s0x4741c385b6598c49:0xaed40d98a50b3d8c!8m2!3d47.4876073!4d19.204917!6m1!1e1

[15] Karl Rothammel: Antennakönyv Online: http://ha5cfj.hu/dm2abk/main.html (Downloaded:04/05/2016)

[16] RG58 Datasheet Online: https://www.pasternack.com/images/ProductPDF/RG58C-U.pdf (Downloaded:04/05/2016)

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Andrea TICK – Dalma VINNAI
Tick.Andrea@uni-bge.hu - dalma.vinnai@hotmail.com

INTERNET OF THINGS – MONITORING THE HUNGARIAN BUSINESS SECTOR AND CONSUMERS

Abstract

Humanity runs towards automatization in every aspect of life. Daily processes become automatized, the environment as well as the tools we use every day. By following this pattern we create a possibility for an easier, more predictable and enjoyable lifestyle. It is presumable that in a few decades everything will be connected with everything, controlled centrally by people, driven by machine learning techniques and relying on Internet connection. These changes will affect our lives significantly, however, there is no other option in order to maintain the sustainability of our environment. Internet of Things (IoT) will have an important role in private life as well as in business. It will give the opportunity to monitor devices and processes more accurately, mining huge amount of data and create precise and predictable statistical forecasts. Nevertheless, it will have an impact on revenues, operational costs, capital expenses, human resources, marketing and sales strategies, technical innovations and the operation of enterprises as well. It will change the culture of business and the culture of life. This paper focuses on the IoT phenomenon, its construction, purpose, the analysis of the underlying solutions as well as discusses the potential growth of the future Hungarian IoT market and analyses the Hungarian consumer.

Az emberiség az élet minden területén az automatizálás felé rohan. A napi folyamatokat, a környezetünket, az eszközeinket automatizáljuk abban reménykedve, hogy egy könnyebb, kiszámíthatóbb és élvezhetőbb életstílust tudunk kialakítani. Várhatóan néhány évtized múlva minden mindennel össze lesz kötve, központilag emberek által irányítva, gépi tanulási módszerekkel vezérelve és internet kapcsolatra hagyatkozva. Ezek a változások alapvetően megváltoztatják az életünket, azonban, a környezet fenntarthatóságának érdekében elkerülhetetlen. A „dolgok interneté”-nek (Internet of Things (IoT)) része lesz mind a hétköznapi mind az üzleti életben. Lehetőséget ad az eszközök és a folyamatok precízebb monitorozására, adatbányászatra és pontos, kiszámítható statisztikai előrejelzések elkészítésére. Hatása lesz a bevételekre, a működési, a tőke, az emberi erőforrás, a marketing költségekre, az eladási stratégiára, a technikai innovációkra és a vállalati működésre is. Megváltoztatja az üzleti kultúrát és az életminőséget. Ezen cikk az IoT jelenséget vizsgálja, annak célját és a mögöttes megoldásokat. A cikk megvizsgálja a magyar IoT piacban rejlő potenciális növekedést, és elemzi a magyar felhasználót.

***Keywords**: IoT; Internet of Things; big data; data mining*

INTRODUCTION

Although we refer to IoT (Internet of Things) as one of the newest innovations of information technologies, it has been an existing scientific area for several years. Strictly speaking, it literally applies to things or devices connected to the Internet, collecting data about user habits and device activities, forwarding these to cloud-based servers which store them centrally and provide the opportunity to create forecasts by using them. Although there is a huge hype around IoT nowadays, the concept existed for decades [1]. "Conventional diagrams of the Internet include servers and routers and so on, but they leave out the most numerous and important routers of all: people…. If we had individual and self-thinking computers, they could use the data gathered without any help from people's side – we would be able to track and count everything, and greatly reduce waste, loss and cost" [2]. IoT has "the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction". IoT solutions could be based on wireless technologies (Bluetooth, NFC), the Internet and micro-electromechanical systems, for example RFID (Radio Frequency Identification) [3]. RFID and sensor technology enable computers to observe, identify and understand the world—without the limitations of human-entered data. The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so" [2]. According to Gartner [4] "The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment".

The broadband addressing IPv6 overcame the constraints imposed by the limited address space of IPv4 and enabled the massive expansion of Internet of Things devices. Based on the statement made by Steve Leibson, "the address space expansion means that we could assign an IPv6 address to every atom on the surface of the earth, and still have enough addresses left to do another 100+ earths" [3].

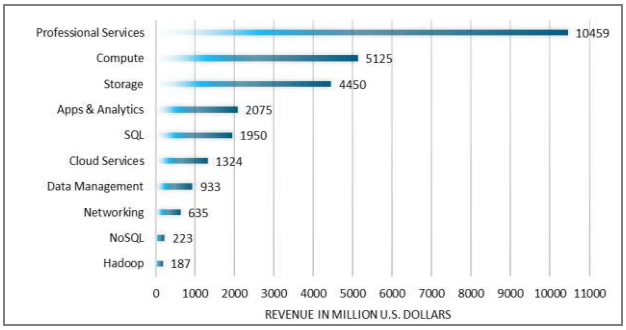
THE UNDERLYING TECHNOLOGY

Building a platform, such as Internet of Things needs underlying technologies which aim to secure the proper functioning of the solution. In order to create an automatized IoT environment, not only devices with sensors are needed, but also a communication channel between the devices, the capability of the devices to communicate; a cloud storage, where data could be stored; analytical formulas which can analyse the collected data; the ability of machine learning, and precisely written commands which instruct the machine to act in a certain way.

Big Data

Without the term 'big data' it is quite impossible to talk about Internet of Things as a service innovation. Since every single IoT device produces massive amounts of data, in order to analyse them, we need the capabilities of cloud computing and built-in solutions, such as BI of big data. The appearance of bigger storages, such as the cloud, enabled us to collect our specific data set in one single place. Today many enterprises started to collect, store, compile and analyse massive amount of data in real time, and we indicate it as 'big data' in consideration of the 3Vs: *velocity* (speed of data), *volume* (amount of data) and *variety* (the range of data types). A fourth V has also been announced that has an impact on data [5]: *veracity*, which expresses the uncertainty of the data. Since the needs of businesses have changed there is a huge demand for "powerful, new analytical techniques and data-sharing models to handle the size and complexity of the necessary data-processing operations" [6].

Figure 1. shows the statistics in 2014 how big data affected each segment of business globally in terms of revenue.



1. Figure. Global big data revenue by segment in 2014 (in million US dollars) [7]

1. Volume

With the appearance of Internet, businesses and enterprises became capable to monitor human behaviour through their online activities. While each purchase is recorded during e.g shopping online, the server also stores the time and date when the purchase has occurred. „As firms have moved their day-to-day operations to computers and then online, it has become possible to compile rich data sets of sales contacts, hiring practices, and physical shipments of goods. Increasingly, there are also electronic records of collaborative work efforts, personnel evaluations, and productivity measures. The same story can also be told about the public sector, in terms of the ability to access and analyse tax fillings, social insurance programs, government expenditures, and regulatory activities" [8] According to certain IBM research [5] about 2.5 quintillion bytes (approximately 2.3 trillion gigabytes) of data are created each day, and with a vague estimation, it is forecasted that 40 zettabytes (43 trillion gigabytes) of data will be created a day in 2020, an increase of 300 times from 2005. Based on the research it is shown that 100 terabytes data are stored by a U.S. company on average. The same amount of data created by IoT devices and the amount generated by YouTube videos stand in need of capacity differently.

2. Variety

Variety is another decisive feature in terms of big data. As the system should be able to collect different types of information on a large scale, starting from monitoring the hours of sunshine, through the amount of precipitation, and the consumption of the electrical system; the capacity for collecting such variety needs to be extended. At the same time, calculating capabilities must be raised extremely in order to become able to monitor upcoming data from different IoT devices.

3. Velocity

Examining velocity means collecting information about the speed of data which is dominant in many ways. As one part of IoT devices has to transfer information in real time and need to change the circumstances in accordance with the collected data, this feature is a determining one. The success of a business depends on the velocity of the data transmission.

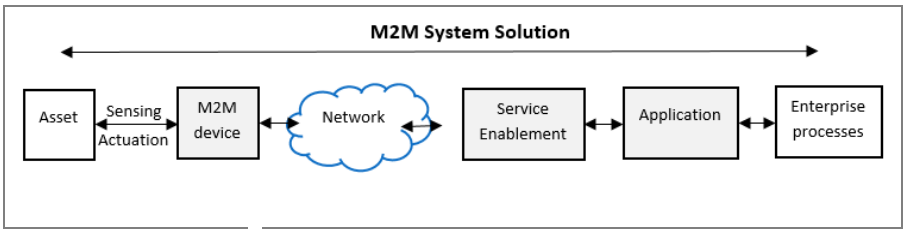
Machine Learning

Machine Learning means "weak" or "specialized" artificial intelligence – a machine that recognizes patterns in data and learns to perform a specific prediction, but has no general intelligence. The opposite end of the spectrum would be "strong" Artificial Intelligence, a machine that can solve general problems like a human. Machine Learning enables the

machine to monitor and analyse a large amount of data sets. Even if the examined information is extremely complex and the deviation is significant, the machine could still define correspondence and relations between the data [9]. Machine learning can be valuable in predicting outcomes as in healthcare, or e.g. in filtering spam emails. Machine Learning is grouped from different aspects, supervised vs. unsupervised, active vs. passive, online vs. batch learning. The role of the training, test and validation data sets, the active or passive role of the learner and the method of online or batch learning all depend on the task to be executed.

M2M communication

The M2M is a solution which enables the communication between devices of the same kind and a certain application, through a wired or wireless network. In general, the machine-to-machine communication is deployed to reduce costs, increase safety or achieve productivity growth [10]. M2M communication happens between devices through different connection channels, such as Bluetooth, RFID or magnetic information routes. In case of M2M, data sharing or the connection between devices through the Internet is not always supported. Reasons could be the lack of lasting batteries and the fact that the typical IoT devices with sensors are not smart enough to be able to connect to the Internet directly. Figure 2. displays a typical M2M solution that is composed of M2M devices, a communication network which enables the connection between devices, an application logic and the integration of the M2M apps into business processes.



2. Figure. M2M System Solution [10]

Security of IoT

Basically two types of security methods are needed, firstly, the protection of the devices, the data on them, and securing a save communication path between different things. This requires hardware security on the devices, and software related protection through the communication channels. The other security concern is storing the collected data by sensors/IoT devices in the cloud. Storing information in the cloud raises human-related concerns as well. Data is easily accessible, needs hardly any hardware capacity, however, on the other hand, storing all the data in the cloud requires intelligent encrypting and high level security using alternative methods in encryption.

Cloud computing

Finally, we have to mention cloud computing as a key component in the usage of IoT since the storage of massive amounts of data at a business enterprise would be too complicated, expensive and exhausting. When it comes to analyzing the huge amount of data collected by IoT devices the attributes of could computing like “infinite computing resources”, virtualization, dynamic flexibility and scalability, cost reductions are among the ones to be explored and utilized. With cloud solutions, CFOs can stop worrying about capital expenses, and start covering the company’s license and IT cloud infrastructure needs monthly as operational expenses. This will not only result in cost optimization, but will take over the

responsibility to maintain the infrastructure from businesses – since cloud providers will handle it –, and also will improve the productivity, because the data and solutions are available from anywhere. It will also have a significant impact on innovating the companies and evangelize them with the newest and most up-to-date software solutions [11].

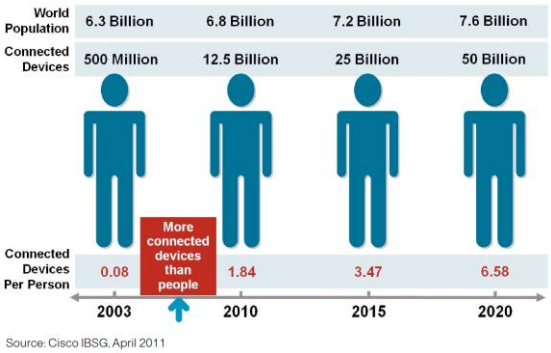
IOT INITIATIVES AND MARKET POTENTIAL

A.I.O.T.I. is last years' most impressive initiation by the European Union. "Aware of the potential of using the IoT, in March 2015 the European Commission initiated the Alliance for Internet of Things Innovation (AIOTI), aiming at creating an IoT Ecosystem that would enable Europe to get a global lead in this field and foster a Digital Single Market (DSM) for IoT. The overall goal of this Alliance is, therefore, to strengthen links and to build new relationships between the different IoT players (industries, SMEs, start-ups, stakeholders) and sectors, also promoting interoperability and convergence between standards, thus facilitating policy debates, and preparing a Commission's initiative for large scale testing and experimentation, scheduled for 2016" [12]. Although the alliance was just recently born – roughly about 8 months ago – already 325 members have joint the network from different sectors and industries like manufacturing, healthcare, mobility, automotive, supply chains, energy, utilities, cities, buildings, lightning, etc. The alliance intends to bring together key IoT market participants both from the public and the private sector. Members become able to contribute in shaping IoT-related EU regulations and could participate in large-scale pilots as well. It does not matter if a company comes from the small-and-medium sized segment, as a start-up, or as a large company (IBM, Bosch, Intel, Cisco), everyone has equal possibilities to contribute in this fellowship.

In November, 2015 Gartner [13] held one of the most important events amongst CIOs and Senior IT Executives, the Gartner Symposium/ITxpo. Among other things, Gartner shared its newest research findings on IoTs and the impact it could bring into businesses by 2020. According to this, the company forecasted a significant growth in the number of IoT units in specific segments. Data provided by high qualified analysts presume that almost 21 billion devices will exist by 2020 which will be referred as IoT solutions. This is an astonishing number, but highlighting the incredible revenue effect it could present in the business area, it could be a strong negotiating fact as well. Furthermore, Gartner [13] also stated that the endpoint spending in businesses will reach 1 477 billion US dollars based on current statistical data [13].

Intel predicts that the 2 billion IoT devices used in 2006 will grow to 200 billion by 2020. According to their projection, about 26 devices will surround each person on the Earth. Knowing this number, it would be expected that most of the devices will play an important role only in the consumer sector, however, the biggest part of these devices will be used in major industries, such as business-manufacturing (40.2%), healthcare (30.3%), retail (8.3%), security (7.7%) and transportation (4.1%) [14].

According to Cisco [15], by the end of 2020, 6.58 IoT devices will be "attached" to one person, and altogether, 50 billion IoT tools will be in the market for the entire population as seen on Figure 3. It seems an extremely overestimated number compared to the statistics of Gartner, but Cisco goes even further. According to the company, the 6.58 devices per person is relatively low, since the overall number of devices were divided by the number of the entire population. However, many people of the current 7.2 billion do not have access to the Internet, and it is roughly estimated, but around 3 350 million people use the Internet today [16]. By implementing this number into the figure, "the number of connected devices per person jumps up to 7.57 in 2015, instead of 3.47" [16].



3. Figure. IoT devices per person [15]

IDC also forecasted that "by 2017, 90% of datacentres and enterprise systems management will rapidly adopt new business models to manage non-traditional infrastructure and BYOD (Bring-Your-Own-Device) categories. Just as by 2018, 16% of the population will be millennials and accelerating IoT adoption due to their reality of living in a connected world" [17].

THE ANALYSIS AND POTENTIALS OF THE HUNGARIAN MARKET

The statistics above could easily make people wonder whether the change will be that significant all around the world or just in certain parts of it. That is why examining the effects it will have on the Hungarian market and businesses of the country is crucial. On the IoT market the statistical forecast by Gartner [4] are the commonly accepted standards. As Table 1. shows Gartner distinguished the IoT markets based on the areas of presence. Our analysis focus on the Hungarian business segment since it has a bigger potential in development than the customer segment.

1. Table. Internet of Things units installed based by category (million units) [13]

Category	2014	2015	2016	2020
Consumer	2,277	3,023	4,024	13,509
Business: Cross-Industry	632	815	1,092	4,408
Business: Vertical-Specific	898	1,065	1,276	2,880
Grand Total	**3,807**	**4,902**	**6,392**	**20,797**

Table 2., however, displays the IoT endpoint spending by category. It calculates with a 115% increase, having 682 billion dollars in 2014 going up to 1 477 billion by 2020.

2. Table. Internet of Things endpoints spending by category (billions of dollars) [13]

Category	2014	2015	2016	2020
Consumer	257	416	546	1,534
Business: Cross-Industry	115	155	201	566
Business: Vertical-Specific	567	612	667	911
Grand Total	**939**	**1,183**	**1,414**	**3,010**

Although building a country specific statistical forecast based on international trends could be misleading, since the revenue and unit growth could differ based on other country specific factors like the geographical places, a country's economic situation and economic growth potentials, GDP etc. however, it still could show a theoretical potential obtainable in the national market.

The current research in this field is restricted to only such companies that provide complex solutions of IoT devices with sensors, where the collected data is stored in the cloud, BI and

big data analytics are provided to enable data processing and analyses, and which have an overall sense of innovation, such as remotely controlling the IoT devices located in homes. That is the reason it was crucial to focus on the innovation part of IoT, What made the research difficult is that the Hungarian IT market is extremely small and, at the same time, the target group is much smaller compared to other markets. When analysing the Hungarian market it is crucial to know the consumers and their attitude towards IoT, since they drive the market and part of the business demand. According to the Principal Software Engineer of LogMeIn, the Hungarian market has some disadvantageous factors that set back the Hungarian IT market from outstanding and rhythmic growth. In the Hungarian market language barriers still hinder the proliferation of IoT devices resulting in differing preferences compared to the international market. Furthermore, the adaptation to new things and solutions is also slower. A further obstacle is that the Hungarian consumers are extremely price sensitive and finally, that the Hungarian legal process of approval to import new innovations to the country is lengthy, cumbersome and complicated. By the time an IoT gets a green light it becomes out-of-date. Consequently, to boost the spread of IoT devices the Hungarian market would need either more Hungarian vendors developing IoT solutions or create a less complicated legal regulation system for IoT innovations to enter the country.

According to IDC (International Data Corporation) Hungary [18], which is the only research company in Hungary that has already dealt with the analysis of the significance of the IoTs and M2M devices in the national market, the IoT device market should be split into different groups: one of them uses only M2M and GSM solutions and the other one covers all of the IoT devices which is presented in the market. Since the M2M communicating devices with SIM card have a significantly simpler technology than solutions with RFID, NFC, Bluetooth and the Internet, this is going to be analysed first in this chapter.

As Gartner differentiated the segments using IoT, IDC did the same as well, but they created smaller and more specific groups, such as Fleet Management, Security, Commerce, Smart metering, Health and Other. They also divided the market by layers, such as Hardware, Service, and Access. Fortunately monitoring the number of IoT devices using SIM card is a lot easier than those without it.

It is crucial to mention that IDC counted SIM cards used by only those devices which are not used by consumers. Therefore phones, 3G capable tablets, and any interacting devices are excluded from these numbers. More precisely an M2M SIM card could be built in a home alarming system, or any IoT device-like tool, the difference is that these devices are not able to communicate through the Internet or any other communication channel (RFID, Bluetooth, and NFC).

Table 3. shows the actual and the expected number of M2M SIM cards between 2013 and 2017, and displays that the M2M SIM card market could more than double just in 4 years. This suggests that in the next 2 years many innovations could twist into the market. Since this is only one part of the IoT devices, much larger growth could be expected. The strongest rise is visible in the commerce segment, especially between 2013 and 2014 (a 321% growth), but knowing the facts, that the government made an obligatory POS terminal change from offline version to the online POS cash-registers, this is totally understandable.

3. Table. M2M SIM Cards (pcs)

	2013	2014	2015	2016	2017
Fleet Management	109 000	152 000	173 000	187 500	200 000
Security	145 000	150 000	155 000	165 000	175 000
Commerce	56 500	238 000	250 500	315 000	360 000
Smart metering	75 500	87 500	92 500	117 500	137 500
Health	10 000	12 000	14 500	18 000	25 000
Other	119 500	139 500	162 500	192 500	242 500
Total	**515 500**	**779 000**	**848 000**	**995 500**	**1 140 000**

a. Source: IDC interview November 2015

In terms of spending, however, different numbers are represented. The largest growth is expected in the field of smart metering, forecasting a 77.32% annual growth between 2013 and 2017 (See Table 4.).

4. Table. M2M spending by segment - 2013-2017 (HUF million)

	2013	2014	2015	2016	2017
Fleet Management	6 968	9 890	9 388	9 490	9 980
Security	11 490	11 375	11 658	12 815	13 285
Commerce	3 980	18 619	7 363	10 825	8 570
Smart metering	1 973	1 453	4 397	24 006	19 506
Health	598	616	714	860	1 280
Other	7 223	7 816	8 867	10 345	13 692
Total	**32 232**	**49 770**	**42 385**	**68 341**	**66 314**

b. Source: IDC interview November 2015

The two most developing layers will be hardware and service as seen in Table 5., which is absolutely not surprising in case of IoT solutions. New devices will be presented in the market since the demand for service boosts innovation and import. The growth of hardware is inevitable because of the new devices, and, at the same time, the demand for services will grow both from the consumers' side, but from the vendors' point of view. This could result in a market gap waiting to be filled. Providing services for vendors – such as predictive analysis – could result in preventive maintenance, therefore, companies will be able to revise their services and products. Table 5. shows a 24.42% and a 18.07% annual growth in the hardware and a service market respectively, so hardware is expected to outgrow the service demand. This was also justified by LogMeIn, who bought up Xively [19], an originally UK-based company, to provide a much needed and adequate service for vendors developing IoT solutions.

5. Table. M2M spending by layers 2013-2017 (HUF million)

	2013	2014	2015	2016	2017
Hardware	12 779	25 227	16 080	36 464	30 624
Service	15 224	19 140	20 861	26 080	29 585
Access	4 228	5 403	5 444	5 798	6 105
Total	**32 232**	**49 770**	**42 385**	**68 341**	**66 314**

c. Source: IDC interview November 2015

Table 6. gives a rough forecast of revenues from the IoT devices in the future Hungarian industrial market till 2018 provided by the Principal Software Engineer of IDC. The forecast was created by a joined work of the Czech and the Hungarian subsidiaries. According to the forecast the Hungarian IoT market is expected to jump by 150% in terms of revenue (in $

millions) between 2013 and 2018. Comparing the IDC and Gartner forecast, we can examine the years from 2014 and 2016 and calculate an expected growth from them.

6. Table. Hungary IoT spending ($ million)

INDUSTRY	Revenue in year (million $)					
	∑ of 2013	∑ of 2014	∑ of 2015	∑ of 2016	∑ of 2017	∑ of 2018
Consumer	147,41	186,88	272,56	336,08	447,72	509,99
Government	284,70	317,37	386,27	427,01	527,74	589,73
Healthcare	55,55	64,22	77,06	87,50	104,38	120,73
Insurance	0,54	0,70	0,88	1,13	1,47	1,73
Manufacturing	68,76	84,06	103,90	117,11	144,93	164,27
Resource Industries	1,65	1,73	1,88	2,01	2,29	2,44
Retail	1,61	1,94	2,25	2,76	3,31	3,83
Transportation	58,65	65,36	75,57	87,24	111,36	125,18
Utilities	3,97	4,87	6,19	8,10	11,63	16,54
Cross Industry	7,28	9,32	11,58	15,69	22,66	30,86
Other Industries	53,11	58,07	79,23	91,12	116,27	128,97
Grand Total	683,23	794,53	1 017,38	1 175,75	1 493,75	1 694,26

d. Source: IDC interview November 2015

IDC forecasts a 48% growth in terms of total revenue from 2014 to 2016, which is in compliance with the Gartner forecasts of the international market since it expects a 50% growth in the IoT market in terms of revenue. (from $ 939 billion in 2014 to $ 1414 billion in 2016). According to this, Hungary, even with its disadvantageous market circumstances, is capable of following the international market trends.

CONSUMER ATTITUDE TOWARDS IOT IN THE HUNGARIAN MARKET

The Hungarian IoT market has some drawbacks compared to the international market since it is relatively small, consumers have language barriers thus having special needs that the producers and the vendors need to react to. The previous chapter dealt with the industrial, cross-industrial sector. However, if this market has such a big potential, then the consumer attitude towards IoT devices on the Hungarian market is also expected to change and follow the international trend. The research, which finally gave a non-representative sample, but made it possible to draw some conclusions surveyed 132 people, out of which 112 answered the online survey. The age of the surveyed ranged between 18 and 65, 68% of them being between 18 and 25 (Generation Y). At the same time 68% of the surveyed was aware of what IoT was but only 37% of them considered it a super innovation. 32% of the surveyed did not care about IoT or have not heard about it, which raises the question whether it is as popular as the market situation presumes. The results also showed that 81% of these people had at least 1 smart device, which is presumably a smart phone. The sample showed an average of 2.6 devices meaning 2 or 3 smart devices. This device is probably a smart phone, since Statista [7] states that only in 2014 approximately 1.2 billion smart phone units were sold to end-users. Approximately 3% of the surveyed stated that they had more than 10 smart devices. According to Statista [7], the number of people who will use smartphone by 2019, will increase by 67%, and by 2018 almost 37% will be the penetration of the total global population which uses smartphone [7].

Comparing the spending on smart devices or IoT the survey gave the following results. While the surveyed people spend an average HUF62 500 on smart phones they would spend an average HUF424 137 on IoT, which is a remarkable difference. In the first case roughly 83% of the surveyed spend under HUF100 000 on smart devices while in case of IoT devices

83% of the surveyed would spend under HUF300 000. Most of the surveyed would spend between HUF 50 000 and HUF100 000 on IoT. Using the population data from the Central Statistical Office [20], the number of population between 25 and 65 was roughly about 6 664 153, so the average annual amount of money a consumer in Hungary would spend on IoT devices would be between HUF 326 thousand and HUF552 thousand (90% confidence), while the total spending would be between HUF2.2 billion and HUF3.5 billion (90% confidence).

7. Table. The amount of money people would spend on smart devices

Spent amount of money (thousand HUF)	Number of people
None	9
0 – 50	60
51 – 100	28
101 – 200	11
201 or more	8
Total:	***116***

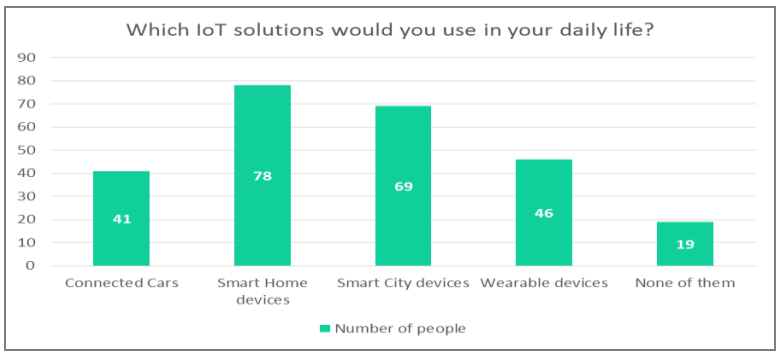
e. Source: Online survey

8. Table. The amount of money people would spend on IoT devices

Spent amount of money (thousand HUF)	Number of people
0	4
1 – 50	22
51 – 100	28
101 – 200	22
201– 300	11
301 – 700	7
701 – 1 500	6
1 501 or more	16
Total:	***116***

f. Source: Online survey

Grouping the IoT devices people gave the following answers as seen in Figure 4. As it shows smart home and smart city devices have a significant potential in the market.



4. Figure. Distribution of IoT solutions people would use in daily life

The following factors were among the fears and threats mentioned as risk factors that keep people away from IoT solutions: risk of over automatization; avoiding independent thinking; disaster management; untraceable data moving; data theft; lack of data security; hacker attacks; threat on community security; lack of personality rights; cyber criminality; technology addiction; depending on digitalization; non-technology people will be unable to follow the system.

Based on personal opinions most of the surveyed people expect to use only machine driven devices by 2050. These opinions are rather pessimistic compared to the prognostications made by research companies. The main blockers are the lack of IT knowledge and fears of new technologies. Another barrier could be the situation of the Hungarian economy and market, the average salary of people, which lead to less possible spending on IoT solutions. Education on IoT might also significantly impact the attitude of the consumers. Until this gap is not solved adequately, no significant growth can be expected in the consumer market.

CONCLUSION

It is unperceivable that Internet of Things as an innovation will have a huge impact on our life. It will not only affect the way we live, business and everyday processes, but finally will provide a solution for many problems, such as sustainable environment, waste, energy and traffic management, possible issues in logistics. With the help of it, we will be able to create smart cities and homes, and absolutely involve the technology into our life. IoT devices will play a significant role in urban transportation, healthcare and agrarian solutions as well. The tools we use in our everyday life are going to be developed and appear on the market as IoT devices.

Internet of Things couldn't exist without many solutions we already have today. Big data, machine learning, machine-to-machine communication and cloud computing will have a huge role in the creation of IoT environments. Spending time, money and effort on the development of the above mentioned solutions is crucial. In time, everything will become controllable and trackable from anywhere with the help of Internet, and everything become connected to everything with the help of secondary solutions such as cloud computing, machine learning, etc. The devices will generate and collect massive amounts of data, then store them locally on the device itself, but essentially transfer them to the cloud.

However, with the appearance of innovative solutions and devices, serious concerns raise as well. Vendors still have to find solutions to store the consumers' data anonymously, safely and securely, but at the same time make it possible to track the devices and transfer the collected data to the cloud for review only by authorized people. If we want to keep the quality of the products and services provided by IoT, security gaps need to be filled in.

This paper presented that while the Hungarian IoT market in the industrial and business fields is capable of following the international growth, the consumer market will probably leg behind due to economic, financial, security and privacy concerns as well as some human preconceptions about cloud computing, big data, security and privacy.

References

[1] Kobie, N., "What is the internet of things?" In The Guardien, http://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google, 24. 11. 2015

[2] Ashton, K., "That 'Internet of Things' Thing" RFID Journal. June 2009, pp.1.,http://www.rfidjournal.com/articles/view?4986. 26. 11. 2015.

[3] Rouse, M., WhatIs.com. 2014. http://whatis.techtarget.com/definition/Internet-of-Things, 26. 11. 2015

[4] Gartner, 2015. Gartner. http://www.gartner.com/it-glossary/internet-of-things/, 25. 11. 2015

[5] Quintero, D., Genovese, W.M., et.al., "IBM Software Defined Environment˘", IBM RedBooks, IBM, pp. 192, 2015.

[6] OECD, “OECD Digital Economy Outlook 2015”, OECD Publishing, Paris, pp.245. 2015.

[7] Statista, 2014. http://www.statista.com/statistics/301558/big-data-revenue-worldwide-by-segment/, 30. 11. 2015

[8] Einav, L. & Levin, J., “The Data Revolution and Economic Analysis”, the National Bureau of Economic Research, Cambridge, MA, pp.3., 2014.

[9] Érsek, A., Structured Interview, Microsoft, 2015

[10] Holler, J. etz.al.., 2014. “From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence”, Academic Print, Waltham, MA, 2014, pp.11-12.

[11] “Modeling the Economic Impact of Cloud Computing”, KPMG pp.10.-18., 2012

[12] Cousin, P., “About AIOTI” In ‘Internet of Things Success Stories” Vol.3., November 2015, pp.3.

[13] Meulen, R., “Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015”, November 2015 http://www.gartner.com/newsroom/id/3165317, 29. 11. 2015

[14] Intel, http://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png, 2015, 05. 12. 2015

[15] Evans, D. “The Internet of Things, How the next evolution of the internet is changing everything”, CISCO IBSG, pp. 3. April 2011

[16] Internet World Stats, http://www.internetworldstats.com/stats.htm, 2015, 05. 12. 2015

[17] IDC, “IoT Market Forecast: Worldwide IoT Predictions for 2015”, Conference, December 2014, http://iotinternetofthingsconference.com/2014/12/07/iot-market-forecast-worldwide-iot-predictions-for-2015/, 07. 12. 2015

[18] Tóth, L., Interview, IDC, November 2015

[19] Bray, H. 2 LogMeIn: King of the Internet of Things?”, November 2015 http://www.betaboston.com/news/2015/11/07/logmein-king-of-the-internet-of-things/, 29. 01. 2016

[20] KSH, 2015 [Online] Available at: https://www.ksh.hu/docs/hun/xstadat/xstadat_eves/i_wdsd004b.html 05. 12. 2015

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Gyarmati József - Vég Róbert László
gyarmati.jozsef@uni-nke.hu - vegh.robert@uni-nke.hu

A KATONAI LOGISZTIKA ALAPKÉPZÉSI SZAK PÁNCÉLOS- ÉS GÉPJÁRM-ŰTECHNIKAI MODULJÁNAK FELÉPÍTÉSE A KORÁBBI KÉPZÉSEK TÜKRÉBEN, SZAKMAI SZEMSZÖGBŐL

Absztrakt

A cikk a páncélos- és gépjármű-technikai szaktisztek képzésének változását elemzi az elmúlt két évtizedben. Bemutatjuk, hogy hogyan elégítette ki az oktatás a folyamatosan változó elöljárói igényeket, amelyek a gépjárműtechnika szakos tisztek képességeiket és kompetenciákat írták elő. Továbbá bemutatjuk, hogy ennek milyen hatása volt a szakmai órák mennyiségére.

This paper describes the changes of education systems of the logistic officer in vehicle specialization. We show the process that satisfies the requirements of the HDF in the officer training. In this paper is also described the changes of quantity of the lessons of car mechanism.

Kulcsszavak: *logisztikai tisztképzés, mérnök, gépjárműtechnika, képzés, műszaki ~ education of logistics officer, vehicles, engineer*

BEVEZETÉS

A katonai logisztika tartalmazza a haditechnikai-, és ezen belül a páncélos és gépjármű-technikai szolgálatot. Az itt dolgozó tiszteket az elmúlt évtizedekben különböző szinteken és különböző elöljárói iránymutatások alapján, változó keretben, ebből adódóan más-más arányokban kialakított szakmai tartalommal lettek képezve a katonai felsőoktatásban. Hogyan és miképpen érintették ezek a változások a képzések szakmai tartalmát?
Cikkünkben ezen fő kérdésre keressük a választ. Nem kritikát fogalmazunk meg, csak szigorúan a tényekre támaszkodva szeretnénk bemutatni, hogy egy új ismeretanyag, vagy egy új kompetencia hogyan befolyásolja a szakmát. Hogyan kell kialakítani, megtervezni a frissen végzett tisztek által birtokolt tudásanyagot, hogy abba még elfogadható és használható mennyiséget képviseljen a szakmai ismeret? Milyen mértékben kell elvárni a fiatal tiszttől a pályakezdés során az önképzést, vagyis mely ismeretek önálló elsajátítását lehet elvárni, és milyen mértékű pályakezdési segítségnyújtás várható el a csapattól, ahol az első beosztásukat betöltik?

Az oktatásban minden ismeret átadásához megfelelő időre van szükség. Kicsit összetettebb ez a kérdés a szakmai ismeretek esetében. Például a „Rendszerben tartás”, ami már egy olyan tantárgy, amit közvetlenül felhasznál a végzés után a munkájában, nem oktatható előzmény nélkül. Ennek a tárgynak a megértéséhez előtanulmány szükséges, pl. Járműszerkezetek, aminek a megértéséhez viszont megint előtanulmány szükséges (Áramlástan, Hőtan,

Gépelemek), és a sor még tovább folytatható. A szakmai tárgyaknak jól kialakult rendszere és egymásra épültsége van. Nem lehet belőlük elemeket csak úgy kivenni, hiszen ez a rá épülő tárgy megértését teszi lehetetlenné. Tehát ha egy új elvárt kompetencia miatt a szakmai tárgyak mennyiségét kell csökkenteni, akkor nem lehet kiválasztani egy kevésbé fontos tárgyat és azt egyszerűen elhagyni, hanem arányosan mindegyiket csökkenteni kell, vagyis a szakma mindenképpen sérül. A katonai vezetői kompetenciák mellett tehát a szakmai kompetencia kérdése igen összetett.

A katonai főiskolák megalakulásával elindult egy magasabb szintű tisztképzés, amelynek keretében a tantárgyakat tantárgyi programokban rögzítették és dolgozták ki. Ezek a tantárgyi programok tartalmazták az adott ismeretkörök elsajátításának célját, a tantárgy tananyagát témakörönként, valamint a tantárgy helyét és szerepét a képzés rendszerében. [1]

Magyarország alaptörvénye megfogalmazza a Magyar Honvédség alapfeladatát, amelyből következnek a képzés alapelemei. Az alaptörvény szerint: „Magyarország fegyveres ereje a Magyar Honvédség. A Magyar Honvédség alapvető feladata Magyarország függetlenségének, területi épségének és határainak katonai védelme, nemzetközi szerződésből eredő közös védelmi és békefenntartó feladatok ellátása, valamint a nemzetközi jog szabályaival összhangban humanitárius tevékenység végzése.” [2]

A rendszerváltást követően a tisztképzésben a hagyományosnak mondható háborús feladatokra történő felkészítés mellett megjelentek a békeműveleti felkészítés követelményei is. A tisztnek képesnek kell lennie arra, hogy magas színvonalon és eredményesen ellássa szakmai és vezetői feladatait, amelyre a képzés során szintén fel kell készíteni. [3]

A képzési szakok megpróbálják a hallgatókat felkészíteni a mindenkori elvárásokra, ahol a megrendelő igényeit kell teljesíteni. Esetünkben a megrendelő a Magyar Honvédség, aki meghatározza a tisztképzéssel szembeni elvárásait. A megrendelői igények mellett természetesen megjelennek az akkreditációs és felsőoktatási rendszer minőségi követelményei is. Természetesen a széles körű követelmény rendszerben olyan összhangot kell teremteni, hogy a katonai szakmai érdekek is maradéktalanul érvényesülni tudjanak.

A vizsgálat tárgya a három különböző képzési szakon belül (gépészmérnöki szak, had- és biztonságtechnikai mérnöki alapképzési szak, katonai logisztika alapképzési szak) a páncélos- és gépjármű-technikai képzés változásaira terjed ki.

PÁNCÉLOS- ÉS GÉPJÁRMŰ-TECHNIKAI SZAKIRÁNY A GÉPÉSZMÉRNÖKI SZAK OKTATÁSI RENDSZERÉBEN

A szak tantervének kidolgozását meghatározta:

- a felsőoktatásról szóló többször módosított 1993. évi LXXX törvény,
- a katonai és rendvédelmi felsőoktatási intézmények vezetőinek, oktatóinak és hallgatóinak jogállásáról szóló 1996. évi XLV törvény,
- a 157/1996 MHPK VKF intézkedés a felsőoktatási intézmények hallgatói katonai kiképzésével és katonai életre nevelésével kapcsolatos, illetve a 2000 után kibocsátandó tisztekkel szemben támasztandó katonai-szakmai követelményekről,
- a 46/1996 HM utasítás a katonai felsőoktatási intézményeknek a Magyar Honvédség haderejéből történő kiválásával kapcsolatos feladatokról.

A képzés általános céljaként meghatározták, hogy olyan gépészmérnökök végezzenek, amelyek képesek a Magyar Honvédség főiskolai végzettséget igénylő parancsnoki beosztásainak ellátására. A hallgatók kiképzésénél célul tűzték ki, hogy olyan ismeretek birtokában legyenek, amelyekkel tisztként képesek alegységük béke- és háborús

tevékenységét megszervezni, vezetni, beosztottjaik kiképzését irányítani. Képesek legyenek általános katonai és szakmai ismereteiket fejleszteni és a tisztekkel szemben támasztott társadalmi és katonai elvárásoknak megfelelni. [4]

A gépészmérnök szaknak fegyverzettechnikai, páncélos-technikai, gépjármű-technikai és műszaki-technikai szakirányai voltak, de a műszaki technikai szakiránynál nem történt beiskolázás. A kezdeti párhuzamos beiskolázást (páncélos- és gépjármű-technikai) felváltotta a csak gépjármű-technikai szakirányon történő képzés.

A tantervben szakirányonként meghatározták a speciális szakmai követelményeket, amelyek alapjául szolgálnak a kidolgozott tantárgyaknak.

A páncélos- és gépjármű-technikai szakirányú gépészmérnök tisztnek ismernie kellett:

- a szerelési és javítási technológiák megtervezéséhez szükséges természettudományok törvényszerűségeit, az alakító, a hőkezelő, a hegesztő technológiákat, a méréstechnikai, elektrotechnikai összefüggéseket és mindezek ellenőrzésének módszereit, az igénybevétel során bekövetkezhető meghibásodások jellegét,
- az alkatrészpótláshoz szükséges anyagjellemzőket,
- a korszerű haditechnikai eszközök működési elveit, az üzembentartás szabályait, valamint a vonatkozó biztonságtechnikai és balesetelhárítási szabályokat,
- a csapatszintű gazdálkodás feladatait, szabályait, a szükséges számvetések kidolgozásának módszereit, az eszköz- és anyagellátás rendjét,
- a harc logisztikai biztosításának alapelveit, rendszerét, szervezetét, a szakkiképzés általános módszereit és követelményeit. [5]

A meghatározott ismeretek elsajátítását a szak 8 féléves képzési időben 3600 tanóra ráfordítással valósította meg. A szakirányra jellemző ismeretek lefedését a szakmai törzsanyag (33.2 %), a differenciált (katonai-) szakmai ismeretek (17.3 %) és az általános és specifikus katonai tananyag (24.5 %) tanulmányterületek látták el.

A páncélos- és gépjármű-technikai (itt a szigorúan műszaki tartalmú gépjárműves képzést kell érteni) képzést döntően meghatározta a differenciált szakmai ismeretek tanulmányterület. Amennyiben össze akarjuk hasonlítani a különböző képzéseket, és ezeken belül a szakmai területeket, akkor fontos pár meghatározó tantárgyat megvizsgálni, amelyeket az 1. sz. táblázat tartalmaz.

1. sz. táblázat: Főbb tantárgyak a differenciált szakmai ismeretek tanulmányterületből.

	tantárgyak	*óraszám*
1.	Belsőégésű motorok	150
2.	Járművek szerkezete	180
3.	Gépjármű villamos berendezések	120
4.	Rendszerben tartás	210
	Összesen:	660

A táblázatból is látható, hogy ez a négy tantárgy jelentős óraszámmal rendelkezett a teljes képzési időn belüli óraszámhoz képest (18.3 %). A tantervben meghatározott tantárgyak oktatása biztosította a meghatározott ismeretszintek elérését.

A tantárgyak oktatását segítette új korszerű oktatástechnikai és diagnosztikai berendezések alkalmazása is, mint pl. a Smart Board oktatási rendszer a kidolgozott multimédiás tananyagokkal. [6]

PÁNCÉLOS- ÉS GÉPJÁRMŰ-TECHNIKAI MODUL A HAD- ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI ALAPKÉPZÉSI SZAK OKTATÁSI RENDSZERÉBEN

A Magyar Honvédség folyamatos átalakulása, a feladatrendszer változása megkövetelte, hogy a tisztképzés is változzon, és áttérjen a szűk specialista képzésről egy általánosabb felkészítés felé. A korábbi Gépészmérnök, Közlekedésmérnöki, Villamosmérnöki és Informatikai mérnöki szakok összevonásával létrejött a Had- és biztonságtechnikai mérnök alapképzési szak, amely a logisztikai képzés számára optimális megoldást nyújtott. A végzős hadnagyok a végzettségüknek megfelelő szakaszparancsnoki beosztásokba kerültek, így meg kellett teremteni az alegység parancsnoki és a szakági szakmai felkészítések összhangját. Mivel ez a képzés a műszaki képzési területhez tartozott, ezért az akkreditációs követelmények teljesítése és a katonai érdekek érvényesítése is lehetővé vált. [7]

A képzés általános célja olyan had- és biztonságtechnikai mérnökök képzése, akik alkalmasak a Magyar Honvédség haditechnikai, a védelmi szféra technikai eszközeinek üzemeltetésére, fenntartására, a kapcsolódó új technológiák bevezetésére, alkalmazására.

Az alapszakon haditechnikai-, műszaki, katasztrófavédelmi és közlekedési-, katonai elektronikai-, repülőműszaki- és biztonságtechnikai specializációkon folyik a képzés, jelenleg már kifutó rendszerben. *Az alapszak tanterve specializációnként meghatározza az elsajátítandó szakmai kompetenciákat, amely a páncélos- és gépjármű-technikai képzés során az alábbiak:*

- a rendszeresített páncélos- és gépjármű-technikai, valamint műszaki-technikai eszközök és rendszerek üzemeltetésével és üzembentartásával kapcsolatos feladatok tervezése és szervezése,
- páncélos- és gépjármű-technikai, műszaki-technikai eszközök javítását kiszolgáló technológiák és diagnosztikai vizsgálatok bevezetése, alkalmazása, kidolgozása,
- alkalmi harci kötelékek, alegységek béke és háborús tevékenységei logisztikai biztosításához kapcsolódó szakirányú biztosítási feladatok tervezése, szervezése, végrehajtása és irányítása,
- szakalegységek béke és háborús tevékenységeinek tervezése, szervezése, irányítása, a szakmai továbbképzés feladatainak végrehajtása. [8]

A meghatározott ismeretek elsajátítását a szak 7 féléves képzési időben 2880 tanóra ráfordítással valósítja meg. A páncélos- és gépjármű-technikai képzést döntően meghatározza a differenciált szakmai anyag tanulmányi terület kötelező, kötelezően választható és választható tantárgyai. Amennyiben össze akarjuk hasonlítani a különböző képzéseket, és ezeken belül a szakmai területeket akkor fontos pár meghatározó tantárgyat megvizsgálni, ahogyan a gépészmérnöki szaknál is történt, amelyeket az 2. sz. táblázat tartalmaz.

2. sz. táblázat: Főbb tantárgyak a differenciált szakmai anyag tanulmányterületből.

	tantárgyak	*óraszám*
1.	Belsőégésű motorok	165
2.	Járművek szerkezete	110
3.	Gépjármű villamos berendezések	45
4.	Rendszerben tartás	155
	Összesen:	475

A táblázatból is látható, hogy ez a négy tantárgy jelentős óraszámmal rendelkezik a teljes képzési időn belüli óraszámhoz képest (16.4 %). A tantervben meghatározott tantárgyak oktatása biztosította a meghatározott ismeretszintek elérését.

PÁNCÉLOS- ÉS GÉPJÁRMŰ-TECHNIKAI MODUL A KATONAI LOGISZTIKA ALAPKÉPZÉSI SZAK OKTATÁSI RENDSZERÉBEN

A missziós szerepvállalásainkkal átértékelődtek a műveleti felkészítés súlypontjai, vagyis a legjobb szakmai felkészültség sem ér semmit, ha az nem párosul azokkal a katonai ismeretekkel, jártasságokkal és készségekkel, amelyek biztosítják az erők megóvását, a harc megvívását valamint annak vezetését. A tisztjelöltek logisztikai felkészítésénél „nem elegendő a szakasz- és századparancsnoki beosztásokból kiindulni, mivel a fiatal logisztikusok gyakran az avatás után 1-2 éven belül, minden átmenet és közbülső lépcsőfok nélkül a szakaszparancsnoki beosztásból már egység-, magasabbegység-szintű szakági beosztásban találják magukat”. [9]

2010-ben megszületett a döntés egy új nemzeti tisztképzés kialakításáról, amelyben megtörténik a közszolgálati életpályára történő felkészítés is, ugyanakkor a MH Ludovika Zászlóalj megalakításával a honvéd tisztjelöltek katonai szocializációjának szervezeti keretei is létrejöttek. Az Országgyűlés a 2011. évi XXXVI. törvényével döntést hozott a Nemzeti Közszolgálati Egyetem létrehozásáról. [10] Az új képzési feltételek bázisán kialakult egy olyan integrált logisztikai képzés, amely megfelel a logisztikai támogatás doktrinális alapjainak. A képzésben megjelent az egyetemi közös modul, ami biztosítja azon közszolgálati alapismeretek elsajátítását, amelyek lehetővé teszik a későbbi átjárhatóságot a közszolgálati életpályán belül a különböző hivatásrendek között. A katonai logisztikusok számára fontosak ezen ismeretek, mivel a hazai katonai műveletek során szükséges a közigazgatási és rendvédelmi szervekkel a szoros együttműködés.

A Katonai logisztikai alapképzési szak nyolc félévből áll, az alapkiképzés a tanterv részeként bekerült a képzésbe. A korábbi képzés hét féléve nyolcra bővült, de mivel az alapkiképzés és az egyetemi közös modul egy-egy félével lefoglal, így ténylegesen csak hat félév áll rendelkezésre szakmai-katonai felkészítésre. A katonai logisztikai szakmai alapozás egységes rendszerbe került, és a korábbinál lényegesen nagyobb súllyal jelent meg a vezetőképzés témaköre, ugyanakkor meg kellett őrizni a korábbi katonai szakmai ismeretek arányát olyan formában, hogy a vezetőképzés is megvalósuljon.

A katonai logisztikai alapképzési szak tanterve meghatározza az egyes specializációk képzési célját, és az elsajátítandó szakmai kompetenciákat. Jelen esetünkben a páncélos- és gépjármű-technikai képzés a haditechnikai specializáción belül foglal helyet. A haditechnikai specializáció képzésének célja: „az általános és specifikus katonai ismereteik és készségeik birtokában a választott modulnak megfelelő alegység-parancsnoki, és szaktiszti beosztásokban – nemzeti és több nemzeti környezetben, békeidőszakban, válságkezelő-, katasztrófa elhárítási-, béketámogató és háborús műveletekben egyaránt – a haditechnikai biztosítás specializáció feladatai végrehajtásának tervezésére, szervezésére, irányítására, ellenőrzésére.” [11]

A differenciált szakmai ismeretek tanulmányterületből a főbb tantárgyakat a 3. számú táblázat mutatja be.

3. sz. táblázat: Főbb tantárgyak a differenciált szakmai ismeretek tanulmányterületből.

	tantárgyak	*óraszám*
1.	Belsőégésű motorok	120
2.	Járművek szerkezete	120
3.	Gépjármű villamos berendezések	30
4.	Rendszerben tartás	120
	Összesen:	390

A táblázatból is látható, hogy ez a négy tantárgy kevesebb óraszámmal rendelkezik a teljes képzési időn belül (13.5 %) a korábbi két másik képzéshez képest, de szem előtt kell tartani azt is, hogy jelen esetben nem mérnöki képzésről van szó. Az látható, hogy a Had- és biztonságtechnikai mérnöki alapképzési szakhoz képest kisebb ezeknek a tantárgyaknak az óraszáma, de azt nem lehet kijelenteni, hogy a meghatározott ismeretszintet ne lehetne teljesíteni ezáltal.

A végzett tisztek általános katonai és szakmai felkészültsége nem csökken, viszont vezetői és parancsnoki képességeik erősödnek, amennyiben a képzési és kimeneti követelmények valamint a tanterv követelményei maradéktalanul teljesülnek.

ÖSSZEFOGLALÁS

A gépészmérnöki szakon levő páncélos- és gépjármű-technikai szakirány és a had- és biztonságtechnikai mérnöki szakon levő páncélos- és gépjármű-technikai modul hasonlóságot mutat mind a meghatározott speciális követelmények területén, mind az ezeket lefedő tantárgyi struktúra területén. Ez természetes is, mert mindkét szak a műszaki tudományokon belül helyezkedett el, és a honvédség igénye is hasonló volt, legalábbis nem mutatott hatalmas eltérést.

A katonai logisztika alapszak, haditechnikai specializáció, páncélos- és gépjármű-technikai modul szintén nagy hasonlóságot mutat a fenti két modullal. A referenciának választott tantárgyak oktatásra kerülnek ugyan, de jól megfigyelhető az óramennyiség csökkenése. A jelenleg működő katonai logisztika szak esetében ez már csak a gépészmérnök szak óraszámainak 59%-a.

Összességében tehát kijelenthető, hogy az új szak esetében megmaradt a szakma, hiszen a differenciált szakmai törzsanyagban hasonló tantárgyak kerülnek oktatásra. A katonai logisztika szak alapításával némiképpen változtak és kiegészültek a képzési célok. Új képzési célként jelent meg a közszolgálati ismeretek oktatása, valamint erősödött a vezetői képességek kialakítását célzó tárgyak oktatása. Ezen célokat a szakmai tárgyak rovására lehetett csak teljesíteni, ami maga után vonta a szakmai tárgyak óraszámának csökkenését.

Felhasznált irodalom

[1] Dr. Pohl Árpád: A műveleti felkészítés rendszere a logisztikai tisztképzésben. Hadtudományi Szemle, 2015. VIII. évfolyam 1. szám. ISSN 2060-0437

[2] Magyarország alaptörvénye. Magyar Közlöny, 2011. évi 43. szám. http://www.kozlonyok.hu/nkonline/mkpdf/hiteles/mk11043.pdf (letöltés ideje: 2016. február 16.)

[3] Dr. Pohl Árpád: A műveleti felkészítés követelményeinek néhány aspektusa a logisztikai tisztképzésben. Hadtudományi Szemle, 2015. VIII. évfolyam 1. szám. ISSN 2060-0437

[4] Nyt.szám: 92/871/2077. A Bolyai János Katonai Műszaki Főiskola gépészmérnöki szak tanterve nappali tagozatos tisztképzés számára. Bolyai János Katonai Műszaki Főiskola, Budapest, 1997.

[5] Nyt.szám: 91/871/2077. Tantárgyi programok a gépészmérnöki szak páncélos-technikai szakirány, gépjármű-technikai szakirány, műszaki technikai szakirány részére. Bolyai János Katonai Műszaki Főiskola, Budapest, 1997.

[6] VÉG Róbert: Új oktatástechnikai eszközök alkalmazása a gépjármű-technikai képzésben. Bolyai Szemle különszám (HADITECHNIKA 2006 szimpózium). Budapest: ZMNE nyomda, 2006. ISSN: 1416-1443.

[7] Pohl Árpád: Az új rendszerű logisztikai tisztképzés – valóban „eltűnt a szakma”? Hadmérnök, 2015. X. évfolyam 1. szám. ISSN: 1788-1919.

[8] Had- és biztonságtechnikai mérnöki alapszak tanterve. 1. kötet. Az alapszakon közös követelmények, nappali tagozatú, ösztöndíjas és kettős jogállású, hallgatók részére. Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar, Budapest, 2005.

[9] Dr. Pohl Árpád: Az új tisztképzés – a logisztikus megoldás. Hadtudományi Szemle, 2014. VII. évfolyam 4. szám. ISSN 2060-0437

[10] Magyar Közlöny 2011. évi 33. szám, 2011. március 28.

[11] Katonai logisztika alapképzési szak tanterve. Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, Budapest, 2013.

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Haig Zsolt - Kóródil Gyula
haig.zsolt@uni-nke.hu - korodi.gyula@uni-nke.hu

A KATONAI MŰSZAKI DOKTORI KÉPZÉSBENREJLŐ POTENCIÁLIS TARTALÉKOK
I. RÉSZ
A Katonai Műszaki Doktori Iskola hallgatói körében végzett kérdőíves felmérés eredményei

Absztrakt

A Katonai Műszaki Doktori Iskola 2002 óta toboroz, képez és segít tudományos fokozatszerzéshez doktoranduszokat. A szerzőket az a kérdés foglalkoztatja, hogy lehetséges-e tanulságokat levonni a PhD hallgatók és munkáltatóik, továbbá az oktatók képzéssel kapcsolatos tapasztalataiból, elvárásaiból? Tudunk-e felszínre hozni olyan elvárásokat, igényeket melyek eleddig nem kerültek kellő módon megfogalmazásra? Mit lehetne tenni annak érdekében, hogy a PhD hallgatók hatékonyabban kihasználják a kutatóműhelyek szellemi kapacitását és a hosszú távú együttműködés lehetőségét? Fenti kérdések tisztázása érdekében kérdőívet szerkesztettünk és kértük a hallgatók és oktatók szíves közreműködését illetve építő interakcióját. Ehelyütt is köszönetet mondunk minden együttműködő Kollégának értékes kritikai észrevételeikért, illetve javaslataikban rejlő segítő-javító munkájukért.

The Doctoral School of Military Engineering have recruited, and trained PhD students and helped them to obtain doctoral degree since 2002. The authors' main question is, how can be drawn the lessons from the PhD students' and their employers', and educators' experiences as well as requirements of training? Can we bring to the surface any expectations, demands that have not been formulated so far? What can be done to ensure that the PhD students more efficiently take advantage of the intellectual capacity of the research centers and the possibility of a long-term cooperation? In order to clarify these problems we constructed questionnaire and we pleased the constructive interaction of the students and the teachers. Here we also thank all of the coworkers for their critical comments and their proposals to assist potential help in work.

Keywords: *PhD képzés, kérdőíves felmérés, tudományos kutatás ~ PhD training, survey, scientific research*

BEVEZETÉS

A doktoranduszképzés – szerény megítélésünk szerint – leginkább az aranymosásra emlékeztető munka: fáradtságos, izgalmas és gazdagító tevékenység. Megszámlálhatatlan jelentkező hozza briliáns gondolatait, invenciózus kutatási koncepcióját, amiből aztán a Doktori Iskola a legjobbakat kirostálja és aktívan közreműködik a PhD fokozat megszerzéséhez vezető folyamatban. Egyszerűsítve a kérdést: a témavezetők a tudományos munkában még relatíve járatlanabb doktoranduszaikat segítik kutatói tapasztalataikkal, meglévő tudományos műhelyük potenciáljával, honi- és nemzetközi kapcsolataikkal.

A szerzőkben itt támadt hiányérzet, nevezetesen a megszerzett tudományos fokozatok száma és a tudományos eredmények védelmi szektorban (vagy a versenyszférában) történő felhasználása között kitapintható az aránytalanság. Az alap- és alkalmazott kutatás, K+F, végül a piaci bevezetés kontinuumában tapasztalható némi törés. Nevezetesen a tudományos fokozat megszerzéséhez szükséges eredmények inkubációjára lenne szükség ahhoz, hogy a megszámlálhatatlan értékes „output" a tudomány Parnasszusáról leereszkedve alkalmassá és képessé váljon a technologizálásra és a piaci bevezetésre. Így elérhetjük, hogy az aranymosó a megtalált rögöt – a megfelelő „ékszerészi munka" után – hasznosítsa, mégpedig úgy, hogy minden résztvevő számára világossá váljon az általa hozzáadott érték és annak hozadéka.

Azt tapasztaljuk, hogy a KMDI-ben 2002 óta eltelt időszakban látott doktori cselekményeknek elenyésző hányada vált szabadalom- vagy pályázatképes termékké, és ezzel nem az egyes kutatók eredményeit kívánjuk leminősíteni. A dolgozat célkitűzése, hogy a teljes képzési rendszer összefüggéseinek vizsgálatával, a volt hallgatók kérdőíves felmérésére alapozva választ kapjunk arra, hogy a Doktori Iskola miként járulhat hozzá a mind több gyakorlatorientált és (megfelelő inkubációt követően) piacképes tudományos végtermék eléréséhez, hasznosítható eredményekkel megszolgálva a védelmi szektor, mint „befektető" invesztícióját. A tanulmány I. részében a KMDI volt hallgatóinak, a II. részben pedig az oktatóknak, témavezetőknek készített kérdőíves felmérés eredményeit tesszük közzé.

A KATONAI MŰSZAKI DOKTORI KÉPZÉS BEMUTATÁSA

A Katonai-műszaki Doktori Iskola 2002-ben kezdte meg a PhD képzést a Nemzeti Közszolgálati Egyetem (NKE) jogelőd intézményében a Zrínyi Miklós Nemzetvédelmi Egyetemen (ZMNE). Az iskola doktorandusz képzésben kitűzött főbb céljai között szerepel: a PhD hallgatók magas színvonalú oktatása, képzése; a védelmi szféra számára a fejlesztés iránymutatását adó oktató-kutató elit kinevelése, a tudományos műhelyépítés és a kiválóak sikeres menedzselése érdekében; nemzetközi összehasonlításban is mérhető kutatási eredmények produkálása mind az oktatók (témavezetők), mind a PhD hallgatók által. [1]

A KMDI-ben folyó katonai műszaki tudományi képzés és kutatás a műszaki tudományterülethez tartozó tudományágaknak a teljes védelmi szektorban történő alkalmazására fókuszál. Kutatói tevékenységét gyakran több tudományterület és tudományág határterületén műveli, azok interdiszciplináris kérdéseit feldolgozva, szinergiáit keresve. A kutatások olyan technikai eszközök, technológiák fejlesztésére irányulnak, amelyek alkalmazhatóak a védelmi szektorban, tehát a honvédségben, a rendészet, a katasztrófavédelem stb. terén. Az előbbiekből következik, hogy a katonai műszaki tudományok nagyon szoros kapcsolatban állnak a műszaki tudományok mindegyik tudományágával, a hadtudományhoz pedig a haditechnikai eszközök és eljárások alkalmazása terén kapcsolódik.

A Doktori Iskola kutatási területei közé tartozik a katonai műszaki infrastruktúra, a haditechnika és robotika, a védelmi elektronika, informatika és kommunikáció, a katonai környezetbiztonság, a katonai logisztika és védelemgazdaság, a biztonságtechnika és a és katasztrófavédelem. [2] Ezen kutatási területek a Hadtudományi és Honvédtiszt-képző kar akkreditált

MSc szakjaira épülnek, megvalósítva ezzel a BSc - MSc - PhD képzés teljes kontinuumát. Az iskola „credo”-jából idézett mondat jól érzékelteti, hogy a végzett hallgatóinkat igyekszünk mind versenyképesebb tudással felvértezni: *„A megszerzett (PhD) doktori fokozat (oklevél) birtokosa jó esélyekkel indulhat mind az állami, mind a versenyszférában a legkülönbözőbb szakterületeken magasabb vezetői, oktatói és kutatói munkakörökért folytatott versenyben.”* [1]

Az elmúlt években a KMDI arra törekedett, hogy tudományos műhelyként funkcionáljon az elitképzés és a kiválóak kinevelése céljából. Ennek érdekében az oktatást és a kutatást egymás koherenciájában szervezte és irányította. Meghatározta és megismertette a doktoranduszokkal a katonai műszaki tudományok területén a kutatók kutatás-etikai normáit. A védelmi szféra katonai műszaki tudományok kutatási területeihez kapcsolódó „civil”, azaz nem katonai szervezetei számára is utánpótlást biztosított. Növelte a képzésben résztvevők és az iskola oktatási és kutatási teljesítményét, és sikerrel szorgalmazta a saját új kutatási eredmények rendszeres közzétételét is. A Doktori Iskola e törekvéseit és eredményeit igazolja, hogy a Magyar Felsőoktatási Akkreditációs Bizottság (MAB) 2015 év végén a MAB 2015/9/IX/52/2/938. sz. határozata alapján a KMDI akkreditációját – a működési feltételek folyamatos biztosítása esetén – a 2019. december 31-ig megerősítette. [3]

A KMDI ezen eredményei mellett is azonban szükséges időről-időre megvizsgálni, hogy a képzés és kutatás feltételei milyen mértékben teljesülnek, és a hallgatók által elért eredményeknek milyen a hatásuk és a felhasználhatóságuk. A Doktori Iskola munkáját célzó felmérés elsősorban problémafeltáró önvizsgálat. Valamennyi kritikai észrevételnek a saját munkánk hatékonyságának és a hallgatókkal való segítő együttműködésnek a megmérettetésén kell alapulnia. A hiányosságok és a gyenge pontok aktív kutatásának és beazonosításának célja nem csak a bírálatok megfogalmazása, hanem a jövőbeli tudósképző munkánk javításában és annak hatékony kommunikációjában rejlő tartalékok kiaknázása.

A DOKTORANDUSZOK ÉSZREVÉTELEIT ÉS JAVASLATAIT FELMÉRŐ KÉRDŐÍV KIÉRTÉKELÉSE

A KMDI 2002-től 2015-ig terjedő képzési idejében végzett és felavatott doktor, továbbá a képzés befejezése után PhD fokozatot nem szerzett ex-hallgatója számára egységes kérdőívet szerkesztettünk. Az egyszerűbb, gyorsabb válaszadás és azok hatékonyabb kielemzése érdekében eldöntendő kérdéseket állítottunk össze, illetve lehetőséget adtunk a válaszadóknak, hogy a doktorandusz, annak munkahelye és a doktori iskola közötti háromoldalú együttműködés hatékonyságát javító észrevételeiket, javaslataikat lényegre törően kifejthessék. A kérdőíveket a Google Drive kérdőívszerkesztőjével készítettük el, az erre mutató linket megküldtük minden volt doktoranduszunk. A felmérésben részt venni kívánók online felületen tudták kitölteni az űrlapokat, amelyre több mint egy hónapos időablakot hagytunk. Egyes kérdéseknél több választ is megjelölhettek a megkérdezettek. Az így kapott információkból nyert adatbázist szintén a Google Drive kérdőívszerkesztő segítségével dolgoztuk fel. A kérdőívet 26 fő,[1] többségében fokozatot is szerzett volt hallgató töltötte ki, ami a végzettek számához viszonyítva bár nem nagy szám, azonban úgy véljük, hogy véleményük mindenképpen figyelemre méltó és segíthetik a doktori képzés fejlesztését.

A hallgatók részére összeállított kérdőívekkel az alábbi főbb kérdésekre kerestük a választ:

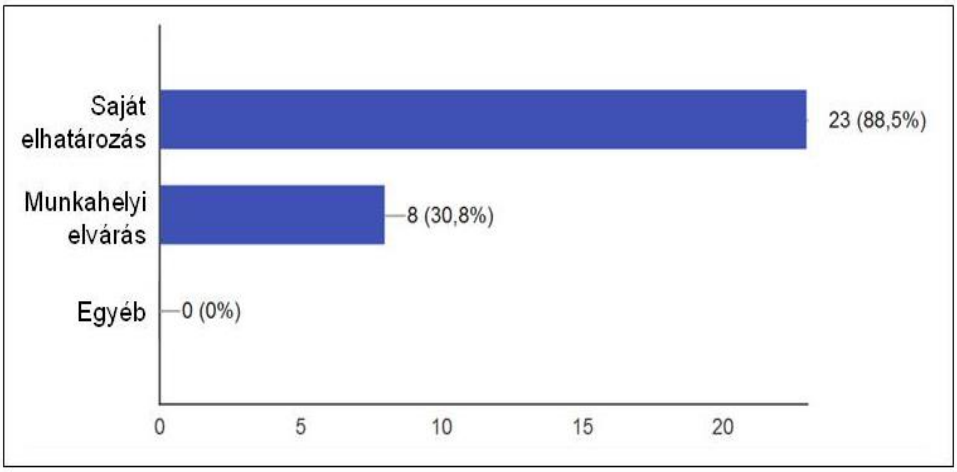
- a jelöltek témaválasztása mennyiben egyéni döntésképpen született, vagy milyen fokban a védelmi szektor (vagy a versenyszféra) által orientált, tematizált;

[1] A grafikonokon a válaszadók számösszege nem minden esetben 26 fő. Az eltérést az okozza, hogy egyes kérdésekre több válasz is adható volt, ill. bizonyos kérdésekre nem mindenki válaszolt (pl. mert nem szerzett fokozatot).

- a doktori disszertációk tudományos eredményei milyen arányban jutottak el (írásban vagy a védés prezentációjaképpen) a védelmi szektor döntéshozóihoz, és hogy ez az arány miképpen javítható;
- a doktori iskolában született tudományos eredmények és az azokból fakadó ajánlások milyen arányban kerültek gyakorlati alkalmazásra. Itt nem szükséges különösen ellenpontozni, hogy mi a különbség a tudományos eredményeknek is csak jóindulattal elfogadott „asztalfiók-produktumok" és az újabb kutatásokat inspiráló, pályázatokat elnyerő, bevezetett és rendszerbe állított tudományos innovációk között;
- a végzett PhD-hallgatók megmaradtak-e tudományos kutatóműhelyük vérkeringésében, folytatnak-e posztdoktori tudományos kutató tevékenységet;
- melyek lehetnek a lemorzsolódás okai?

Beiskolázás a PhD képzésre

Az 1. ábrán látható grafikon szerint a megkérdezettek esetében a beiskolázást döntően egyéni ambíció és elhatározás motiválta, és kisebb részben a munkahely elvárása volt a doktori képzés megkezdése. 5 esetben viszont az egyéni kezdeményezés és a munkahelyi elvárás szerencsésen találkozott. Ahogy az egyén életében jelentős döntés a PhD fokozatszerzés, úgy ez a kérdés a munkáltató szempontjából is komoly kihatásokkal bír. A pályakezdő kolléga nélkülözése és helyettesítése ugyanúgy megoldandó feladat, mint a munkavállaló hiányából fakadó problémák megoldása. Ha az életpálya modell tervezése során a beiskolázó előre kalkulálja a potenciális doktoranduszok PhD képzését, ezzel aktív és segítő szereplővé léphet elő. Így elérhető, hogy a doktori iskolába nem kénytelen-kelletlen „elengedik" a kollégát, hanem az adott tudományos projekt részeként, ütemezetten és kieső munkáját tervezetten pótolva válik partnerré a munkahely.

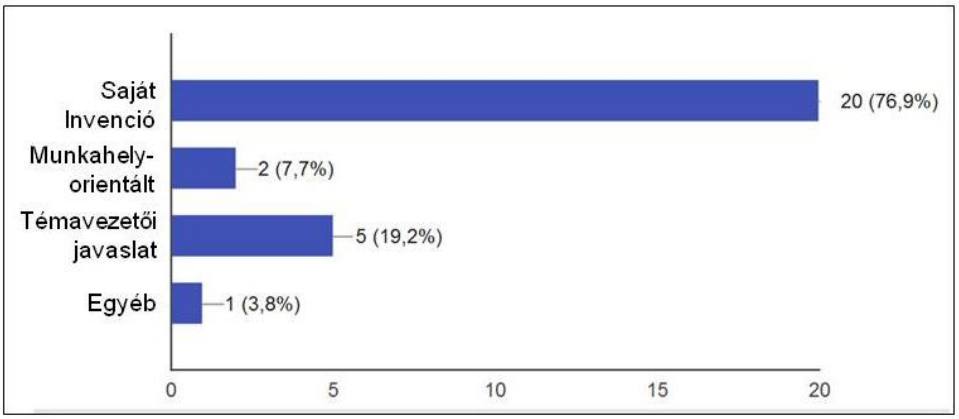


1. ábra: A PhD beiskolázás indoka

Témaválasztás

Az előző kérdés szerves folyományának tűnik, hogy a doktoranduszok többsége önnön intenciók mentén kezdik meg tudományos munkájukat, kisebb hányaduk támaszkodik a témavezető javaslatára. A 2. ábra szerint a válaszadók témaválasztását néhány kivételtől eltekintve saját invenció határozta meg, a „megrendelő" és beiskolázó munkahely szerepe e tekintetben marginálisnak tekinthető. Összevetve ezt az előző kérdéssel szembetűnhet, hogy bár a munkahely több esetben is preferálja a PhD képzést, azonban a témaválasztást a hallgatóra bízza. Ezzel

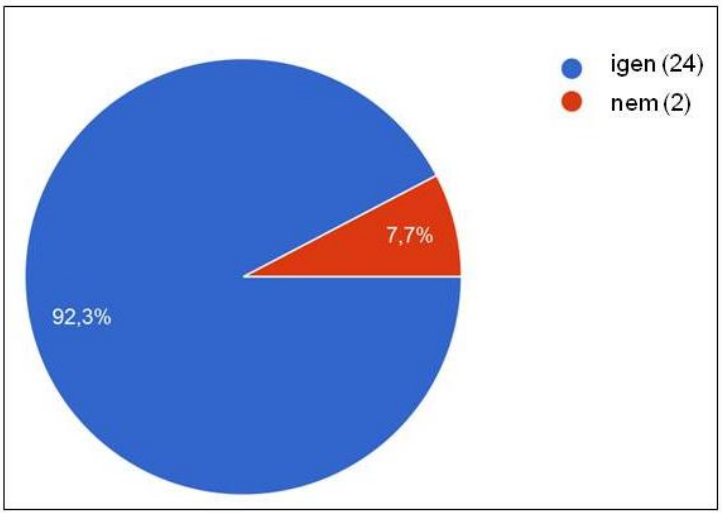
diszharmonikussá válhat az a kontinuum, ami megítélésünk szerint úgy volna optimális, hogy a munkavállaló és munkáltató konszenzus alapján időzíti és tematizálja a PhD képzést. Így a doktorandusz képzésének befejeztével, a PhD fokozat megszerzésével egy magasan kvalifikált munkaerővel gazdagszik a beiskolázó, nem is beszélve a gyakorlatba ültethető tudományos eredmények iniciálta további K+F lehetőségekről.



2. ábra: A témaválasztás

Lemorzsolódás

A 3-4 ábra alapján látható, hogy a lemorzsolódás aránya kicsi. Ez fakadhat az ambiciózus doktoranduszokból és/vagy a munkáltató és a KMDI hatékonyan segítő munkájából. Mindenképpen pozitívumként értékelendő a megkezdett, de be nem fejezett PhD képzések alacsony aránya. A doktoranduszok átgondolt, felelős döntése ugyanúgy kitapintható az adatok mögött, mint a hallgatók és a doktori iskola között megkötttetett szerződés komolysága.

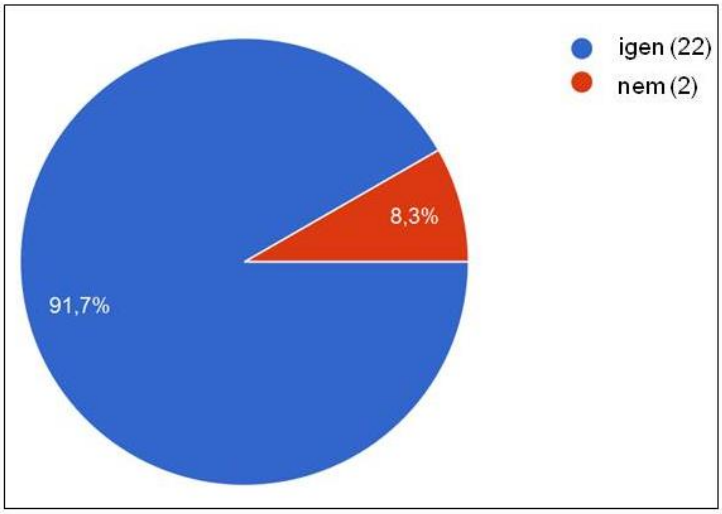


3. ábra: Abszolutóriumot szerzők aránya a válaszadók körében

Ehelyütt meg kell azonban jegyezni, hogy ennyire nem pozitív az összkép, mivel a válaszolók között többségben voltak a fokozatot szerzettek. A felmérésben résztvevők közül csak két fő volt, aki nem szerezte meg az abszolutóriumot és így nem is szerzett fokozatot. Az Országos Doktori Tanács honlapján található adatok alapján azonban láthatjuk, hogy 2015-ig 401 fő lett felvéve a KMDI-be, közülük 259-en kapták meg az abszolutóriumot és 172 fő szerezte meg a PhD fokozatot. [4] Itt is meg kell azonban jegyezni, hogy a felvett 401 fő közül

jelenleg képzésben van 68 fő, ill. további 65 főnek még nem járt le az abszolutóriuma, tehát még fokozatot szerezhetnek. Ezen adatok alapján megállapíthatjuk, hogy a vizsgált időtartam alatt 268 főnek kellett volna eredményesen, tehát fokozatszerzéssel befejezni doktori tanulmányait. Ennek fényében a fokozatszerzési arány 66%-os, ami országos szinten igen jónak mondható.[2]

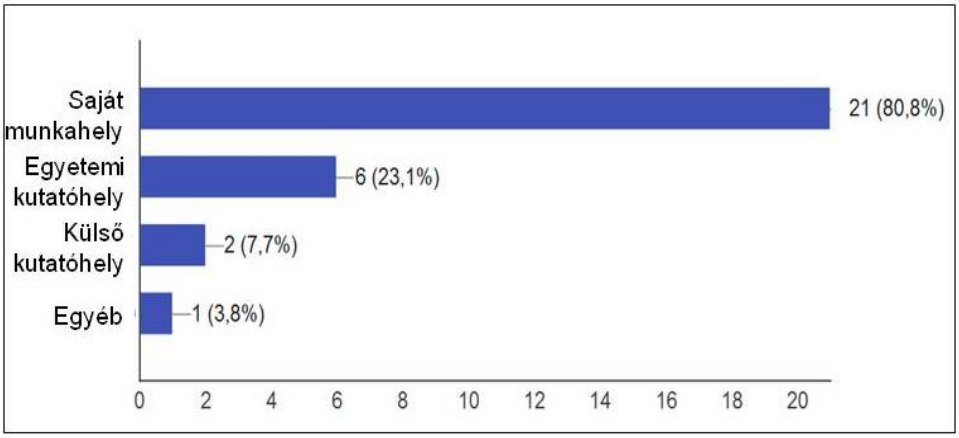
Az abszolutórium, ill. a fokozat megszerzésének hiányát a válaszolók részben anyagi, financiális okokra, a 2. nyelvvizsga hiányára, illetve a belső indíttatás megszűnésére vezették vissza.



4. ábra: Abszolutórium- és fokozatszerzési arányok a válaszadók körében

Kutatóhely

Az 5. ábrából egyértelműen kitűnik, hogy a doktoranduszok kutatóhelye a PhD képzés alatt jellemzően a munkahelyük maradt és kisebb hányadban jelölték meg az egyetemet kutatóhelynek. Két fő más külső kutatóhelyet vett igénybe, illetve többen több lehetőséget is kihasználtak kutatómunkájukhoz. Az egyetemi kutatóhelyként való igénybevétele betudható annak, hogy a KMDI nem rendelkezik saját kutatási infrastruktúrával, az egyetemen az intézetek és tanszékek infrastruktúrája adja a doktori képzés kutatói eszközparkját.



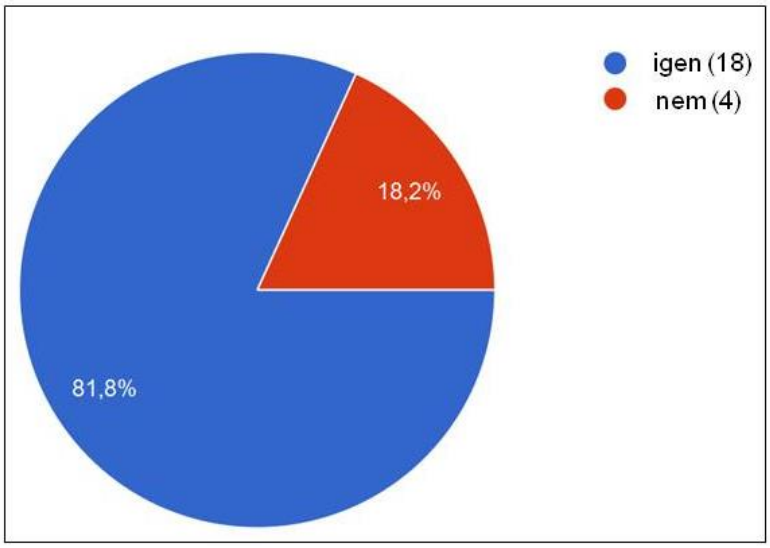
[2] Egy 2009-ben készült tanulmány szerint hazánkban a végzettek száma (adott évben) az új belépők (felvettek) százalékában 37%-os, az OECD országokban pedig 67%. [5]

5. ábra: A doktorandusz kutatóhelye a képzés alatt

Az NKE e tekintetben sajátos helyzetben van, mivel az egyetem elsősorban a társadalomtudományok területen folytat képzést, a műszaki területi képzés az utóbbi években háttérbe szorult. Ez pedig rányomja a bélyegét a műszaki kutatási infrastruktúra fejlesztésére is. Ezért a doktoranduszok inkább választják a saját munkahelyi erőforrásaikat kutatási eredményeik alátámasztására. Megítélésünk szerint a KMDI ez irányú szerepének növelésében még lehetnek tartalékok, ha nem is kimondottan doktori iskolai kutató laboratóriumok kialakításában, inkább a tanszékek felé megfogalmazott igények formájában.

Témavezetőn kívüli más segítség igénybevétele

Az előző kérdéssel szervesen összefügg, és mint a 6. ábrából kitűnik, a külső (esetleg munkahelyi) konzulens szerepe jelentős. A válaszadók több mint 80%-a igénybe vette/elfogadta a témavezetőn kívüli külső segítséget. A válaszadók közül sokan szakmai és kutatásmódszertani segítséget kaptak kollégáiktól, a doktori iskola oktatóitól. Tudományos rendezvényeken és konzultáció keretében hazai és nemzetközi szakértők tapasztalataira is többen támaszkodtak. Ezen a ponton is érdemes számba venni, hogy a KMDI ad-e elegendő intézményes muníciót (labor, kísérletes háttér, statisztikus, módszertani szakember, egyéb szakértő) a doktoranduszoknak? A szerzők tisztában vannak a kutató laborok, kísérletes műhelyek anyag- és eszköz igényeivel illetve ezek költségvonzataival. A finanszírozhatatlan elképzelések csak a fikció kategóriát gazdagítják, ezért itt a KMDI oktatóinak „teljes kutató-műhely tőkéjére" utalunk. Tudományos előéletünkből fakadóan valamennyien rendelkezünk olyan kapcsolatrendszerrel, amit hallgatóink rendelkezésére bocsáthatunk. Az egyes oktatók ilyen háttere közkinccsé is válhatna azzal, hogy beadjuk a KMDI „trezorjába" a témavezetői kutatói infrastruktúrát. Ezzel több milliós igények irracionális megfogalmazása helyett létrehozhatunk egy olyan közös adatbázist, ahol minden doktorandusz megtalálhatja az adott probléma szakszerű vizsgálatához szükséges kutatóhelyet.

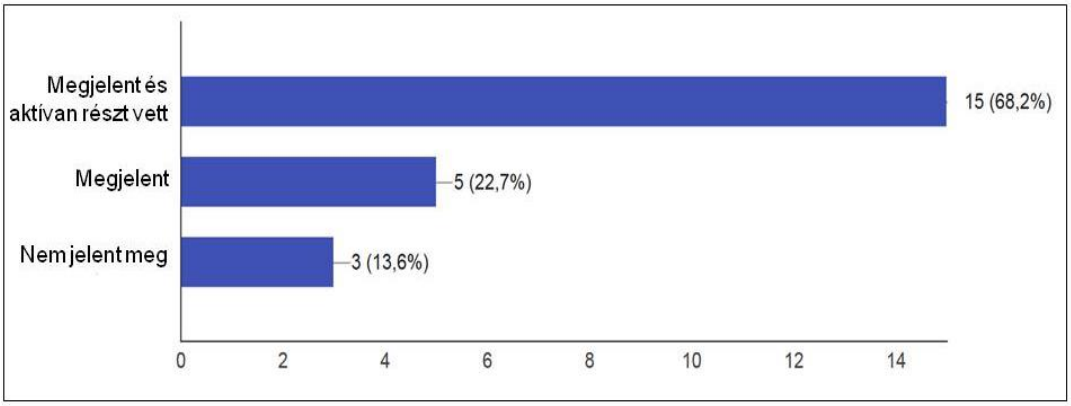


6. ábra: Témavezetőn kívüli segítség igénybevétele

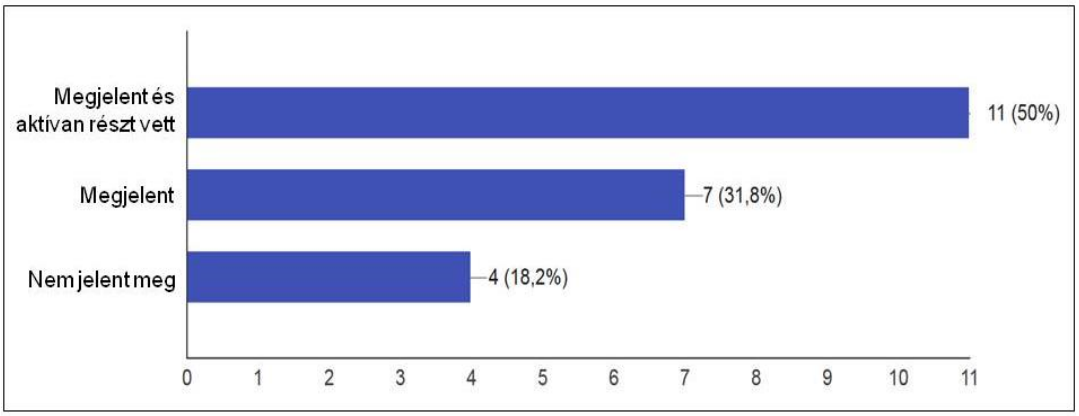
Munkahelyi vezető részvétele a fokozatszerzési folyamatban

A tapasztalat azt mutatja, hogy a képzés és a fokozatszerzés során a munkahelyi vezetők figyelemmel kísérik beosztottaik tudományos tevékenységét. Ezt támasztja alá a 7. és 8. ábra is, miszerint mind a munkahelyi vitán, mind pedig a nyilvános védésen a vezetők megjelennek és

ott aktívan részt vesznek. A szerzők az elmúlt években számtalan munkahelyi vitán és védésen vettek részt, és általános tapasztalat, hogy a vezetők hozzászólásukkal elsősorban az adott szakterület szakmai-tudományos igényeit fogalmazzák meg, a megoldandó problémákat hozzák felszínre. Ez rendkívül előremutató, hisz felelős vezetőként Ők látják át az adott terület feladatit. Ugyanakkor ez az érdeklődés az eredmények további felhasználásakor már nem érződik ennyire, mint azt a későbbiekben látni fogjuk.



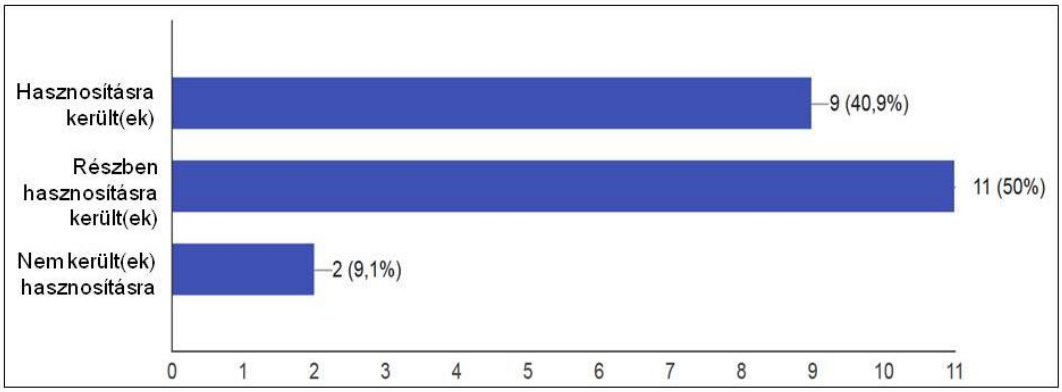
7. ábra: Munkahelyi vezető részvétele a műhelyvitán



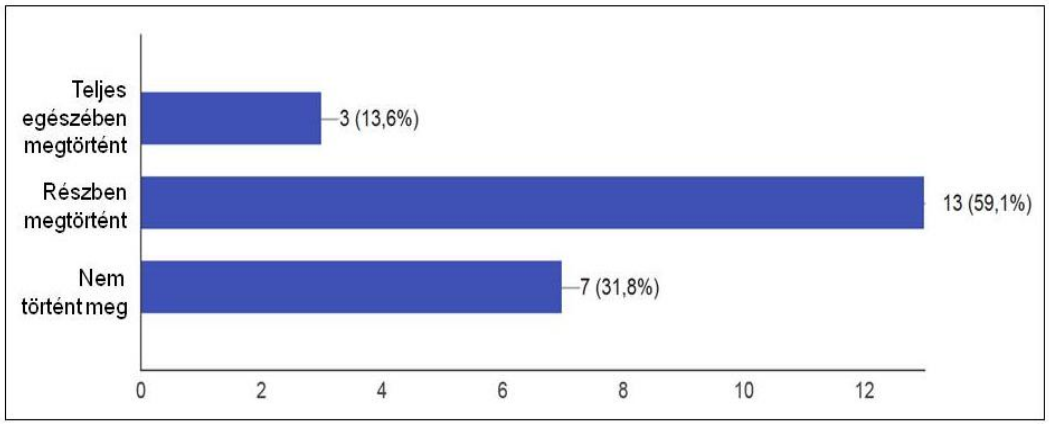
8. ábra: Munkahelyi vezető részvétele a nyilvános védésen

Tudományos eredmények hasznosulása

A 9. grafikon alapján szembetűnő, hogy az elért tudományos eredmények nagy része nem került hasznosításra. Mindösszesen a válaszolók közül 2 fő jelentette ki, hogy az elért eredményeket teljes mértékben felhasználták, 9 fő pedig úgy nyilatkozott, hogy tudományos eredményei csak részben hasznosultak. Az ajánlások gyakorlatba való átültetésénél még szembetűnőbb ez az arány (lásd 10. ábra). A felmérés alapján kimutatható tehát, hogy a tudományos eredményeknek leginkább a doktorandusznál van utóélete. Ez némileg ellentmond az előző pontban leírtakkal, miszerint a munkahelyi vitán és a védésen való részvétel elvileg az eredmények iránti érdeklődést mutatják, ennek ellenére ez a hasznosulásban nem érhető egyértelműen tetten.

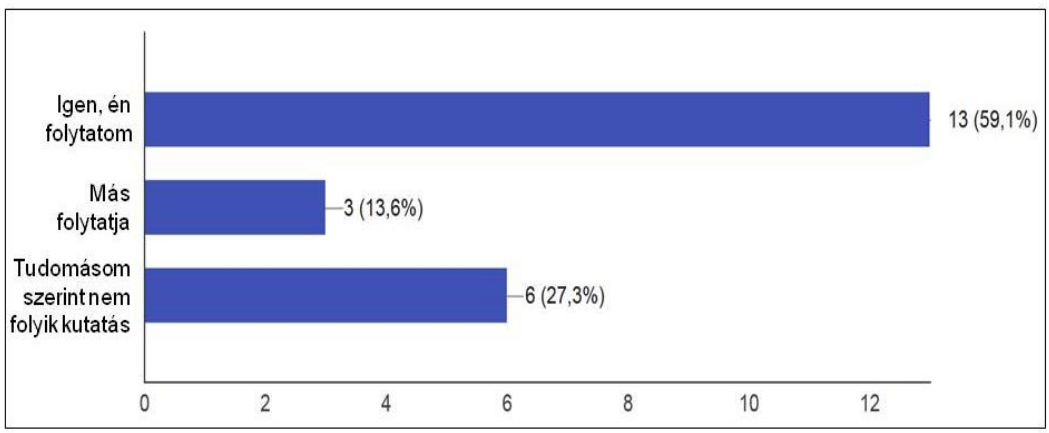


9. ábra: Tudományos eredmények felhasználása



10. ábra: Ajánlások gyakorlatba ültetése

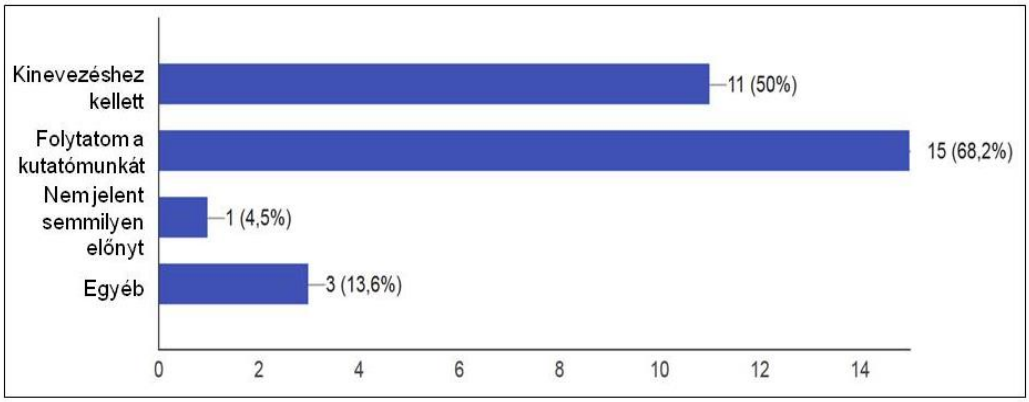
A kedvezőtlen adatok elemzése több okra is rávilágít. Egyrészt valószínű, hogy olyan kutatások is folynak/folytak a Doktori Iskolában, amelyek eredményei nem feltétlenül realizálhatók, akár a pénzügyi források szűkössége, vagy esetleg a szándék hiánya miatt. Másrészt vélhetően több olyan eredmény is „születik” aminek megvalósulása nem jelent számottevő pozitív változást, nem mutat jelentősebb technikai-technológiai fejlődést. Harmadrészt felmerül a kérdés, hogy a fokozatot szerzettek milyen mértékben követik nyomon eredményeik hasznosulását. Vélhetően nem fordítanak nagy energiát arra, hogy eredményeiket kellő mértékben „propagálják”. Erre mutat rá a 11. ábra is, miszerint az adott témakörben további kutatómunka végzése elsősorban a tudományos eredményt elérő érdeke, és csak kis mértékben látszik, hogy ezen eredmények alapján mások is folytatják a megkezdett kutatást.



11. ábra: A kutatás további folytatása

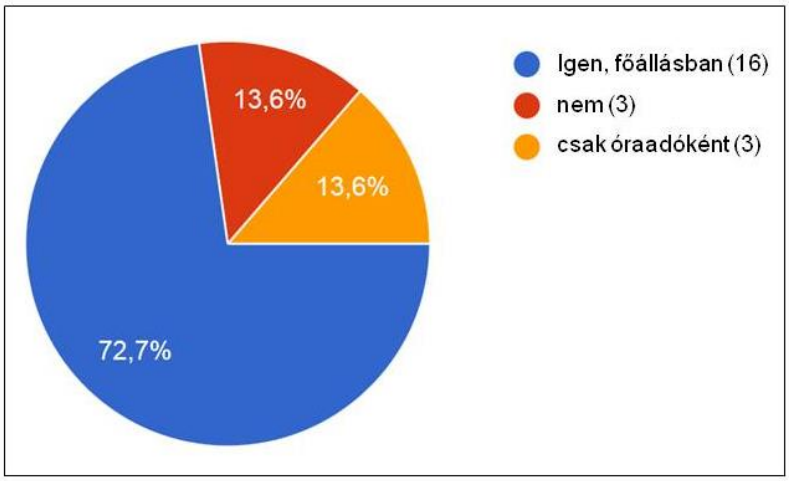
A fokozatszerzés utáni oktató-kutató tevékenység

A 12. grafikon alapján látható, hogy a PhD fokozat leginkább a doktorandusz munkahelyi előmeneteléhez, kinevezéshez volt szükséges, és e válaszolók többsége folytatja is a kutatómunkát. Figyelemre méltó az is, hogy egy kivétellel mindenki úgy nyilatkozott, hogy a doktori fokozat mindenképpen előnyt jelent a további szakmai előmenetelben. Összevetve ezt a 13. ábrán lévő adatokkal az is látható, hogy e kinevezések a felsőoktatásban már korábban is oktatóként dolgozókra vonatkoznak. A válaszokból az is látszik, hogy a PhD fokozat birtokosainak többsége folytatja kutatómunkáját részben abban a témakörben, amiben új tudományos eredményeket ért el (lásd 11. ábra), részben pedig szakterületéhez kapcsolódó mát területeken.

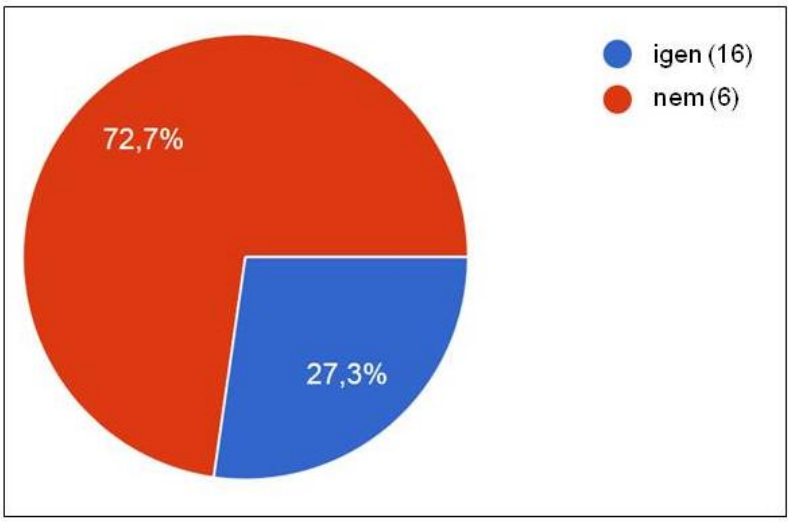


12. ábra: A PhD fokozat hozadéka

A 13. ábrán található adatokból látható, hogy a PhD fokozat jellemzően nem főállásban tudományos tevékenységgel foglalkozó, K+F projektekben részt vevő „valódi kutatót" takar, hanem a felsőoktatási ranglétrán menetelni kívánó oktató produktuma. Ez többnyire érthető is, hiszen a felsőoktatási törvény az egyetemi oktatókkal szemben kritériumként írja elő a tudományos fokozatot, ill. a doktori képzés megkezdését, doktorjelölti státusz meglétét.



13. ábra: Oktatás felsőoktatásban



14. ábra: Doktori iskolában tagság

Mindenképpen figyelemre méltó, hogy az esetek nagyobb hányadában megszakad a kapcsolat a doktori iskolával és máshol sem folytatódik érdemben, vagyis a fokozatot szerző nem vesz részt doktori képzésben. A 14. ábra szerint mindössze 6 fő válaszolt úgy, hogy az egyetemi képzés legfelső szintjén is aktív tevékenységet folytat, közülük a többség témavezetőként is működik, egy főnek pedig már van végzett doktorandusza is. Közülük a nagy többség a KMDI-ben fejti ki e tevékenységét, de vannak akik több doktori iskolának is tagjai. Ez a viszonylag alacsony szám annak fényében, hogy a többség az akadémiai szférában dolgozik mindenképpen említésre méltó, hisz az egyetemek általában elvárják a tudományos fokozattal rendelkezőktől e tevékenységet. A fokozatszerzés utáni oktató-kutató tevékenységre, és különösen a doktori képzésben való részvételre vonatkozó válaszok arra is rámutatnak, hogy voltak akik a PhD fokozat megszerzésével lezártnak tekintik a tudományos munkát, avagy egyesek megértették a további közös munka lehetőségeit, perspektíváit.

KÖVETKEZTETÉSEK, JAVASLATOK

A kutatási téma meghatározása vonatkozásában a munkáltató – doktorandusz – KMDI háromszögben a képzést igen sok esetben finanszírozó munkáltató és a képzést végző Doktori Iskola relatíve háttérbe húzódnak. A jelölt többnyire hozza a kutatási témáját – ami illeszkedik a Doktori Iskola meghirdetett témáihoz – és ennek a védelmi szektor számára profitábilis hozadéka nem minden esetben realizálódik kellő súllyal.

A védelmi szektor döntéshozói nagyobb hangsúllyal, orientált tudományos érdeklődéssel, érdemben priorizált témákkal, kvázi „megrendelt” kutatásokkal jobban segíthetnék a témaválasztást és predesztinálhatnák a hasznosítható eredményeket. E tekintetben vannak előrelépések, miszerint a Honvédelmi Minisztérium évente megküldi azokat a témákat, amelyek kutatását preferálja, és a képzési költségek átvállalásával is támogatja. Ez egy jó kezdeményezés, azonban el kellene érni, hogy e témák időben jussanak el a Doktori Iskolához. Legtöbb esetben az Egyetemi Doktori Tanács (EDT) már elfogadta a következő tanévi témahirdetéseket, amikor a megrendelői igény megérkezett. A védelmi szektor többi szereplője azonban ilyen témaigényekkel eddig nem jelentkezett.

Véleményünk szerint a megoldás tehát abban rejlik ha védelmi szektor teljes spektrumában közreműködők világosan orientált műszaki tárgyú kutatási témákat határoznak meg, és azt időben eljuttatják a képző intézményhez. A képzés során a „megrendelő” folyamatosan, de legalább évente ellenőrzi, hogy mit finanszíroz, akár a publikációs tevékenység felügyeleté-

vel, akár rövid kutatási jelentés formájában. A fokozatszerzési folyamat végfázisában pedig aktív szereplőként vesz részt – mint ahogy ezt egyébként a felmérések is alátámasztják –, a munkahelyi vezető megjelenik, és véleményt formál a műhelyvitán majd a védésen, végül pedig személyes reputációját és kapcsolati tőkéjét is latba veti a téma kibontakoztatása érdekében.

A PhD fokozat megszerzése ugyan a KMDI stúdium befejezését jelenti, mégis el kell érnünk, hogy a doktorandusz sokkal inkább kezdő-, mintsem végpontnak tekinthesse azt a saját- és a Doktori Iskola közötti tudományos interakció vonatkozásában. Véleményünk szerint világos elvek mentén szervezett és a jelölt, a KMDI illetve a doktoranduszt beiskolázó majd visszafoglalkoztató munkáltató közötti folyamatos trialógussal elérhető, hogy a tudományos eredmények, mint originális szellemi termékek ne „az asztalfióknak készült" teóriák, hanem a praktikum számára szóló és megvalósítást nyert invenciók legyenek.

A kutatási téma sok esetben alig leplezhető módon „csak" a PhD fokozat megszerzéséhez szükséges, a doktorandusz egyéni fokozatszerzése az alap-motiváció, a képzést sok esetben finanszírozó védelmi szektor semmit sem (vagy aránytalanul keveset) tud profitálni a befektetéséből. Meggyőződésünk, hogy védelmi szektor illetve az állami- vagy versenyszféra munkáltató szervének, mint a tudományos kutatást kezdeményező, témája kialakításában résztvevő „megrendelőnek" folyamatosan artikulálni kell elvárásait.

A kutatómunka egészének interakciójában részt vevő munkáltatónak ki kell lépnie a „csak" finanszírozó szerepkörből és az elért eredmények aktív „végfelhasználójává" is kell válnia. Így kamatoztatni képes a tudományos munka hozadékát és a végzett doktor továbbfoglalkoztatásával magasabban kvalifikált munkavállalóra tehet szert. Ezen siker non plus ultra hozadéka lehet, ha egy (vagy több) tudományos eredmény felhasználható a honvédség, rendőrség, katasztrófavédelem, nemzetbiztonsági szolgálatok tevékenységében, ill. mint pályázat-képes innováció, a kutatási források kiaknázásával piacra vihető K+F outputjává válik. Ezáltal a kutató, a Doktori Iskola és a munkáltató számára egyaránt világosan értelmezhető az együttműködés tudományos és innovatív hozadéka.

A fentiek alapján megfontolandó tehát a legkiválóbb tudományos eredmények megméretetése akár a szabadalom-képesség szempontjából, ill. azok – szükség szerinti megfelelő inkubációját követően – tudományos pályázati koncepciók magvaként történő hasznosítása. Így elérhetővé válhat elsősorban a védelmi szektor, de akár a hazai- és az EU-s piac számára is piacképes output, vagyis a tudományos eredményből termék vagy szolgáltatás létrehozása. Ez megteremtheti a bekerülés lehetőségét a nemzetközi tudományos élet vérkeringésébe is, akár kutatói csereprogram, konferencia részvétel, fajsúlyos publikációk vagy workshop formájában.

A lemorzsolódás – amely bár kedvezőbb arányt mutat a hazai doktori iskolákhoz viszonyítva – csökkentése érdekében a megkezdett képzés a doktorandusz oldaláról minden esetben legyen komoly elhatározás és átgondolt kutatói koncepció folyománya és ne bármikor visszavonható „ötlet-betörésből" származó tévút, vagy múló szeszély. A KMDI felvételi eljárása pedig legyen mind tökéletesebb szelekciós szűrőállomás, amit a talentummal és ambícióval felvértezett, kitartó tudományos habitussal rendelkező kutatók képesek abszolválni.

Meglátásunk szerint a tudományos alkotó folyamatot kollektív „befektetésként" célszerű értelmezni. Az EDT a PhD fokozatot ugyan egyetlen – a disszertáció tudományos eredményeit több éves kutató-rendszerező munkával elérő – jelöltnek ítéli oda, azonban célszerű elérni olyan kölcsönös előnyökön alapuló konszenzust, melynek szintjén a tudományos eredmények felhasználhatóságából illetve a további kutatást igénylő kérdésekből a doktori fokozatot megszerző és képzőhelye egyaránt profitálni tud.

Meg kell találnunk a közösen értelmezhető inspirációt, annak érdekében, hogy a PhD fokozat megszerzése után a PhD doktor – a jelenleginél nagyobb arányban – a KMDI oktatója, témavezetője legyen, törzstaggá váljon, témát hirdessen. A Doktori Iskola számára akkor

„hullott termőtalajra” a tudományos befektetés magja, amennyiben a PhD fokozat birtokosa nem veszíti el kapcsolatát tudományos műhelyével, hanem oktatóvá, témavezetővé lép elő, kutatómunkájának alkalmazási lehetőségeit kibontakoztatja, doktoranduszokat nevel, és témavezetővé, majd törzstaggá válik (abszolút optimális esetben iskolateremtő tudományos potenciálra tesz szert). Ebben a folyamatban az iskola nem lehet csupán passzív résztvevő, kutatóműhely-hálózatának folyamatos bővítésével, működő rendszerbe szervezésével kell inspirálnia végzett és doktorrá avanzsált hallgatóját a további tudományos kooperációra.

Felhasznált irodalom

[1] Katonai Műszaki Doktori Iskola bemutatkozása http://hhk.uni-nke.hu/kutatas-es-tudomanyos-elet/doktori-iskolak/katonai-muszaki-doktori-iskola/bemutatkozas (letöltve: 2016. 04. 18.)

[2] Katonai Műszaki Doktori Iskola Képzési Terve 2016 http://hhk.uni-nke.hu/uploads/media_items/kmdi-kepzesi-terv-2016.original.pdf (letöltve: 2016. 04. 18.)

[3] A MAB 2015/9/IX/52/2/938. sz. határozata a Nemzeti Közszolgálati Egyetem 153 azonosítószámú katonai műszaki tudományok besorolású doktori iskolájáról. http://www.doktori.hu/index.php?menuid=538&id=165 (letöltve: 2016. 04. 18.)

[4] Katonai Műszaki Doktori Iskola adatlapja. http://www.doktori.hu/index.php?menuid=191&di_ID=165 (letöltve: 2016. 04. 18.)

[5] Mészáros S.; Szabó G.: A doktorképzés (PhD) elvei és gyakorlata hazánkban és az OECD-országokban. Magyar Tudomány, 2009. január, Magyar Tudományos Akadémia folyóirata, pp. 86-94

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Kóródi Gyula
korodi.gyula@uni-nke.hu

A VÉDELMI SZEKTORBAN SZOLGÁLÓK EXTRÉM FIZIKAI TERHELÉS UTÁNI REGENERÁCIÓJÁNAK JAVÍTÁSA MÁGNESTERÁPIÁVAL

Absztrakt

Minden módszer, ami műveleti vagy harcászati területen egyszerűen alkalmazható és képes lerövidíteni a regenerációhoz szükséges pihenési időt, nagyban hozzájárulhat a hivatásos élő erő hadrafoghatóságának javításához. Az extrém izommunka kapcsán emelkedett tejsav-szint a sportolók esetében enyhe intenzitású, aerob jellegű fizikai aktivitással korrigálható, a védelmi szektorban azonban igen korlátozottan biztosítható erre irányuló extra elfoglaltság. A laktát szint várhatóan szignifikánsabban gyorsabb ütemben történő csökkenése az elméleti igazolását adja a feltételezett gyorsabb regenerációnak. A laktát szint szignifikánsan gyorsabban csökken az első órában, a mágnesterápiával történő regeneráció esetén is. A terápia gyakorlati felhasználhatóságát igazolandó fegyverösszeszerelés teszt eredményi igazolták várakozásainkat. A mágnesterápiával történő regeneráció hatására mindhárom csoport eredményeihez képest szignifikánsan jobb eredmények születtek.

Each method which is simple to apply and is able to shorten the time needed to rest for regeneration, operational or tactical areas can greatly contribute to improving the living forces combat readiness. In connection with the extreme muscle work raised lactic acid levels in the case of athletes with mild-intensity physical activity, aerobic in nature it can be corrected, but the defense sector in a limited way to ensure extra to do so activity, much preferable opportunity forced regeneration during a favor and not recoverable rest / sleep. is expected to significantly faster reduction in the lactate level of the theoretical proof gives the assumed faster regeneration. Lactate level decreases significantly faster during the first hour, as is the case of the regeneration magnetic therapy as well. The practical use of therapy to justify weapons assembly test results confirmed our expectations. The effect of magnetic therapy on regeneration compared to the results of all three groups significantly better results.

Kulcsszavak: *regeneráció, laktát szint helyreállítás, mágnes terápia ~ regeneration, lactate recovery, magneto therapy*

BEVEZETÉS

A védelmi szektor személyi állományát érő extrém környezeti hatások és ártalmak, a misszióban szolgálók egzotikus betegségei, a potenciális robbanószer okozta vagy ABV-sérülés veszélye, a speciális körülmények között történő mentés, a védőfelszerelések alkalmazásából fakadó megterhelés, a védőoltások rendszere és gyógyszeres betegség-megelőzés, a poszttraumás stressz leküzdése csak néhány példa a honvéd- katasztrófaorvostan különleges elméleti felkészültséget és gyakorlati tapasztalatot igénylő kihívásai közül. A speciális feladatokat végrehajtó és sokszor extrém balesetveszélynek és/vagy egészségkárosító hatásoknak kitett hivatásos állomány egészségének megőrzésének/helyreállításának leghatékonyabb módja a folyamatos kockázat-elemzésen alapuló proaktív megelőzés. A megterhelések és a regenerációhoz szükséges idő és módszerek személyre szabott tervezése és kivitelezése biztosítja katonák, tűzoltók, terror-elhárítók, rendőrök esetében is, hogy a következő feladatot a felkészültségükhöz képest legmagasabb színvonalon /és magasabb biztonsági dimenzióban/ legyenek képes végrehajtani. A harcászati tevékenység vagy műveleti területen történő bevetések során azonban nem mindig biztosítható a megfelelő pihenési időtartam betartása, ami jelentős kockázatot jelent mind a parancs-teljesítés szempontjából mind a katona egészségvédelme tekintetében. Minden módszer, ami műveleti vagy harcászati területen egyszerűen alkalmazható és képes lerövidíteni a regenerációhoz szükséges pihenési időt, nagyban hozzájárulhat a hivatásos élő erő javításához személyes biztonságuk javítása mellett.

Az elektromágneses tér a katonai-műszaki tudományok egyik legfontosabb területének tekinthető, ugyanakkor annak biológiai hatásaiban rejlő lehetőségek kiaknázása még távolról sem tekinthető teljesnek. A védelmi szektor hivatásos állományának szervezetét érő megterhelések folyamatosan változó kumulatív hatása, annak belső környezeti állandóságát billenti ki az optimum zónából és indít el folyamatosan kompenzációs mechanizmusokat. A környezetből fakadó speciális megterhelések és azok belső környezetre (gázcsere, só-víz háztartás egyensúlya, táplálékfelvétel, izommunka, hőszabályozás, cirkadián ritmus, pszichés- és kognitív balansz) kifejtett hatásai örökös hajtóerőt jelentenek a mind stabilabb homeosztázisért tenni képes úttörő megoldások kutatása terén. Az új katonai műszaki technológiák biológiai felhasználása lehetőséget nyit a klinikai alkalmazásokra a szuperszelektált, egészséges, sőt extrém terhelés-élettani paraméterekkel rendelkező hivatásos populáció vizsgálatára. Az elektromágneses mezővel (EMF-vel) kapcsolatban a tudományos világ pozitív hatásokról számol be, nem említ esetleges negatív az egészséget veszélyeztető eseményeket, laboratóriumi vizsgálatoknak kitett emberek esetében [7,8].

A mágnesterápia szakirodalma több esetben számol be a keringési rendszer állapotának javulásáról illetve a keringés fokozódásáról [6] Ez utóbbi önmagában is jelentheti azt, hogy a fizikai terhelés utáni "oxigénadósság" gyorsabban kerülhet kiegyenlítésre illetve a mikrocirkuláció szintjén végbemenő metabolikus eltérések is eredményesebben kompenzálhatók.

Az extrém izommunka kapcsán emelkedett tejsav-szint a sportolók esetében enyhe intenzitású, aerob jellegű fizikai aktivitással korrigálható[5], a védelmi szektorban azonban igen korlátozottan biztosítható erre irányuló extra elfoglaltság, sokkal kecsegtetőbb lehetőséget kínál a másra nem hasznosítható pihenés/alvás alatt történő forszírozott regeneráció. Mivel a mágnesterápia a hivatásos élő erőtől semmilyen plusz aktivitást nem igényel, kifejezetten alkalmas lehet az időegység alatt magasabb hatásfokú regenerálódás elérésére egy magnetoterápiás matracon történő alvás/pihenés. Így a hadrafoghatóság szempontjából oly fontos regenerációs idő lerövidül, úgy, hogy a restitúció gyorsítására a bajtársaink passzív idejét használjuk fel.

MÓDSZEREK

A bevont résztvevőknél spiroergometria segítségével meghatározzuk az anaerob küszöböt és a szubmaximális és vita maxima terheléshez tartozó pulzusértékeket. Minden résztvevő négyszer fogja végrehajtani az edzettségi állapotának megfelelő terheléses tesztet. Az első esetben semmilyen eszközzel sem, a másodikban könnyű fizikai tevékenységgel, a harmadikban mágnesterápiával, a negyedikben placebo terápiával "segítjük" a regenerációt a nyugalmi pulzus visszaállását követően.

A gyártó által rendelkezésre bocsátott, két teljesen egyforma eszközzel (A,B) történik a kezelés. A két eszköz közötti különbség, hogy a B eszköz nem generál mágneses teret, ezzel az eszközzel történik a placebo kezelés. Mivel a két eszköz kezelése is teljesen megegyezik (programválasztás, időzítés. stb.) a kezelést végző sem tudja, hogy az A vagy a B eszközzel történik-e a valódi terápia.

Ezzel a módszerrel kívánjuk garantálni, hogy a kettős vak, placebo kontrollált kutatást végezzünk.

Páciens gyűjtés, bevonási és kizárási kritériumok

A páciensek a hivatásos állomány tagjaiból, életkoruknak megfelelő egészségi állapotú, szolgálatra alkalmas, egészséges katonák közül kerülnek kiválasztásra, összesen 17 fő.

Bevonási kritériumnak tekintjük az életkort (30-40 év) valamint a lehetőségekhez mérten közel azonos testösszetételt (testzsír% 13-17) és edzettségi állapotot (maxVO2,...) illetve az életkornak megfelelő normál vérnyomásértéket.

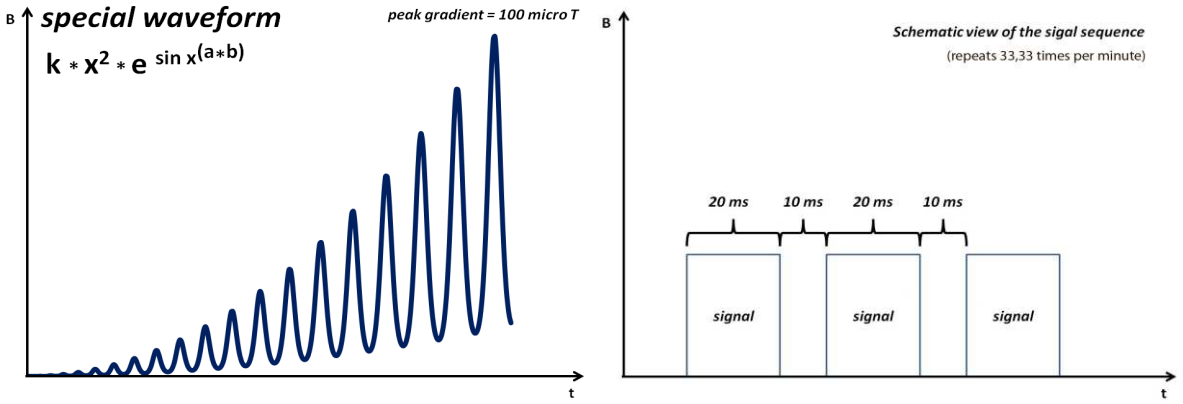
Kizárási kritérium bármely a kontraindikációk között szereplő egészségügyi probléma, valamint a bevonási kritériumoknál megadott határértékek átlépése.

Alkalmazott eszköz és a kezelés dózisa; Pulzáló jel

A 70-es évek óta a klinikai gyakorlatban is használt az ún. pulzáló jelforma, amikor is az egyes jelcsomagok meghatározott időközönként követik egymást, ami a jelforma meghatározó jellemzője. Ezek a jelformák számos betegségtípus kezelésére sikeresen lettek tesztelve az elmúlt évtizedekben. Az első FDA által csonttörések kezelésére jóváhagyott terápiás eszköz is ilyen jelformára épül[2].

Az ilyen típusú eszközök hatékonyságának befolyásoló tényezője a jelcsomagok és a közöttük lévő szünetek hossza. Valamennyi említett eszköz az alacsony frekvenciatartományban működik. A jelcsomagok közötti szünet lehetővé teszi, hogy az esetlegesen a szövetekben generálódó hőmérsékletemelkedés kevesebb, mint 1 C legyen egy 30 perces kezelés alkalmával.

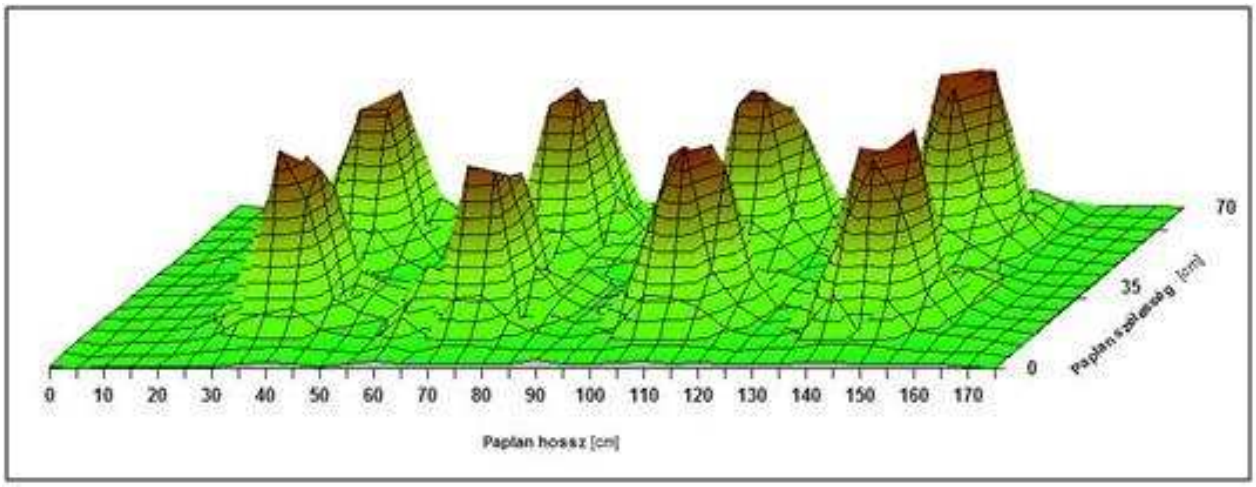
A kutatásban használt készülék egyedi jelformát alkalmaz. Alapja egy amplitúdó (exponenciálisan) modulált sinus hullám. Alsó és felső burkológörbéje egy-egy másodfokú egyenlet. Aszimmetrikus hullámforma.



1. ábra Alkalmazott jelforma fizikai jellemzői

A jelcsomag hossza 20ms, a csomagok közötti szünet 10ms. A jelforma percenként 33,33-szor ismétlődik. A jel intenzitásmaximuma 100 microT (mérési pont a matrac felett 20cm).

A matrac applikátor mérete: 180 x 70 cm, amely lehetőséget biztosít a teljes test egyidejű kezelésére. Az applikátor 8 db indukciós tekercset tartalmaz.



2. ábra Az alkalmazott matrac által generált mágneses tér háromdimenziós ábrája

Az alkalmazott mágnesterápiás készülék klinikai és otthoni kezelésre is használható.

A fentiekben megadott paraméterekkel rendelkező eszközt használtuk a kezelésre, maximális intenzitással 15 percen át.

Biztonsági megfontolások

A vizsgálatban alkalmazott eszköz minősített, II/A osztályba sorolt orvostechnikai eszköz. Rendelkezik minden szükséges engedéllyel. Az ÁNTSZ OSSKI szakvéleménye alapján az eszköz által generált pulzáló elektromágneses tér (mint nemionizáló sugárzás) minden esetben a megengedett egészségügyi határértékek alatt marad. A MAUDE és COCHRANE adatbázisok nem tartalmaznak a kutatásban használt vagy azzal ekvivalensnek tekinthető eszközzel kapcsolatos kedvezőtlen eseményről szóló jelentést. A WHO ajánlásai alapján a maximum 300 microTesla erősségű mágneses terek nem tekintendőek az egészségre ártalmasnak. Saját korábbi kutatásaink alkalmával vizsgáltuk a Ku70 gén expresszióját a terápia hatására, amely eredmények alapján arra következtethetünk, hogy az alkalmazott kezelés nem okoz akut DNS károsodást.

Összegezve az eszköz biztonságosan, várhatóan mellékhatások nélkül használható.

Diagnosztikai eljárások, mért paraméterek, adatgyűjtés

A kutatás megkezdése előtt minden résztvevő általános belgyógyász-kardiológus szakorvosi kivizsgálás keretében kerül minősítésre, minden terhelés után azonnal és negyed óránként, összesen tízszer mérjük a serum laktát szintet[9].

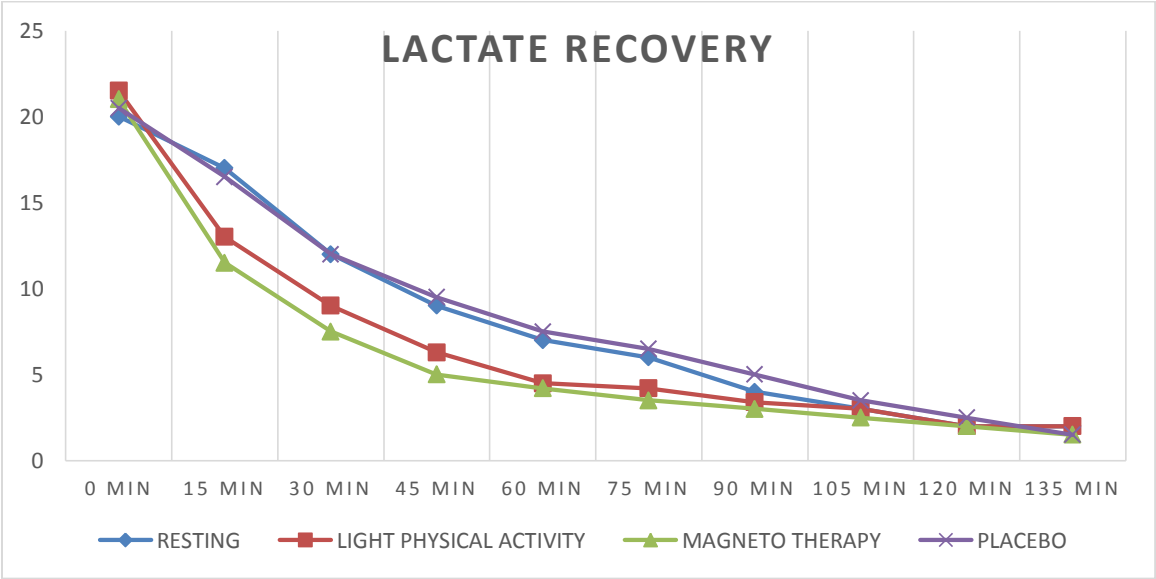
A laktát szint várhatóan szignifikánsabban gyorsabb ütemben történő csökkenése az elméleti igazolását adja a feltételezett gyorsabb regenerációnak. A gyakorlati használhatóság bizonyításaként a résztvevőkkel a terhelés után azonos idővel „fegyver összeszerelés“ tesztet végeztetünk, amelyet a gyorsabban regenerálódó csoport tagjai szignifikánsabban rövidebb idő alatt tudják végrehajtani. A tesztre a legendás AK 47 Kalasnyikov gépkarabélyt választottuk széleskörű ismertsége miatt. A Magyar Honvédségben a típus részleges szét- és összeszerelésének rekordja 18,2 másodperc (Révay Zoltán honvéd, 1971)

Statisztikai módszerek

Statistica for Windows program segítségével, a mért paraméterek alapján variancia analízissel (ANOVA) vizsgáljuk a csoportok közötti különbség valódiságát. A szignifikancia szintet p=0,05 értéken rögzítjük.

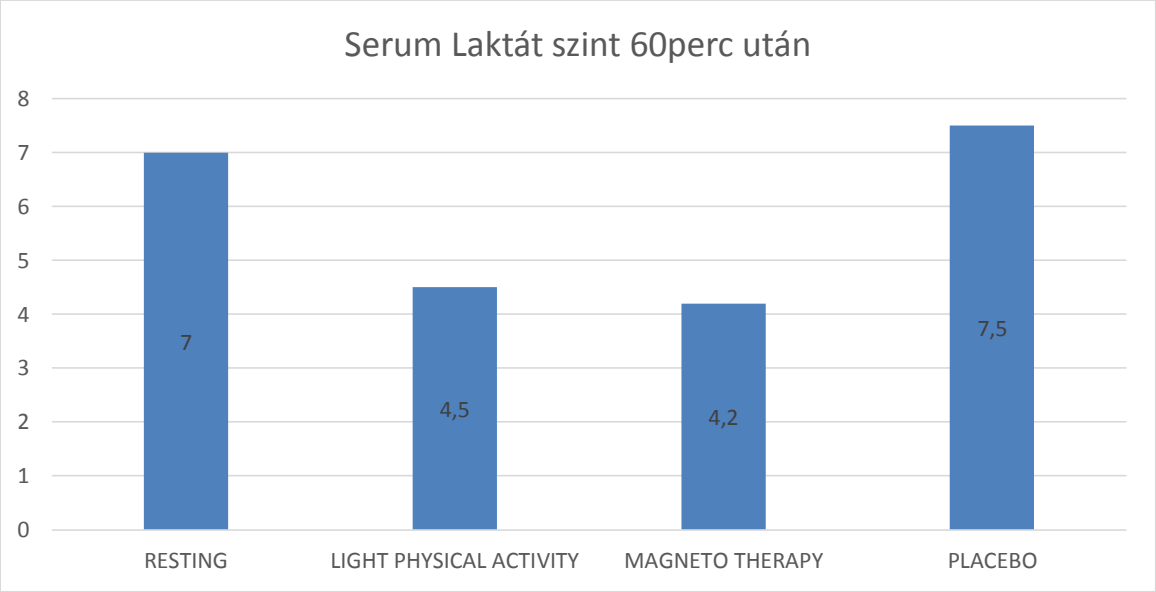
EREDMÉNYEK

A várakozásainknak megfelelően a passzív pihenés és a placebo kezelés hatására a serum laktát szint változása közel azonos ütemű. Ehhez képest a könnyű fizikai aktivitással történő regeneráció hatására a laktát szint szignifikánsan gyorsabban csökken az első órában, ugyanígy a mágnesterápiával történő regeneráció esetén is. E két utóbbi módszer között szignifikáns különbséget nem, csak numerikus eltérést tapasztaltunk a mágnesterápia javára.



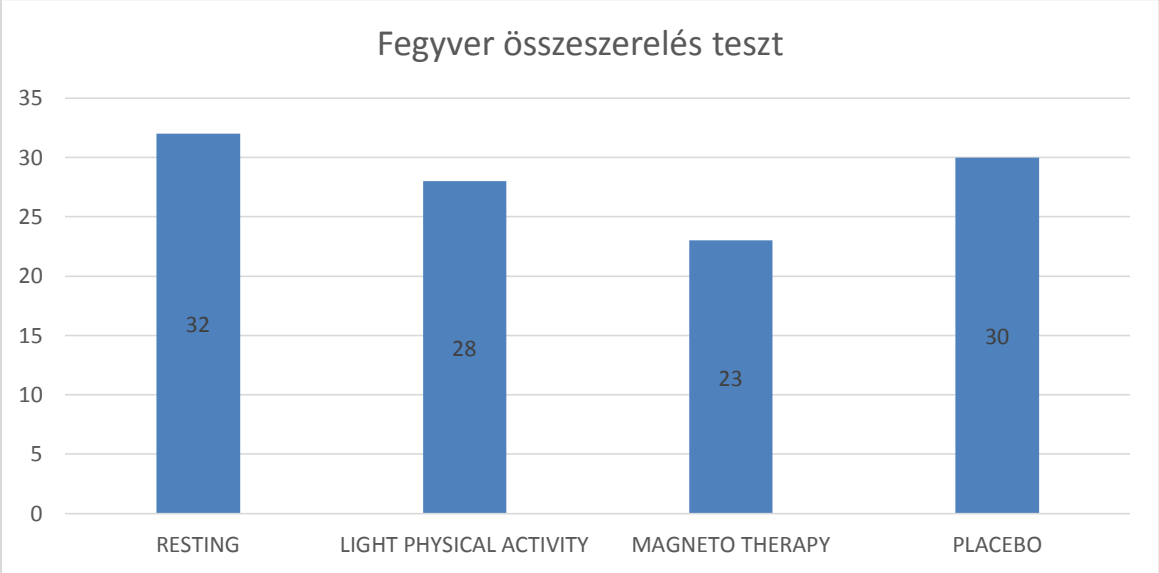
3. ábra Laktát szint időbeli változása különböző regenerációs módszerek hatására

A fegyverösszeszerelés időpontjában (60 perc regeneráció után) a könnyű fizikai aktivitást végzők és a mágnesterápiával kezeltek eredményei között csak numerikus különbség volt az utóbbi javára, ugyanakkor e két csoport eredményi szignifikánsan különböznek a passzív pihenők és a placebo kezelést kapók eredményeitől.



4. ábra Laktát szint 1 órával a fizikai aktivitás után

A terápia gyakorlati felhasználhatóságát igazolandó fegyverösszeszerelés teszt eredményi igazolták várakozásainkat. A mágnesterápiával történő regeneráció hatására mindhárom csoport eredményeihez képest szignifikánsan jobb eredmények születtek.



5. ábra Fegyverösszeszerelés teszt eredményei

KÖVETKEZTETÉSEK

Intenzív erőfeszítés, mint például futás hatására, amikor hirtelen megnő a szervezet energiafelhasználása, a tejsav gyorsabban termelődik a szövetekben, mint ahogy lebomlik, ezáltal nő a tejsav koncentrációja. Ez egy hasznos folyamat, mert így a NAD+ koncentrációja nem csökken, vagyis az energiabefektetés fenntartható ugyanakkor extrém terhelés hatására a kórosan megnövekedett laktát gátlólag hat a fizikai teljesítményre. A max terhelés 60%-a felett elérkezik egy szint, amit a szervezet már nem képes fenntartani, glükózból keletkezett piruvát nem lép be a

citrát-körbe, O2 hiányában a keletkezett tejsav felgyülemlik, az izmokban acidózis lép fel. A megnövekedett tejsavmennyiség többféle úton csökkenthető. Például a jó oxigénellátással rendelkező izomrostokban oxigén hatására piroszőlősavvá alakul, mely ezt követően a citromsavciklusban hasznosul, vagy egy másik úton a Cori-ciklus útján a májban glükózzá alakul[4].

Ismert tény, hogy az extrém fizikai terhelés hatására fellépő „oxigénadósság" és ezzel együtt a megemelkedett laktat szint csak akár 6-8 óra elteltével áll vissza a normál szintre, ugyanakkor, ha enyhe intenzitású edzéssel folytatjuk a terhelést, akkor a folyamat sokkal gyorsabb. A jelenség magyarázata, hogy a fizikai aktivitásban résztvevő vörös izomrostok jelentős mennyiségű laktátot fogyasztanak és hozzájárulnak az oxigénadósság rendezéséhez [3].

Erőteljes terhelésű edzés hatására az izom glikogéntartalmának csökkenése figyelhető meg. Terhelések során a máj fokozott katabolizmussal biztosítja egyes szervek az optimális vércukor szintjét. Mindez az izomglikogén szint csökkenését vonja maga után, aminek feltehetően az az oka, hogy a sportolók nem tudnak elegendő kalóriát (szénhidrátok) felvenni ami a regenerációs periódusban feltölthetné a raktárakat. Másrészről a terhelés során kialakult kis sérülések beavatkozhatnak a glükóz izomba történő transzportmechanizmusába és következményesen az izomglikogén szintézisébe is. Ennek oka a glükóz receptor fehérje-a GLUT-4- koncentrációjának - a sérülés miatt bekövetkező - csökkenése az izommembránban, vagy a GLUT-4 mRNS-ének alulszabályozása lehet[1]. Gyanítható, hogy a csökkent izomglikogén lehet az oka a „nehéz lábak" panaszának, mely számos túlterhelt sportolónál tapasztalható, éppúgy mint a csökkent vérlaktát-szint a szubmaximális és maximális terhelések után. Az alacsony glikogén szint természetesen limitálja a teljesítményt.

A mozgás hatására bekövetkezõ fokozott oxigén fogyasztásból eredő fokozott szabad gyök termelődésnek és a gyökök hatásai ismertek. Ismert, hogy izomkontrakció során az izomban is termelődnek szabad gyökök, illetve hogy ezek az izomrostokat károsító hatással bírnak. Az akut mozgással összefüggő kimerültség során a szarkoplazmatikus retikulum funkciójának és a kalcium egyensúlynak a zavara a szabad gyökök miatt következik be. Így az izomzat túledzése izomzati károsodást és fáradtságot okoz, amelyet részben a szabad gyökök által károsított makromolekulák indukálnak. A terhelés utáni ultrastruktúrális károsodás és az izommembrán integritásának csökkenése lehet az oka a túledzésre jellemző más tünetek megjelenésének. Mindez magában foglalja az elhúzódó izomerő csökkenést, izomfájdalmat, kalcium egyensúly felborulását és a fokozott fehérje sérülést.

El kell fogadnunk azt az alapvetést, hogy napjaink digitális harcmezejének legértékesebb szereplője az ember, mert a katona életét pénzben kifejezni nem tudjuk, ellentétben bármely technikai eszközzel. Harcoló bejtársunk helyébe nem tudunk egyszerűen beilleszteni ugyanolyan katonai életúttal ÉS harctéri tapasztalattal ÉS pszichés ÉS mentális ÉS fizikális paraméterekkel rendelkező alteregót, akinek személyiségét azonos módon illeszteni tudjuk a katonai alakulat egységébe. Ezen a nézőponton keresztül világítható meg minden olyan procedúra értéke, amely a hadrafoghatóságot, a harcértéket, a bevetések közötti regenerációt akár csak néhány százalékkal is potencírozni képes. Mert az extrém kritikus körülmények között ezek a nüanszok dönthetnek a katonai feladat sikeressége vagy éppen bajtársaink megsérülése vagy akár elvesztése vonatkozásában. Jelen munka 1 újabb %-ot kíván hozzátenni a harcosaink hatékonyságához és ezen keresztül honfitársaink biztonságához.

Felhasznált irodalom

[1] Richter E.A., Daugaard J.R., 1995. Eccentric exercise decreases glucose transporter GLUT4 protein in human skeletal muscle. Journal of Physiology, 482: 705-712.

[2] Bassett, C. A. L., Pawluk, R. J., & Pilla, A. A.: Acceleration of fracture repair by electromagnetic fields. Annals of the New York Academy of Sciences, 1974; 238, 242–262.

[3] Ebbeling C., P.M. Clarkson. 1989. Exercise-induced muscle damage and adaptation. Sports Medicine, 7:207-234.

[4] Ji L.L. 1993. Antioxidant enzyme response to exercise and aging. Medicine and Sciences in Sport and Exercise, 25: 225-231.

[5] Kohut L., Extrém fizikai terhelésnek kitett katonai állomány keringési és élettani vizsgálata, PhD dissertation, National University of Public Service, Hungary, 2008.

[6] Rikk J., Finn K.J., Liziczai I., Radák Zs., Bori Z., Ihász F., Influence of Pulsing Electromagnetic Field Therapy on Resting Blood Pressure in Aging Adults, Electromagnetic Biology and Medicine, June 2013; 32(2): 165–172

[7] Ruppe I., Hentschel K., Eggert S.: Schienengebundene Transportsysteme. Schienengebundene Transportsysteme. Teil 1: Exposition durch statische und niederfrequente elektrische und magnetische Felder an der Magnetschwebebahn Transrapid 07 (Untersuchungsbericht), SchrR BAuA 1995(Fb 11.001): 1 - 104

[8] Sander, R., Brinkmann, J., Kuhne B.: Laboratory studies on animals and human beings exposed to 50 Hz electric and magnetic fields. CIGRE, International Congress on Large High Voltage Electric Systems, Paris, 1–9 September; CIGRE Paper 36–01; 1982.

[9] Urhausen A., W. Kindermann. 2000. Aktuelle Marker für Diagnostik von Überlastungszuständen in der Trainingspraxis. Deutsche Zeitschrift für Spormedizin, 51(7-8): 226-233.

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Kuti Rajmund
kuti.rajmund@sze.hu

TERRORCSELEKMÉNYEK UTÁN VÉGZETT KOMPLEX KÁRFELSZÁMOLÁSI MŰVELETEK AKTUÁLIS KÉRDÉSEI

Absztrakt

A hivatásos kárfelszámolási feladatokat végrehajtó szervezetek szerepe a különleges veszélyhelyzetek kezelésében, azon belül a terrorcselekmények következményeinek elhárítása során rendkívül fontos. Magyarország nem tartozik a világ súlyos terrorcselekményekkel érintett övezetei közé, de a közelmúltban, Párizsban és Brüsszelben történt robbantások rámutattak, hogy egy terrortámadás bekövetkezésének valószínűsége hazánkban sem nulla. Ha viszont bekövetkezik az esemény, a Terrorelhárítási Központra, a Magyar Honvédség Különleges Egységeire, a Hivatásos Tűzoltóságra, mint elsődleges beavatkozó szervezetekre komoly, összetett feladatok hárulnak. A sikeres mentés alapja a beavatkozás irányítási, taktikai feladatainak pontos kidolgozása, valamint a kárfelszámolási műveleteket végző szervezetek közötti zavartalan együttműködés. Írásomban elemzem a rendkívüli körülmények között történő mentési feladatok problémáit, bemutatom az együttes feladatmegoldás, rugalmas irányítási mechanizmus, megfelelő taktika alkalmazási lehetőségeit.

The roles of professional organizations dealing with damage liquidation at special treatment of emergencies are very important, also to mitigate the consequences of terrorist acts. Hungary is not included in the areas affected by terrorist acts, but the recent bombings in Paris and Brussels have pointed out, that the probability of terror attack might not be zero in our country. However, if the event occurs, complex tasks are incumbent on Counter-Terrorism Centre, Hungarian Defence Forces and special units of the professional fire service as primary responding organizations. The base of a successful intervention is accurate developing of the management, tactical tasks and the smooth cooperation between the organizations conducting remedial operations. In this article, I analyse the problems of rescue operations in exceptional circumstances; I present joint problem solving, flexible management mechanism and opportunities to apply appropriate tactics.

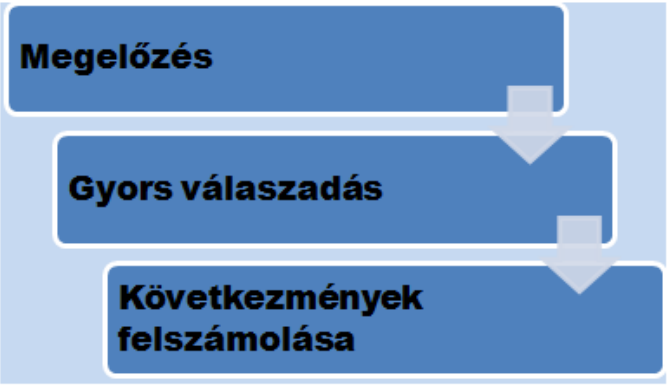
Kulcsszavak: *Terrorizmus, terrorcselekmények, komplex kárfelszámolási műveletek, ~ Terrorism, terror acts, complex remediation operations.*

BEVEZETÉS

A terrorizmus kérdése napjaink állandó problémája. Nem telik el úgy egyetlen nap sem, hogy a híradásokból ne hallanánk a világ valamely pontján bekövetkezett terrorcselekményekről. Az utóbbi hónapokban az Európai Unió több nagyvárosában történt terroristák által végrehajtott fegyveres támadások, robbantások azt mutatják, hogy nem pusztán megfélemlítésről, fenyegetettségről van szó, hanem ártatlan emberek halálát okozó kiszámíthatatlan terrortámadásokról. Ezek az események rávilágítottak arra, hogy egy lehetséges terrorcselekmény bekövetkezésének valószínűsége Magyarország viszonylatában sem nulla, ezért hazánk kormánya megtette a megfelelő biztonsági intézkedéseket. Egy-egy bekövetkező terrorcselekményre egyszerűen lehetetlen felkészülni, ugyanis a terroristák a legkülönfélébb módszereket alkalmazzák a totális pusztítás érdekében. A terrorizmus problémakörével foglalkozó szakemberek szerint az egyik legfontosabb kérdés a terrorcselekmények bekövetkezésének megakadályozása.[1] A megelőzés kérdését prioritással kell kezelni, azonban egy esetlegesen bekövetkező terrortámadással mindig számolni kell. Ha mégis bekövetkezik az esemény, a lehető leggyorsabban el kell kezdeni az életmentési-kárfelszámolási munkálatokat. Ezzel kapcsolatban viszont több kérdés is felmerül, melyek tisztázásának érdekében írásomban a terrorizmus kezelésével kapcsolatos alapvető feladatok ismertetése után bemutatom a kárfelszámolásra jogosult szervezetek mentési képességeit. Vizsgálom továbbá a beavatkozások szabályait, az irányítás, a kommunikáció kérdéskörét és javaslatot teszek a humán állomány beavatkozásokra történő felkészítésének egyes lépéseire is.

A TERRORIZMUS ELLENI HARC IDŐSZAKAI

Amikor a nemzetközi terrorizmussal kapcsolatos kutatásokat végezzük, vizsgálatainkat a folyamat, rendszer, hálózatos szemléletmódnak megfelelően kell végezni, ennek alapján a terrorellenes lépéseket időbeli intervallumban is elemezni kell. Padányi József korábbi írásában [2] a terrorizmus elleni harcot már folyamatként kezelte és időbeni kiterjedését is vizsgálta. A terrorizmus elleni harc időbeni kiterjedését a következő ábra szemlélteti:



1. ábra: A terrorizmus elleni harc időbeni kiterjedése, (Forrás: Szerző összeállítása [2] adatai alapján)

A fenti ábrán megjelenített fő időszakok egymással szorosan összefüggnek, azokon belül a következő speciális feladatok végrehajtása történik:

Megelőzés:

- Az elkövetett terrorcselekmények tanulmányozása (szervezetek, módszerek, eszközök),
- A terrorszervezetek felderítése, folyamatos megfigyelése,
- A lehetséges célpontok megjelölése, tanulmányozása,
- Veszélyeztetettségi kockázatok csökkentése,
- A terrorcselekmények megelőzésére vonatkozó szabályzók, intézkedések bevezetése, szükség szerinti fenntartása,
- Folyamatos együttműködés az érintett szervezetek között,
- Tapasztalatok beépítése a végrehajtó humán állomány kiképzésébe.

Gyors válaszadás:

- A folyamatban lévő terrorcselekmény megszakítása,
- Válaszcsapás, a fenyegetett erők és eszközök folyamatos védelme,
- Együttműködés az érintett szervezetekkel.

Következmények felszámolása:

- Kárfelszámolás azonnali megkezdése, életmentés, további károk bekövetkezésének csökkentése,
- Másodlagos veszélyforrások felkutatása, kiiktatása,
- Helyreállítás,
- Együttműködés az érintett szervezetekkel.

Az egyes időszakokhoz köthető feladatokat vizsgálva megállapítható, hogy köztük lévő átmenetek nem köthetők időponthoz, több feladat végrehajtása párhuzamosan zajlik, hasonlóan az aszimmetrikus hadviselés során alkalmazott módszerekkel.[3] Jelen cikk terjedelmi korlátai nem teszik lehetővé, hogy az összes speciális feladatot elemezzem, ezért csak a kárfelszámolási tevékenységhez kapcsolódó feladatokat vizsgálom.

A KOMPLEX KÁRFELSZÁMOLÁS KIEMELT KÉRDÉSEI

Magyarországon a mentési-kárfelszámolási műveletek végrehajtására képes, a feladatok ellátásához szükséges erőkkel és eszközökkel rendelkező szervezetek közül a Hivatásos Tűzoltóság és néhány készenléti szolgálatot ellátó speciális mentőegység képes a nap bármely szakában két perc riasztási idővel,[1] technikai eszközökkel felszerelt kiképzett egységekkel a legrövidebb úton az adott kárhelyre vonulni, és ott szervezetten beavatkozni. A beavatkozásnak azonban vannak korlátai. Egy bekövetkezett terrortámadás helyszínén, a robbantáson, tűzön, épületomláson túl számolni kell biológiai, vegyi vagy akár radioaktív anyagok jelenlétével is. A rendkívül veszélyes területeken, extrém körülmények között történő kárfelszámolási, vagy műszaki támogató feladatok végrehajtása komoly kihívást jelent bármely egység számára.[4] Egy ilyen komplex beavatkozáshoz a tűzoltóság sajnos nem rendelkezik minden eszközzel és védőfelszereléssel, de logisztikai háttérrel sem. Kijelenthetjük, hogy egy hosszan tartó összetett kárfelszámolási feladatot csak a társszervekkel közösen, egymás különleges képességeinek maximális kihasználása mellett lehet a leghatékonyabban végrehajtani.[5] A Terrorelhárítási Központ egységei különleges eszközökkel rendelkeznek. A Hivatásos Tűzoltóság a tűzoltási, műszaki mentési, valamint

[1] 39/2011. (XI.15.) BM rendelet, a tűzoltóság tűzoltási és műszaki mentési tevékenységének általános szabályairól, 37.§. (3).

veszélyes anyagok jelenlétében történő beavatkozásokhoz rendelkezik megfelelő eszközrendszerrel. A Magyar Honvédség a különleges műszaki feladatokhoz, veszélyes környezetben, szennyezett területen történő feladat végrehajtáshoz szükséges speciális szakfelszerelésekkel rendelkezik. Ahhoz viszont, hogy ezeket a különleges képességeket megismerjék a különféle kárfelszámolást végző szervezetek, közös gyakorlatokat kell szervezni, és a feladatokat begyakoroltatni az érintett állományokkal. Ez a sikeres mentés elengedhetetlen feltétele.[6]

A kárfelszámolás során a következő kérdéseket kiemelt figyelemmel kell kezelni:

- A bekövetkezett terrorcselekményre történő első reagálás.
- Értesítési, riasztási feladatok végrehajtása (megfelelő erők és technikai eszközök).
- Kiérkezés, eszközök felállítási helyének megválasztása.
- Pontos, és folyamatos felderítés.
- Orvosi támogatás a helyszínen.
- Életmentés gyors megszervezése, megkezdése.
- Kárfelszámolási stratégiai műveletek, kiemelt feladatok, társszervek közötti összehangolása, megkezdése.
- Irányítási feladatok, hatáskörök, intézkedések egyeztetése.
- Helyszín körülhatárolása, környezetének teljes lezárása.
- Kárfelszámolást végző szervezetek közötti kommunikáció, információ áramlás biztosítása.
- Logisztikai háttér biztosítása.
- Környezet folyamatos megfigyelése (rendellenességek, oda nem illő tárgyak stb.).

A KÁRFELSZÁMOLÁS TAKTIKAI PROBLÉMÁI

A terrorcselekmények okozta károk felszámolásához merőben más taktikai fogások alkalmazására van szükség, ezért kiemelt figyelmet kell fordítani arra, hogy a megszokott taktikai lépéseken változtassunk. A megfelelő és hatékony taktika kidolgozásához tanulmányozni kell a terroristák által alkalmazott módszereket, ismerni kell a terroristák fő céljait, melyek a következők lehetnek:

- Teljes megsemmisítés, teljes körű pusztítás.
- A lehető legtöbb polgári áldozat.
- Az infrastruktúra kritikus részének megsemmisítése.
- Gazdaság bénítása.
- Zavarkeltés, pánik okozás.
- Médiában történő szereplés.[7]

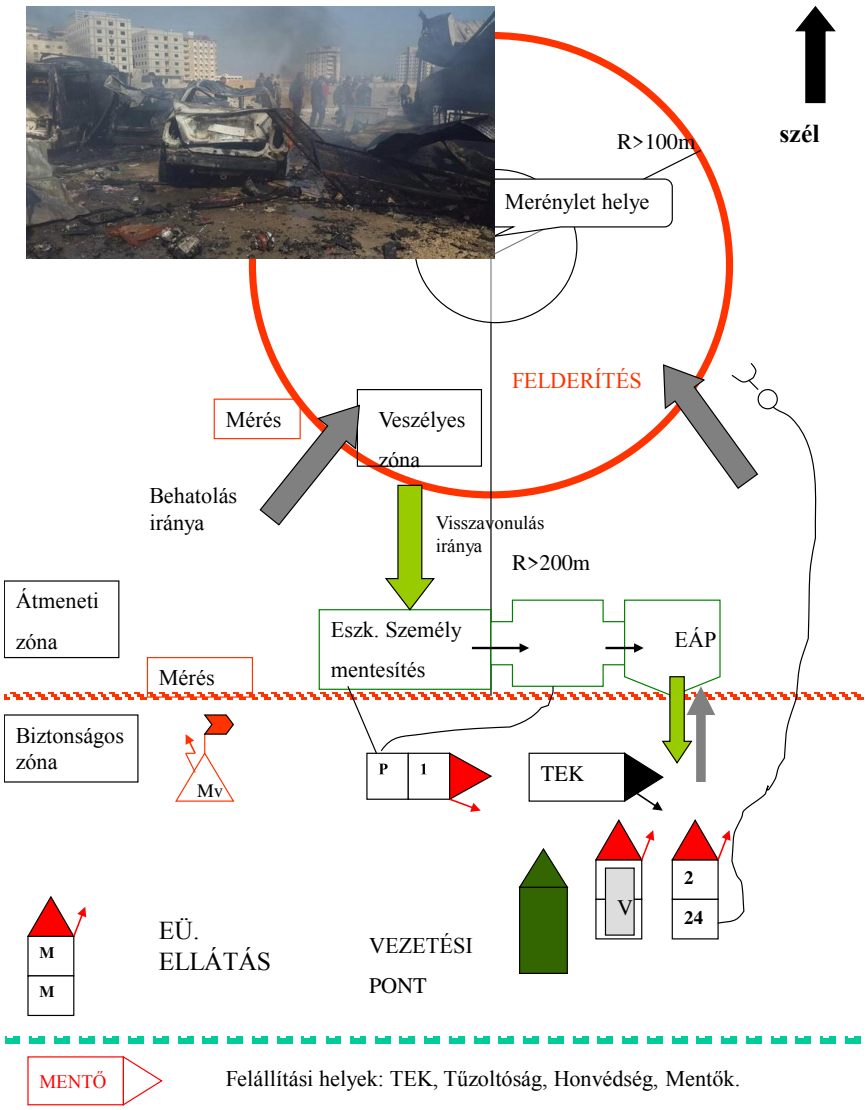
A terroristák egyik fő célja a lehető legnagyobb pusztítás. Ennek érdekében több lépcsőben, a dominó hatás figyelembevételével hajtják végre cselekedeteiket. Ez azt jelenti, hogy az első robbantást követheti, megfelelő időzítéssel több másik is, vagy az egyik robbantás során mérgező vegyi, biológiai, de akár radioaktív anyag is a környezetbe kerülhet. További fontos feladat a beavatkozást végző erők műszaki védelmének biztosítása is, melyben a Magyar Honvédség műszaki alakulatai széleskörű tapasztalatokkal rendelkeznek. [8] Mentés során folyamatosan számolni kell a lehető legnagyobb veszéllyel, ennek megfelelően kell a taktikai lépéseket kidolgozni és a védelmi szinteket meghatározni. Ha a megszokott taktikának megfelelően a mentésre egyszerre, egy időben a legnagyobb erőt vetjük be, valószínűleg a mentőerők közül is több áldozat lesz. A mentésben résztvevők megóvásának érdekében speciális taktikai megoldásokat kell alkalmazni.

Ezek a következők lehetnek:

- A helyszínre érkező mentőerők több útvonalon közelítsék meg a helyszínt, az eszközök felállítási helyét a védelmi szempontok alkalmazásával kell kijelölni.
- A mentésben résztvevő állomány védőfelszereléseinek meghatározása.
- Megfelelő nagyságú terület lezárása.
- Folyamatos mérgező és radioaktív anyag koncentráció mérése.
- Biztonsági zónák kijelölése.
- Ellenőrző áteresztő pontok, mentesítő helyek, egészségügyi ellátó pontok kijelölése.
- A másodlagos események kivédése miatt egyszerre csak kisebb csoportokban lehet bevetni a végrehajtó erőket, a kutatási-mentési terület pontos megjelölésével.
- Az életmentést orvosi felügyelet mellett kell végezni.
- Az állomány cseréjéről gondoskodni kell.
- Logisztikai feladatok ellátása.

Az előzőekből következik, hogy az elsőként a kárhelyre érkező egység parancsnokának a szakértelmén, felkészültségén, pontos döntésein, rendkívül sok minden múlik. Egy-egy eszköz felállítási helyének meghatározása, vagy biztonsági zóna kijelölése, de a beavatkozás menetének meghatározása is, komoly hatással lehet az egész mentés kimenetelére. A következő ábrán egy terrorcselekmény következményeinek felszámolására irányuló beavatkozás elvi sémája látható. A vázlat készítésénél a legnagyobb veszélyforrások előfordulásával számoltam. Ilyen jellegű komplex beavatkozásokhoz egyetlen szabályzat sem tartalmaz konkrét, egységes előírásokat, ezért a nemzetközi és hazai tapasztalatokat is próbáltam figyelembe venni az egyes zónák meghatározásánál.

A mentés során szükségessé váló helyváltoztatások során, főleg ha azok a terrorcselekménnyel érintett épületek irányába történnek, tűzszerészekkel történő egyeztetés is szükséges.[9] A taktikai lépések kidolgozásánál fontosnak tartom figyelembe venni a Magyar Honvédség műszaki alakulatainak külföldi missziókban szerzett tapasztalatait is.[10]



2. ábra: Elvi beavatkozási séma terrorcselekmény esetén, (Forrás: Szerző összeállítása)

KOMMUNIKÁCIÓS PROBLÉMÁK

A kárfelszámolás hatékonyságát, annak kimenetelét nagyban befolyásolja az egységek és a vezetési pont közötti, valamint a kárhelyszínen történő kommunikáció. A nehézségek elkerülése érdekében a közvetlen kárhelyi kommunikációra külön figyelmet kell fordítani, ugyanis az elmúlt évek terrorcselekményeit vizsgálva megállapítható, hogy a terroristák előszeretettel használnak olyan bombákat, amelyeket a rádióelektronikai berendezések (URH-EDR rádió, mobil telefon, személyi hívó) a bombától akár 100 méteres távolságban történő üzemelése hoz működésbe.

A kárhelyszínen tehát és a kárfelszámolást végző egységek, illetve a vezetési pont közötti kommunikációt (legalábbis amíg a tűzszerészek a helyszínt át nem vizsgálták) célszerű robbanás-biztos (RB) kivitelű rádiók alkalmazásával lebonyolítani, amennyiben ezek nem állnak rendelkezésre, akkor hírvivők útján kell továbbítani az információkat, mellőzve minden rádióelektronikai berendezést. A különféle szervezetek közötti kommunikáció

megszervezésére és folyamatos fenntartására szintén nagy hangsúlyt kell fektetni, a folyamatos információáramlás elengedhetetlen feltétele a hatékony kárfelszámolásnak.

KÖVETKEZTETÉSEK

A terrorizmus elleni küzdelem csak széles körű összefogással valósítható meg. Különösen igaz ez a komplex kárfelszámolási feladatok végrehajtására. Nem szabad figyelmen kívül hagyni azt a tényt, hogy a mentési feladatokat végző erők és eszközök is a terroristák célpontjai lehetnek. A beavatkozási szabályok kidolgozásához és folyamatos felülvizsgálatához elengedhetetlen a nemzetközi tapasztalatok feldolgozása. A nehéz körülmények közötti mentési, műszaki védelmi, speciális támogatási feladatok taktikai lépéseinek a humán állomány részéről történő készségszintű alkalmazásához elengedhetetlen a rendvédelmi szervek és a haderő együttes részvételével megvalósuló szimulációs gyakorlatok szervezése.

Sajnos hazánkban egyetlen mentésre jogosult szervezet sem rendelkezik önállóan olyan erő és eszközkészlettel, hogy egy terrorcselekmény következményeinek felszámolására irányuló komplex mentést önállóan képes legyen végrehajtani. A megoldás az összefogásban rejlik. Meg kell ismerni a kárfelszámolásban résztvevő összes szervezet különleges képességeit, ki kell dolgozni a taktikai lépéseket, és gyakorlatokat kell szervezni az érintett állományok részére. Biztosítani kell a kommunikációs és logisztikai hátteret. Folyamatosan figyelemmel kell kísérni a külföldi eseményeket, elemezni a tapasztalatokat. A Magyar Honvédség különleges egységei folyamatos résztvevői nemzetközi katonai misszióknak, melyek közül több küldetést fokozottan terrorveszélyes országban kell végrehajtani. Katonáink a nemzetközi erőkkel együttműködve a legújabb módszereket ismerik meg és modern eszközök alkalmazását sajátítják el, melyek hazai gyakorlatba történő adaptálása kiemelt feladat. Írásommal fel kívántam hívni a figyelmet a téma aktualitására, bízva abban, hogy folyamatosan kiemelt figyelmet kap cikkben vázolt kérdések megoldása.

Felhasznált irodalom

[1] Kőszegvári Tibor – Resperger István: A nemzetközi terrorizmus elleni harc katonai tapasztalatai III. Egyetemi jegyzet, ZMNE Budapest, (2005)

[2] Padányi József: A Magyar Honvédség lehetőségei a terrorizmus elleni harcban, pp. 1-45. ZMNE Budapest, (2003)

[3] Padányi József: Az aszimmetrikus hadviselés során alkalmazandó eljárások, eszközök és módszerek, HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 25: (1-2) pp. 81-82.

[4] Tomolya János – Padányi József: A terrorizmus jelentette kihívások HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA *22***:**(3-4) pp. 34-67. (2012)

[5] Kuti Rajmund: Terrorcselekmények kárfelszámolási lehetőségeinek vizsgálata tűzoltói aspektusból, Védelem katasztrófa- tűz– és polgári védelmi szemle, ISSN 1218-2958, XIV. évf. 3. szám 34-35. p. (2007)

[6] Kuti Rajmund: Terrorcselekmény következményeit felszámoló gyakorlat tapasztalatai, Védelem katasztrófa- tűz– és polgári védelmi szemle, XIV. évf. 4. szám 34-35. o. 2007. ISSN 1218-2958,

[7] Tomolya János, Padányi József: A TERRORIZMUS ÉS A GERILLA HADVISELÉS AZONOSSÁGAI ÉS KÜLÖNBSÉGEI, HADTUDOMÁNY (ONLINE) 24: (1) pp.

126-154. URLcím:
http://www.mhtt.eu/hadtudomany/2014/2014_elektronikus/11_TOMOLYA_PADANYI.pdf
(letöltés ideje: 2016. 04. 11.)

[8] Padányi József: A katonai műveletek terrorvédelme
NEMZETVÉDELMI EGYETEMI KÖZLEMÉNYEK X:(3) pp. 200-206. (2006)

[9] Padányi József: A katonai műveletek terrorvédelme, a tűzszerész kapacitások értékelése, A nemzetközi terrorizmus elleni küzdelem időszerű társadalmi, katonai és rendvédelmi kérdései c. konferencia, Konferencia helye, ideje: ZMNE Budapest, Magyarország, 2007.10.

[10] Padányi József – Tomolya János: A műszaki erők alkalmazása az iraki Szabadság Műveletben
HADTUDOMÁNYI SZEMLE 1:(3) pp. 34-47. (2008)

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Szabó József
szabo.jozsef95@chello.hu

REPÜLÉS A BOLYGÓKÖZI TÉRBEN ŰRDINAMIKA SOROZAT – 5. RÉSZ

Absztrakt

Cikksorozatunk 5. részében az olvasó találkozhat a bolygóközi repülés elvi és gyakorlati kérdéseivel. A cikk bemutatja a Föld hatásszférájának elhagyásával kapcsolatos legfontosabb matematikai összefüggéseket, a heliocentrikus, a távolodási és az indulási sebességek fizikai jelentését. A cikk következő része bemutatja az ember Mars-utazásának problémáit, amely után az olvasó megismerkedhet a Voyagerek Naprendszer-béli repülésének kérdéseivel.

In the 5th part of our article series the reader can face with conceptual and practical issues of flight in the interplanetary space. The present article reviews the most important mathematical interrelations of leave Earth's impact sector, the physical content of heliocentric velocity, speed of recession and start-up speed. The next part of article presents problems of human spaceflight to Mars, after it the reader can face with questions of flight Voyagers in the Solar system.

Kulcsszavak: *a bolygóközi tér, heliocentrikus, a távolodási és az indulási sebességek értelmezése ~ the interplanetary space, heliocentric, the recession and the start-up speeds interpretation*

A FÖLD HATÁSSZFÉRÁJÁNAK ELHAGYÁSA

A korábbi anyagban a Föld körüli repülést elemezve, megismerkedtünk egy adott égitestnek, esetünkben a Földnek a vonzáskörzetében végzendő űrrepülések, manőverek legfontosabb kérdéseivel. Az ott szerzett ismeretek, természetesen minden égitestre vonatkoznak, csupán minden esetben az adott égitestre vonatkozó adatokkal kell számolni. A továbbiakban kilépünk a Föld vonzáskörzetéből, s ha már kijutottunk a bolygóközi térbe, megvizsgáljuk az ott végzendő repülés sajátosságait.

A bolygóközi repülés tehát a Föld hatásszféráján túli repülést jelenti. Egyébként ezt a kérdést vizsgálta a neves orosz tudós, Konsztantyin Ciolkovszkij is, amikor a Föld vonzerejének a legyőzésével számolt és az ehhez tartozó, a Föld hatásszférájának az elhagyását, vonzerejének végleges legyőzését biztosító sebességértéket kereste. Ő a Föld körüli repülés kérdésével nem foglalkozott. A sebességértéket kutatva, Ciolkovszkij, figyelmét a már említett, és később második kozmikus sebességének nevezett sebesség értékének meghatározására fordította. Ő azonban ezt a sebességet a Föld vonzerejének végleges legyőzéséhez szükséges sebességnek nevezte. Ennek meghatározása érdekében energetikai számításokat végzett és ennek a számításnak az eredményeként azt meg is találta.

A továbbiakban megalkotta az egylépcsős rakéta által létrehozható sebességét meghatározó képletet, s a kapott eredmények összevetéséből vonta le a tanúságokat. Ezek elemzése alapján ugyanis egyértelművé vált, hogy egylépcsős rakétával nem lehet a Földet véglegesen elhagyni, de még a Föld körüli pályára sem lehet kivezetni a hasznos terhet, vagyis az űrhajót. Ennek köszönhető a többlépcsős, vagy ahogy Ciolkovszkij nevezte, a „rakétavonat" gondolata. Egyértelmű tehát a megállapítás, hogy a bolygóközi térbe csak többlépcsős rakéta segítségével lehet kijutni. E kutatásnak köszönhetően tárta fel a neves tudós a második kozmikus sebesség fizikai lényegét, és így történhetett, hogy e sebesség korábban megszületett, mint az első. [8, 9, 10] Az első kozmikus sebesség, mint fogalom, ugyanis nagy valószínűséggel csak 1920-as 30-as években jelent meg először Esnault-Pelterié, illetve Ary Sternfeld munkáiban.[8]

Érdekességként megemlítjük, hogy a csillagokhoz való utazás évezredeken át ott volt a köztudatban, de az csak a képzelet szárnyán született és foglalkoztatta az embereket.[2] Jelen tanulmány a bolygóközi térbe való kilépés kérdéseit mutatja be az olvasónak, s egyértelművé teszi a tényt, hogy ez ma már a reális valóság. A képletekkel bizonyított tények egyértelművé teszik azt is, hogy ott már a Nap lesz az a központi égitest, amely meghatározza a mozgás lényegét, s ennek megfelelően, a számításoknál a Nap adatait használjuk fel, s csak azok segítségével juthatunk helyes megoldásra. Érdekességként megemlítjük, hogy a volt Szovjetunióban, az 1960-as 1970.es években voltak olyan nézetek, hogy nem a Holdra szállás a fontos, hanem a Mars körberepülése. Erre készültek tervek is, de azokat elvetették, miután megfelelő rakétahajtómű nem állt rendelkezésükre. Egy ilyen vállalkozás akkor még nem rendelkezett reális alapokkal.[6]

Ha a bolygóközi térbe akarunk kijutni, akkor olyan többlépcsős rakétával kell számolni, amelynél a lépcsők száma általában három vagy négy lehet. Szondákat már küldtek a bolygóközi térbe, de embert még nem. Az ember biztonságát szavatoló eszközöknek a megteremtése bonyolult feladat, amelyre a robotok esetében nincs szükség. Összességében megállapíthatjuk, hogy ha csak a dinamikai problémákat vizsgáljuk, az ember utazása esetén a feladatok jelentős mértékben megszaporodnak. A továbbiakban a dinamikai kérdésekhez szükséges manővereket vizsgáljuk, amelyek megoldásához a következők szükségesek:

1. Az űrhajót Föld körüli, ún. parkoló, vagyis közbülső pályára kell állítani. Egyébként a pályára állításhoz szükséges starttömeg számításai határozzák meg azt, hogy mennyi tolóerő szükséges a rakétakomplexum starttömegének a Föld körüli pályára állításához. Ez fontos mutató, hiszen a tapasztalatok azt igazolják, hogy egy t tömeg

Föld körüli pályára állításához — ha a cél valamelyik bolygóhoz való repülés, és jelentős nagyságú tömeget kell Föld körüli pályára állítani —, a starton, több mint 50 t hajtóanyagtömeg szükséges. Példaként szolgáljon két adat: A Holdra repülés során, a Saturn V rakétakomplexum alkalmazásakor, a Hold körzetébe juttatott tömeg 35-37 t volt és hogy az ehhez szükséges mintegy 120 t tömeget a Föld körüli pályára állítsák, a starton, tonnánként mintegy 17 t hajtóanyagot használtak fel. Azt már a korábbi anyagokból tudjuk, hogy a tolóerő legalább 20-25, de esetenként, ha csak Föld körüli pályára kell kijuttatni a hasznos terhet, akár 50%-kal is meghaladhatja a starttömeg súlyerejét. Itt tehát már jelentősége van annak a ténynek, hogy a cél milyen távolságra van a Földtől, mekkora hasznos tömeget kell a Föld körüli pályára állítani, és a cél eléréséhez milyen sebességre kell a Föld körüli pályára állított, hasznos tehet felgyorsítani.[7]

2. A Föld körüli pályán keringő űrobjektumot a megfelelő pillanatban gyorsítani kell a magasságnak megfelelő II. kozmikus sebességnél nagyobb sebességértékre, hogy a Föld hatásszférájának a határán — az elérendő cél távolsága függvényében — meglegyen a megfelelő nagyságú heliocentrikus sebesség, vagyis a Föld hatásszférájától az űrobjektum olyan távolodási sebességgel haladjon, amely a Föld közepes pályasebességével együtt biztosítja a cél eléréséhez szükséges heliocentrikus sebességet. Példaként megemlíthetjük, hogy a Hohmann-ellipszis esetén, a Mars körzetébe való utazáshoz pl., a Föld hatásszférája határán, közel 3 km/s távolodási sebességre van szükség. (E kérdés részleteinek a tárgyalására, képletek alkalmazásával, rövidesen rátérünk.)[7]
3. A hatásszféra határát elhagyva, az azon túli pályán való repülésre már a Nap vonzáskörzetében kerül sor, olyan heliocentrikus sebességgel, amilyen szükséges ahhoz, hogy az űrhajó a célbolygó magasságára jusson fel vagy süllyedjen le. Fontos szerepet kap a repülés irányítási módszerének a kiválasztása, amely a gyorsan fejlődő űrtevékenység igényeit kielégíti.[4] Ha a cél egy belső bolygó elérése, akkor csökkenteni kell a sebességet, hogy a Nap vonzereje nagyobb legyen, mint a centrifugális erő, és akkor ez az erő az űrobjektumot behúzza a belső célbolygó pályájára. A két manővert, vagyis a Föld hatásszférájának az elhagyását, az első esetben a Föld haladási irányának megfelelő, a második esetben pedig azzal 180°-al ellentétes irányba kell végezni.[1, 3]
4. Megérkezvén a célbolygó hatásszférájának határához, az oda való belépés, és a továbbiakban a repülés végrehajtása a célbolygó hatásszférájában, majd a célbolygó körül, s ha az a cél, hogy leszálljunk a bolygó felszínére, akkor a megfelelő módszer alkalmazásával, végső soron a leszállás végrehajtása lesz a feladat. Ez sem egyszerű feladat, hiszen a leszállás történhet olyan bolygóra, amelynek légköre van és olyanra, amelynek légköre nincs. A Marsra szállás sajátossága, hogy ritka a légköre, de nem mondhatjuk, hogy nincs légköre. Ezért a leszállás módszerét is kutatják, s eddig néhány módszert már ki is próbáltak, de nagy a valószínűsége, hogy a Marsra szállásnál is a Holdra való leszállásnál alkalmazott módszert, vagy annak valamilyen változatát fogják alkalmazni.[5]

Tudni kell, hogy napjainkban, a Naprendszerben, az ember számára csak egyetlen bolygó jöhet számításba ilyen utazási céllal, s ez a Mars. A többi Föld-típusú bolygó, vagyis a Merkúr és a Vénusz alkalmatlan arra, hogy az azokon uralkodó szélsőséges időjárási körülmények miatt oda emberek utazzanak. A Merkúr túl közel van a Naphoz, felületén a hőmérséklet a Nap felőli oldalon eléri, sőt meghaladhatja a 150 °C-t, míg az ellentétes oldalon az uralkodó hőmérséklet −150 °C alatt van. A Vénusz felülete maga a pokol, a közel 100 bar nyomásával és a 350-400 °C-os hőmérsékletével. A külső, vagyis az óriásbolygóknak — lévén gázbolygók — nincs szilárd kérgük, amelyre le lehetne szállni. Az óriásbolygók holdjaira való utazás,

célállomásként, egyelőre — ugyancsak a rajtuk uralkodó eléggé mostoha körülmények miatt — az ember úti céljai között még nem szerepelhet, bár a távolabbi jövőben, feltehetően, az ilyen úti célt sem lehet kizárni, de erre ma még nincsenek meg a szükséges feltételek.[1]

A Nap hatásszférájában való mozgások számvetései annyiban különböznek a korábban tárgyaltaktól, hogy az alkalmazott képletekben, a számítások során nem a Földre vonatkozó adatokkal kell számolni, hanem a Nap gravitációs mutatójának értékét, valamint a Naptól való távolságértékeket kell a képletekben alkalmazni. A nap gravitációs mutatójának meghatározása ugyanúgy történik, mint a Föld esetében, vagyis ezen értéket a gravitációs állandó (6,674 · 10-11 N), valamint a Nap tömegének (1,99 · 1030 kg) értékeit kell szorozni. A felhasznált irodalmakban fellelhető adatok szerint, ennek az értéke KN = 1,32718 · 1011 km3/s2-nek vehető.[3]

A bolygóközi térségben való repülés során megkülönböztetjük a már korábban említett heliocentrikus, távolodási és indulási sebességértékeket.

Heliocentrikusnak nevezzük azt a sebességértéket, amelyet a Nap hatásszférájában létre kell hozni ahhoz, hogy az űrobjektum a kitűzött célbolygó felé elinduljon, s annak pályamagasságára emelkedjen, vagy süllyedjen. Ez a sebességérték két tényezőből tevődik össze. Az egyik tényező az indulási bolygó Nap körüli közepes pályasebessége, vagyis az a sebesség, amelynek értéke a Föld pályasebességével együtt egyenlő a Napra vonatkoztatott második kozmikus sebességnek a Föld pályája menti sebességértékével. Az természetes, hogy a Földdel együtt a hatásszféra is halad, tehát a távolodási sebességet a hatásszféra határától való távolodási sebességként kell értelmezni. A heliocentrikus, valamint a távolodási sebesség meghatározásához ismerni kell az indulási és az érkezési bolygónak a Naptól való távolságát, amely értékek a képletben RI és RII jelöléssel szerepelnek. Ezen adatok birtokában, egyszerű képlet segítségével megállapíthatjuk a heliocentrikus sebesség értékét, majd abból kivonva a bolygó közepes pályasebességét, a távolodási sebesség értékét is megkapjuk. E képletnél abból indulunk ki, hogy az indulási sebesség eléréséhez szükséges energiamennyiség egyenlő a fenti két sebességérték energiájának megfelelő munkamennyiséggel.

A Marsra való utazáshoz — értelemszerűen — először a Föld hatásszféráját kell elhagyni. Ehhez, vagyis a heliocentrikus sebességértéknek a kiszámítására az alábbi képletet alkalmazzuk:[7]

$$v_{hel.} = v_{FI.} \cdot \sqrt{\frac{2R_{II}}{R_I + R_{II}}} = 29{,}785\,km/s \cdot \sqrt{\frac{2 \cdot 227{,}9\,km}{149{,}6 + 227{,}9\,km}} =$$

$$= 29{,}785\,km/s \cdot \sqrt{\frac{455{,}8\,km}{377{,}5\,km}} = 29{,}785\,km/s \cdot \sqrt{1{,}207} = \qquad (1)$$

$$= 29{,}785\,km/s \cdot 1{,}098 = 32{,}704\,km/s.$$

A képletben: v_{FI} — a Földnek a Nap körüli közepes pályasebessége (29,785 *km/s*);
R_I — az indulási bolygó távolsága a Naptól (149,6 x 10^6 *km*);
R_{II} — az érkezési bolygó távolsága a Naptól (227,9 x 10^6 *km*)

A számításnál egyszerűsítettünk, ezért a fenti, a zárójelekben lévő számértékekkel számoltunk.

Az indulási sebesség meghatározásához tehát két energiamennyiség ismeretére van szükség, amelyeket a hatásszféra elhagyásakor szükséges figyelembe venni. Elsőként szükség van a Ciolkovszkij által meghatározott második kozmikus sebességre, valamint a távolodási sebesség értékére. E két sebesség energiaigénye adja az indulási sebesség energiaigényét, amelyet ezen értékeknek a négyzetgyök alatti négyzetre emelésével, majd összeadásával és az

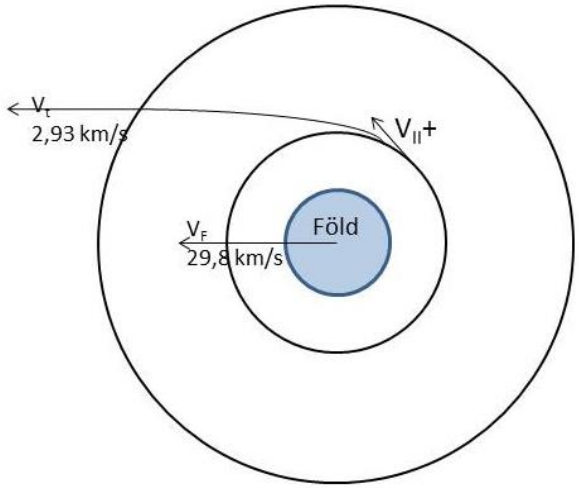
összegnek a négyzetgyök alóli kihozásával kapjuk meg. Ehhez, az alkalmazott képlet, az energia-megmaradás elvét leíró képletből származtatható, amely:

$$\frac{1}{2}mv_i^{\,2} = \frac{1}{2}mv_p^{\,2} + \frac{1}{2}mv_t^{\,2} \qquad (2)\ [7]$$

Ebből, az indulási sebességet (v_i) meghatározó képlet:

$$v_i = \sqrt{v_p^{\,2} + v_t^{\,2}}. \qquad (3)\ [7]$$

A fenti képlethez szükséges sebességértékek számításait részleteiben is megismertetjük. E sebességértékeknek a magyarázata az 1. ábrán látható:



1. ábra. A heliocentrikus, távolodási és indulási sebesség lényege
(*Dr. Ványa László grafikája)*

A bolygóközi térben a mozgás ugyanúgy történik, mint a Föld vonzáskörzetében, csak a Naprendszerben mozgó testekre most már a Nap gyakorol hatást, s a Föld, az űrhajó további útját még egy ideig, csak minimális mértékben befolyásolja, vagyis minimálisan téríti el a Nap vonzereje által kényszerített iránytól, esetleg minimális mértékben csökkentheti a sebességét. A távolodási sebesség jelenléte itt azt jelenti, hogy mint korábban a Föld körüli manővert követően, a körpálya-sebességnél nagyobb sebesség esetén az űrobjektum távolodik a Naptól, a sebességcsökkenés esetén közeledik hozzá. Annak megállapítására, hogy mennyivel nagyobb sebességre van szükség, mint a körpályasebesség, az (1) összefüggés használható. A kisebb sebességet ugyanezzel a képlettel számíthatjuk ki. Ebben az esetben az indulási bolygó sebességénél kisebb lesz az űrobjektum sebessége. Ehhez az alapot az adja, hogy amikor a külső bolygóról jövünk vissza a Földre, akkor megváltoznak a szerepek, a Föld lesz az RII és megváltoznak a négyzetgyök alatti számértékek is. Erre később visszatérünk, és látni fogjuk a változásokat.

A Nap körüli, vagyis a heliocentrikus pályasebesség — ha a Mars az úti cél — tehát 32,7 km/s kell, hogy legyen, mert az így létrehozott 2,915 km/s távolodási sebesség hozhatja létre az űrobjektumnak a Mars pályájára való felemeléséhez elegendő centrifugális erőt. A továbbiakban, a Föld hatásszférájától való távolodási sebességet tehát úgy határozzuk meg, hogy a heliocentrikus sebességből kivonjuk a Föld közepes pályasebességét.

$$V_{táv.} = V_{helioc.} - V_F = 32{,}7 km/s - 29{,}785 km/s = 2{,}915 km/s. \quad (4)\ [7]$$

Miután kiszámítottuk a távolodási sebesség értékét, amely jelen esetben 2,915 km/s, az indítási sebesség meghatározására már korábban megismert és használt képletet használjuk, amelyhez szükség van az adott magasságra érvényes, a Föld felszíne fölött, 200 km magasságra vonatkozó második kozmikus, valamint a már kiszámított távolodási sebességértékekre. Jelen esetben a Föld 200 km-re vonatkozó második kozmikus sebesség vII = 11,015 km/s, a távolodási sebesség pedig vt = 2,915 km/s. Ekkor, ha az indulási sebesség a tengerszint fölötti 200 km magasságról történik:

$$V_{ind.} = \sqrt{V_p{}^2 + V_t^2} = \sqrt{11{,}015^2 + 2{,}915^2} = \sqrt{121{,}33\, km^2/s^2 + 8{,}497 km^2/s^2} = \\ = \sqrt{129{,}827\, km^2/s^2} = 11{,}394\, km/s. \quad (5)\ [7]$$

Ha a Földről kívánjuk az űrobjektumot egy belső bolygóra, pl. a Vénuszra eljuttatni, akkor ugyancsak a Föld haladási irányával ellentétes irányba kell a hatásszférából kijuttatni, s ott kell a szükséges távolodási sebességet létrehozni. A már ismert (1) képlet alapján megkapjuk, hogy az indulási, vagyis a távolodási sebesség, pl. a Földről a Vénusz bolygóra való repülés esetén az alábbi lesz:

$$v_{hel.} = v_F\ km/s \cdot \sqrt{\frac{2 \cdot R_{II}\ km}{(R_I + R_{II})\ km}} = 29{,}785\, km/s \cdot \sqrt{\frac{2 \cdot 108{,}21\, km}{(149{,}6 + 108{,}21)\ km}} = \\ = 29{,}785\, km/s \cdot \sqrt{0{,}839} = 29{,}785\, km/s \cdot 0{,}916 = 27{,}283\, km/s. \quad (6)\ [7]$$

Mivel ebben az esetben egy belső bolygó a cél, a heliocentrikus sebesség értéke kisebb, mint a Föld közepes pályasebessége (29,785 km/s), vagyis 27,283 km/s lesz. Ha a heliocentrikus sebességből kivonjuk a Föld közepes pályasebességét, megkapjuk a távolodási sebességet, amely tehát vt = 27,283 – 29,785 = –2,502 km/s. Ez persze nem lesz negatív érték, csak ebben az esetben ez azt jelenti, hogy a heliocentrikus sebesség értéke 2,502 km/s értékkel kisebb lesz, mint a Földé. Ebben az esetben tehát megteremtjük azokat a feltételeket, amelyekkel az űrobjektum elindul a Vénusz pályája felé, s oda — a Nap vonzása következtében — egyre gyorsulva érkezik.

Ha meghatározzuk az űrobjektumok sebességét, azt tapasztaljuk, hogy a külső bolygó pályája elérésekor jelentősen kisebb, a belső bolygó pályájának elérésekor pedig nagyobb lesz a sebesség, mint az érintett bolygóé. Ezt a sebességvesztést és a sebességnövekedést is a Nap vonzereje okozza, amely ezen a távolságon még jelentős értéket képvisel.

Ha a Marsról visszatérő űrobjektum indulási sebességét vizsgáljuk az (1) képlettel, akkor a következőeredményre jutunk:

$$v_{érk.} = v_b\ km/s \sqrt{2 - \frac{2 \cdot R_{II}}{R_I + R_{II}}} = 24{,}13\, km/s \sqrt{2 - \frac{2 \cdot 149{,}6\, km}{149{,}6 + 228\, km}} = \\ = 24{,}13\, km/s \sqrt{2 - \frac{299{,}6\, km/s}{228 + 149{,}6\, km/s}} = 24{,}13\, km/s \cdot \sqrt{0{,}793} = \\ 24{,}13 km/s \cdot\ 0{,}89 = 21{,}476\, km/s \quad (7)\ [7]$$

A fenti képletben: RI — az indulási bolygó távolsága a Naptól, RII — a célbolygónak a sugárirányú távolsága a Naptól. A négyzetgyök előtti vb a célbolygó közepes pályasebessége. Ha kiszámítjuk, hogy az indulási sebességről mekkora a sebességnövekedés, megállapíthatjuk, hogy az bizony jelentős, és meghaladja a 16 km/s sebességértéket

Ha ugyanezen képlet segítségével kiszámoljuk a Vénusz felé indított űrobjektum érkezési sebességét, jelentős sebességnövekedést tapasztalunk. Ennek is a Nap vonzereje az okozója, csak most ellenkező előjellel. Az alábbi képlettel tehát meghatározhatjuk az belső bolygóra, vagyis a Vénuszra való érkezési sebességet:

$$v_{érk.} = v_b \cdot \sqrt{2 - \frac{R_{II}}{R_I + R_{II}}} == 35{,}05\,km/s\sqrt{2 - \frac{2 \cdot 108{,}21\,km}{149{,}6 + 108{,}21\,km}} =$$

$$35{,}05\,km/s \cdot \sqrt{2 - 0{,}839} == 35{,}05\,km/s\sqrt{1{,}161} = 35{,}05\,km/s \cdot 1{,}077 = \qquad (8)\ [7]$$

$$= 37{,}749\,km/s.$$

A Vénuszhoz való érkezési sebesség tehát vérk. = 37,749 km/s, vagyis nagyobb lesz, mint az érkezési bolygó közepes pályasebessége. Ez minden esetben így van, vagyis — amennyiben a repülés az ún. Hohmann-ellipszisen történik, — a Nap vonzerejének köszönhetően — a külső pálya esetében kisebb, a belső pálya esetében pedig nagyobb lesz az érkezési sebesség, mint a célbolygóé, mivel a Naptól való távolodás során vonzerejének köszönhetően fékezi, közeledés esetén pedig ugyanezen erőnek köszönhetően növeli az űrobjektum sebességét.

A fenti példák is igazolják, hogy a Hohman-ellipszisen való repülési pálya nem mindig teremti meg a célbolygóhoz való érkezés kedvező körülményeit, ezért a célbolygó megközelítésre gyakran használnak olyan pályákat, amelyek a Hohmann-ellipszis és a parabolasebesség pályái közé esnek. Ezt főleg a külső pályák felé indulásnál célszerű alkalmazni, s ez azt jelenti, hogy a távolodási sebesség értéke nagyobb a korábban tárgyaltnál (2,92 km/s). Ilyen esetben célszerű az érkezési sebességet úgy megválasztani, hogy pl, a megközelítési sebesség a célbolygó hatásszférájának a határán néhányszáz m/s legyen (pl. 24,3 km/s). Ebben az esetben, az adott bolygó hatásszférájába való belépés után a bolygó vonzóereje gyorsítja fel az űrhajó sebességét, amely így a bolygó közelében eléri a vbe + vII sebességet, majd bizonyos fékezéssel megfelelő pályára állíthatják és megteremthetik a leszállás feltételeit. Ilyenkor fontos ügyelni arra, hogy a találkozási sebesség ne legyen túlságosan nagy, mert akkor hosszabb ideig kell a fékezőhajtóművet működtetni, ami — különösen az olyan bolygók esetében, amelynek nincs légköre — sok hajtóanyagot igényel, s a visszatérésre esetleg nem jut elegendő belőle. Ez tehát veszélyeztetheti a visszatérés lehetőségét. Mint lehetőség, lehetséges olyan megoldás is, hogy a célbolygó körüli pályán, visszaindulás előtt megteremtik a tankoláshoz szükséges feltételeket, s a visszaindulási bolygó körüli pályán veszik fel a visszatérés során szükségessé váló hajtóanyag-mennyiséget, s így biztosítják a visszatéréshez szükséges manőverek hajtóanyag-igényét.

A megközelítési sebesség értéke tehát nagyon fontos mutató. Esetenként a legkedvezőbb érkezési sebesség értékének megválasztása azért is célszerű lehet, mert a bolygók egymáshoz viszonyított helyzete túl sok várakozási időt tenne szükségessé a visszatéréshez. Ezért van az, hogy pl. a Marsra utazás és a visszautazás esetén a legkisebb energiát igénylő útvonalon az odautazáshoz 11,567 km/s indulási sebesség szükséges, és ebben az esetben a Marsig az utazás mintegy 580 millió km, s ennek megtételéhez 255 napra, vagyis 8,3 hónapra van szükség. Ha az indulási sebességet 11,8 km/s sebességértékre növeljük, akkor az utazás mindössze 165 napig tart, vagyis három hónappal előbb érjük el a célunkat. Ha az indulási sebesség 12 km/s, akkor még további 21 napot nyerünk. Figyelembe kell azonban venni, hogy az indulási sebesség növelésével megnöveljük az érkezési sebességet is, és szükség lehet a sebességcsökkentésre. Ehhez pedig hajtóanyagra van szükség, ami nem mindig áll rendelkezésre. A bolygókra

való repülés során tehát figyelembe kell venni, hogy a visszatéréshez is jelentős mennyiségű hajtóanyagra van szükség, tehát a fékezésre nem mindig jut hajtóanyag. Ezért célszerű a legkedvezőbb érkezési sebességet kiválasztani, és ahhoz szabni meg a hajtóanyag-szükségletet.

Meg kell állapítani, hogy a jövő, és az itt említett probléma megoldása olyan rakétahajtóművekben keresendő, amelyeknek a jelenleginél nagyobb a gázkiáramlási sebessége. Ebben az esetben ugyanakkora a sebesség elérése feleannyi hajtóanyagot igényel, ezért ebben az esetben a fékezésekre is juthat kellő mennyiségű hajtóanyag. Ha a hajtóműből kiáramló gáz sebességét a duplájára lehetne növelni, a hajtóanyagigény ugyanazon feladat esetén — értelemszerűen — a felére csökkenne. A megoldás tehát a rakétahajtómű fejlesztése, ami egyáltalán nem könnyű feladat. Jelenleg az űrnagyhatalmak dolgoznak e probléma megoldásán, de a konkrét eredmények ma még váratnak magukra.

A továbbiakban egy képzeletbeli utazás résztvevői lehetünk, amellyel még csak képzeletben, de már a Marsra utazunk. Az utazáshoz szükséges repülési sebességek meghatározásával kiszámolhatjuk, hogy mennyi az összes sebesség értéke, amellyel a rakétakomplexum kell, hogy rendelkezzen a Marsra utazás és a visszatérés során. Ezt az értéket jellemző sebességnek nevezzük (vj), és ebben az esetben, ha a vállalkozásra pl. Bajkonurból indulunk, az utazás az alábbi összetevőkből áll:

Indulási sebesség 200 *km* magasságról:	11,59 *km/s;*
A Föld forgási sebessége:	- 0,33 *km/s;*
Start utáni helyesbítés:	0,05 *km/s;*
Helyesbítés az út felénél:	0,4 *km/s;*
Helyesbítés a Marshoz érés előtt:	0,2 *km/s;*
Indulási sebesség a Marstól a Föld felé:	3,52 *km/s;*
A Mars forgási sebessége:	- 0,15 *km/s;*
Helyesbítések start után és félúton:	0,5 *km/s;*
Helyesbítések és fékezés a Föld körül:	3,2 *km/s.*
Összesen az oda-vissza utazáshoz:	**19,46 *km/s***

Amint látjuk, a hajtóanyag mennyiségét számolva, a legtöbb, a Földtől való távozáskor és a visszatérésnél a Föld körüli manőverek igénylik. Ezekre a tevékenységekre a teljes sebességhez viszonyítva, a hajtóanyag mintegy 75%-át használják fel. A fenti sebességadatokhoz még hozzá kell adni a Marsra való leszállás és felszálláshoz szükséges sebességmennyiséget a megfelelő rakétahajtómű-fogyasztási adataival számolva. Ennek a mennyisége a teljes igényhez viszonyítva nem számottevő.

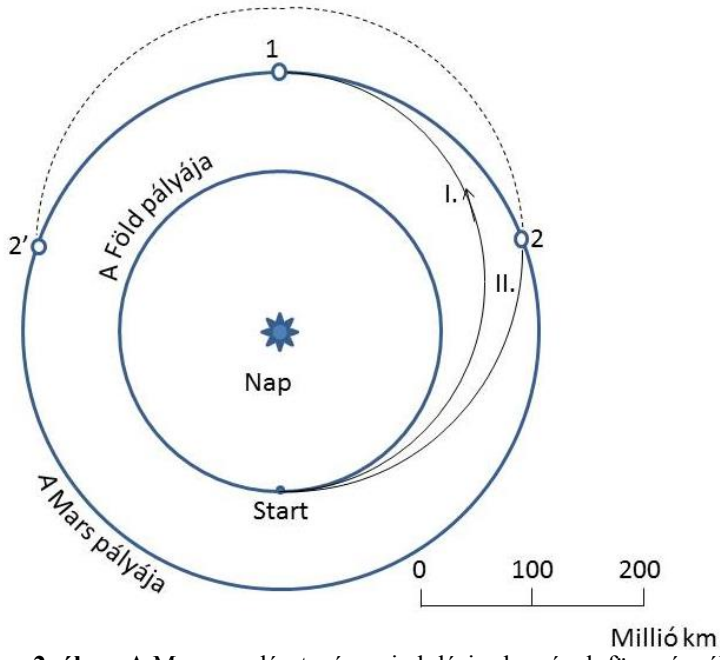
A Marsra és vissza, a Földre tervezett utazáshoz tehát olyan rakétára van szükség, amely összességében 19,46 km/s sebesség létrehozására képes. Egy korábbi képlet segítségével meghatározhatjuk annak a négylépcsős rakétának a z értékeit és összeadva azokat a z$\sum$ értékét, amelynek birtokában a rakétakomplexum e feladat végrehajtására képes. Meg kell itt jegyezni, hogy a z értékének maximuma nem lehet több 10-nél. Ez a képlet, amelyet Ciolkovszkij alkotott, jelen esetben az alábbi:

$$z_{szüks} = e^{\frac{v}{w \cdot n}} = 2{,}71828^{\frac{19{,}46}{3.4 \cdot 3}} = 2{,}71828^{1{,}907} = 6{,}733 \qquad (9)\ [7]$$

A fenti számítás előzetes, ellenőrző jellegű, de azt már megmutatja, hogy a rakéta három fokozata elegendő a kívánt sebességérték biztosításához. A továbbiakban természetesen részletes számításokat kell végezni rakétalépcsőnként, s ez a számítás adja meg a végső eredményt. Még figyelembe kell venni azt is, hogy a rakétakomplexum starttömege nem ismert, hiszen az majd az addig továbbfejlesztett rakétahajtóművek lehetőségeitől függ. Ha a rakéta

starttömege pl. 3500 t, a Szerző általi egyfajta elképzelés szerint felosztva a három lépcső között a starttömeget, megkapjuk, hogy a $z\sum = 9{,}4$ körüli értéket ad. Ez azt jelenti, hogyha a starttömeget osztom 9,4 értékkel, a szerkezeti elemekre és a hasznos teherre jutó része mintegy 372 t lehet. A számítások szerint ebben az esetben, a hasznos teher tömege kb. 50 t lehetne, s akkor az adott komplexum adatai megegyeznének a Saturn V adataival. Ez megközelítően megfelel annak az aránynak, amellyel az Apolló programban alkalmazott Saturn V rakétakomplexum rendelkezett (2800 t starttömegből mintegy 256 t jutott a szerkezeti elemek és a hasznos teher tömegére, vagyis a hasznos teher mutatója mindkét esetben 0,091 lenne. A kismértékű eltérés onnan van, hogy a Saturn V esetében a $z\Sigma = 9{,}2$ körüli értéket képviselt).

Van még egy sajátossága a Marsra, valamint más bolygókra való utazásnak, ez pedig az indulás időpontja. A bolygók ugyanis egymáshoz viszonyítva állandóan változtatják helyüket, mégpedig mindegyik más és más sugarú pályán, különböző sebességgel halad. Ennek következtében pl. a Marsra utazás sem kezdhető meg bármikor. Ha a bolygók pillanatnyi állása és várható mozgásuk alapján indulhat a személyzet, akkor a következő indulásra kb. 2 év és 2 hónap múlva kerülhet ismét sor, mert a két bolygó egymáshoz viszonyított helyzete az utazást ennyi időnként teszi lehetővé. Ugyanakkor, a mai lehetőségeink mellett, a Marsra és visszautazás időtartamigénye 32 hónap. Ennek a magyarázata egyszerű. A mai lehetőségeink szerint, a Marsra utazás ideje kb. 8 hónap. Ez az út oda-vissza, mintegy 16 hónapot vesz igénybe. Ugyanakkor, a két bolygó egymáshoz viszonyított helyzete nem teszi lehetővé, hogy pl. egyhónapos ott-tartózkodás után visszainduljanak az űrhajósok, mert a nyolchónapos utazás után a Föld nem lenne ott, ahová az űrhajósok érkeznének. Ennek pedig így semmi értelme nem lenne. A két bolygó állásából kiindulva tehát ez a kölcsönös helyzet 16 hónapos ott-tartózkodás utáni indulás esetén jönne létre, vagyis az űrhajósoknak a Marson kellene várni kb. 16 hónapot. Felvetődik a kérdés: megvannak ennek a feltételei? Nyilván nincsenek, tehát az ott-tartózkodás feltételeit meg kell teremteni. Tehát, bármilyen problémát is okoz ez a helyzet, nincs választási lehetőség. Amíg a jelenlegi eszközeinkkel számolhatunk, addig a helyzet ez marad, s a 32 hónap csak kismértékben csökkenthető.[1, 3, 7]



2. ábra. A Marsra való utazás az indulási sebességek függvényében
(*Dr. Ványa László grafikája)*

Visszatérés a Marsról

A Marsról való visszatérésnél a manőverek felépítése hasonló, mint amikor a Földről a Vénusz pályájára küldjük a szondát. A Mars körüli pályáról az indulás és a hatásszféra elhagyása a bolygó haladási irányával ellentétes irányba történik, hiszen a Föld most belső bolygó, tehát a Mars pályasebességénél kisebb sebességgel kell indulni, hogy a Nap vonzereje bejutasson bennünket a Föld pályájára. Ugyanakkor természetesen az aktuális sebességértékeket — a heliocentrikus, távolodási és indítási sebességekről van szó — a Marsra vonatkozó adatok segítségével kell kiszámítani.

Adatok a Marsról

A Mars keringési ideje a Nap körül – 1 év és 321,73 földi nap, mintegy 1,88 év, vagyis 779,94 nap. A Föld 2 év és 50 naponként éri utol a Mars bolygót. Ilyenkor van egy bizonyos ablak, vagyis időtartam, amikor a legcélszerűbb űrobjektumot küldeni a vörös bolygóra. Ezt vették figyelembe pl. annak idején, a Mars-szondák indításánál, amikor a Mars-2 és 3-as űrszondákat 1971. május 19-én és 28-án indították majd ezután a következő sorozat, vagyis a Mars-4, 5, 6 és 7 indítására 1973. július 21-én, 25-én, augusztus 5-én és 9-én került sor. Az 1971-es sorozat utolsó indítása és az 1973-as sorozat első indítása között mintegy 25 hónap telt el.

A Marsnak a Naptól való közepes távolsága 227,9 millió km (1,5237 CsE), excentricitása jelentős (0,0934, amely jóval nagyobb a Földénél – az csupán 0,0167); napközeli távolsága 207 millió km, naptávoli pedig 249 milló km. Az elsőben a sebessége 25,32 km/s, az utóbbiban pedig 23,086 km/s. Ezek alapján a Mars közepes pályasebessége – 24,131 km/s.

A Mars forgástengelye és a Naprendszer egyenlítője között bezárt szög — 24°48', vagyis alig tér el a Földétől. Pályasíkja a Földétől csak 1°81'-cel tér el. A Mars gravitációs mutatója KM = 42 840 km3/s2, közepes átmérője – 6792 km, sugara – 3396 km. A nehézségi gyorsulás értéke a felszínen – gM = 0,38gF, vagyis a = 3,73 m/s2. Az első kozmikus sebesség a felszínen: vI = 3,552 km/s, vII = 5,033 km/s. A Mars felszínén tehát, a második kozmikus sebesség értékét ugyanazzal a képlettel számíthatjuk ki, mint amilyet a Föld esetében is alkalmaztunk, csupán a Marsra vonatkozó adatokkal, s ez az alábbi lesz:

$$v_{II} = \sqrt{2 g_0 R_0} = \sqrt{2 \cdot 3{,}73\,(m/s^2) \cdot 3\,396\,000\,m} = \\ = \sqrt{25334160\,m^2/s^2} = 5033\,m/s. \qquad (10)\ [7]$$

Ezután kiszámoljuk a távolodási sebességet, amely a heliocentrikus érkezési sebesség és a Mars közepes pályasebessége közötti különbség:

$$v_{táv} = 21{,}448 km/s - 24{,}126 km/s = -2{,}678 km/s. \qquad (11)\ [7]$$

Ahhoz tehát, hogy a visszainduló űrhajó a Mars pályájáról bejusson a Föld pályamagasságára, a Mars pályasebességénél 2,678 km/s-mal kisebb sebességértékre van szükség. Végül, a kapott eredmények alapján meghatározzuk az indítási sebesség értékét, ha az anyaűrhajó 200 km magasságról indul. Ebben az esetben az adott magasságon a második kozmikus sebesség értéke 4,486 km/s, a távolodási sebesség pedig 2,655 km/s, így tehát:

$$v_{ind} = \sqrt{(4{,}886\,km/s)^2 + (2{,}678\,km/s)^2} = \\ = \sqrt{23{,}873\,(km/s)^2 + 7{,}172\,(km/s)^2} = \sqrt{31{,}045} = 5{,}572\,km/s. \qquad (12)\ [7]$$

Ebben az esetben tehát 5,572 km/s – 3,455 km/s = 2,117 km/s gyorsítást kell végezni, s ekkor az indulási sebesség 5,572 km/s lesz, amely biztosítja a Mars hatásszférájának a határán a szükséges távolodási sebesség létrehozását, mégpedig a bolygó haladási irányával ellentétes irányban.

Felvetődik a következő kérdés: mennyi lesz a visszatérő űrobjektum sebessége, amikor visszaér a Föld hatásszférájának a határára? Azt már tudjuk, hogy a Marshoz, annak pályasebességénél kisebb sebességgel érkezik az űrobjektum. Most azonban, mivel az űrparadoxonnak megfelelően lassítottunk, tehát az űrobjektumunk gyorsulni fog, vagyis a sebesség fokozatosan növekszik. A Föld pályájának elérésekor a sebesség értékét az alábbi képlet segítségével határozhatjuk meg:

$$v_{helioc} = v_F \cdot \sqrt{2 - \frac{2R_{II}}{R_I + R_{II}}} = 29{,}8\ km/s \cdot \sqrt{2 - \frac{2 \cdot 149{,}6\ km}{228 + 149{,}6\ km}} =$$

$$= 29{,}8\ km/s \cdot \sqrt{\frac{299{,}2}{377{,}6}} = 29{,}8\ km/s \cdot \sqrt{2 - 0{,}792} = 29{,}8\ km/s \cdot \quad (13)\ [7]$$

$$\cdot \sqrt{1{,}208} = 29{,}8\ km/s \cdot 1{,}099 = 32{,}750\ km/s.$$

A Marsról indított űrhajó tehát a Föld pályamagasságára érkezéskor eléri a 32,750 km/s sebességértéket. Ez az érkezési sebesség csaknem 3 km-rel haladja meg a Föld pályasebességét. Azt is megállapíthatjuk, hogy a visszatérő űrhajó érkezési sebessége közel annyi lesz, amennyi az indulásnál a Föld hatásszférájának a határán volt (32,7 km/s). Ez azt jelenti, hogy az űrhajó sebessége nagyobb a bolygó (Föld) sebességénél, mégpedig 2,93 km/s értékkel. Ha ezzel a sebességgel érkeznénk a Föld hatásszférájának a határára, és nem tennénk semmilyen intézkedést, vagyis ott nem fékeznénk, akkor a hatásszféra határától a Föld körüli legkisebb magasságig a repülési sebesség törvényszerűen tovább növekedne, s a földközeli pontban elérné a vbe. + vII értéket, amely 300 km magasságban akár a 13,862 km/s értéket is elérheti. Ez a sebességérték az adott magasságon jóval több, mint a második kozmikus sebesség. Az ilyen sebességgel haladó űrobjektum elhagyná a Föld hatásszféráját a korábbi 2,9 km/s sebesség helyett mintegy 3,857 km/s sebességgel, s ezzel a Mars pályáján túli pályamagasságra emelkedne, majd visszatérne a Föld hatásszférájába, de még nagyobb érkezési sebességgel. Ezért van szükség ilyen esetekben arra, hogy a sebességcsökkentés érdekében mind a hajtóműves, mind pedig az aerodinamika fékezést alkalmazzuk.

Ha azt akarjuk elérni, hogy a belépési sebesség, valamint esetünkben a Föld második kozmikus sebesség együttes értéke ne legyen túl nagy, akkor már a hatásszféra határának átlépése után célszerű a sebességet hajtóműves fékezéssel csökkenteni, amikor annak sebessége még csak 2,95 km/s, és a mozgásenergiája még nem túl nagy. Az ideális helyzet az lenne, ha a belépéskor néhány tíz, esetleg 100 m/s lenne a sebességnövekedés, de hát ez adott esetben nem lehetséges, így tehát a továbbiakban mindkét sebességcsökkentés módszerét feltétlenül alkalmazni kell.

Az űrobjektumra egyébként ebben a helyzetben úgy is tekinthetünk, mint amikor az hintamanővert hajt végre, amely, mint tudjuk, felgyorsítja az érkezési heliocentrikus sebességértéket.[3] Ezért jobb megoldás, ha utolérés esetén a belépési sebesség csak kismértékben haladja meg a célbolygó pályasebességét, s az irányítás során olyan földközeli magasságra vezérlik, amelyen az aerodinamikai fékezés hatására a sebesség lecsökken, az űrobjektum elnyújtott ellipszis pályára áll, majd kétszer-háromszor megismételve az aerodinamikai fékezést, a hajtómű működtetésével, fékezéssel állítják olyan pályára, amelyről a leszállási manővereket már

meg lehet kezdeni. Ezt a módszert, az amerikaiak és a szovjetek is kipróbálták a Hold-verseny során, s megtalálták a megfelelő megoldást, amely segítségével néhány kör megtétele után, megfelelő mértékben tudták csökkenteni az ellipszispálya földtávoli pontjának a magasságát, és így biztosítani tudták a szükséges sebességcsökkentést.

Vizsgáljuk meg most azt, hogy mennyi sebességet kellene fékezni abban az esetben, ha az összes sebességfölösleget rakétás fékezési módszerrel kellene elvégezni. Maximális igény esetén ez az érték 2,9 + 3 km/s, vagyis mintegy 5,9 km/s is lehet. Ez jelentős energiát igényelne, vagyis a visszaérkezéskor jelentős mennyiségű tartalék hajtóanyag-mennyiséggel kellene számolni. Ez nem lenne egyszerű feladat, hiszen a tartalék hajtóanyag-mennyiséget az űrhajónak magával kellene vinni a Marsra is. Elég nagy tömegről van szó még a visszaérkezéskor is (50-60 t), amelynek a lefékezéséhez ugyanennyi tolóerő esetén is mintegy 350 s hajtómű-működésre lenne szükség. Ez, tekintettel az indulási tömeg jelentős mértékű növekedésére, esetleg megoldhatatlan feladat lehet. Marad tehát a fentiekben vázolt kombinált fékezési módszer alkalmazása, amikor jóval kevesebb hajtóanyag-felhasználással állítható a visszatérő űrhajó Föld körüli pályára, és a továbbiakban, a Földre való leszállási manőverekhez biztosítható a szükséges hajtóanyag-mennyiség. E probléma természetesen nem jelentkezik, ha a Mars körüli tankolás lehetőségét megteremtik.

Következtetésként megállapíthatjuk, hogy az idegen bolygóról, de egyáltalán, nagyobb távolságról való visszatérés esetén, bonyolult feladatok egész sorát kell megoldani ahhoz, hogy a leszállás feltételeit megteremthessük. Így pl:

- a hatásszféra határán való belépés után a sebességet le kell csökkenteni;
- be kell vezetni az űrobjektumot s Föld légkörébe, olyan magasságon, ahol hatásos a fékezés, de a keletkező hő az űrhajót, és az űrhajósok életét még nem veszélyezteti;
- az aerodinamikai fékezés három-négyszeri megismétlésével, közelíteni kell ahhoz a pályához, amelyről a visszatérési manővert meg lehet kezdeni.

E manőverek mindegyikének a végrehajtása nagy pontosságot igényel, amit ma már az automatikus vezérlés útján képesek pontosan megvalósítani. A központi, de a fedélzeti számítógép is folyamatosan számolja a szükséges adatokat, s a számítógépek megadják a szükséges manőverek helyeit és végrehajtásaik időpontjait. Ezzel a számítógépek jelentős mértékben segítheti a visszatérési manőverek biztonságos és pontos végrehajtását.

A NAPRENDSZER ELHAGYÁSÁNAK PROBLÉMÁJA [12]

A Naprendszer felépítése

A csillagok keletkezésével kapcsolatban, nemrég még több elmélet is létezett. Egyik ilyen elmélet szerint a régmúltban, mintegy 5-6 milliárd évvel ezelőtt talán felrobbant e tájon egy óriáscsillag, annak szétszórt anyagából jött létre többek között a Nap és a szomszéd csillagok, továbbá a Föld is. Évmilliók alatt kialakult tehát a ma már csak Földnek nevezett bolygó, amelyet elhelyezkedése, vagyis a Naptól való távolsága és sok más tényező alkalmassá tett arra, hogy rajta az élet kialakuljon. Van olyan elmélet is, hogy az élet megjelenése, a kozmoszban bárhol lehetséges. De talán most nem is ez a lényeg. Adott egy helyzet, itt van a Föld és kutatjuk, mikor és hogyan jött létre. Sőt, mi éppen most azt kutatjuk, hogyan lehet eljutni egyik csillagtól a másikig. Mekkora ez a távolság, mekkora sebesség szükséges ahhoz, hogy az elképesztően nagy távolságot áthidaljuk, és mennyi idő kell ahhoz, hogy a szomszédunkat elérjük?

Az élet kialakulását követően, eljutottunk abba a stádiumba, amikor megjelent a gondolkodó ember, s hosszú fejlődési folyamat eredményeként eljutott a mai állapotába, amikor már

képes lépésről lépésre tudásával, de már űreszközeivel is a környező világunk titkait felderíteni, s a megismerés folyamataiban jelentős eredményeket elérni. Ahogy Oriana Fallaci írja könyvében, amikor apjával vitatkozik, aki nem akar a Holdra menni, mert ott nincsenek virágok és nincsenek halak. A vitában az írónő többek között így érvel: *„...Az ember a vonaton felfedezte, hogy gyorsan és messzire tud menni, repülni tud, mint a madarak, megirigyelte a madarakat, ellopta a szárnyukat, ráillesztette a vonatra és repült. Magasabbra, egyre magasabbra, mígnem megirigyelte a csillagokat, és kezdetleges másolatokat készített róluk, majd azokon repült tovább, hogy belásson az ég zárt kapuja mögé. De hát az isten szerelmére, ha zárt kaput látsz, nem támad fel benned a vágy, hogy kinyisd és megnézd, mi van mögötte, apám? Az ember története vajon nem a zárt és feltárt kapuk története? Felelj apám."[*11]

Az írónőnek igaza van. Az ember, bizonyára génjeiben hordozza a megismerés vágyát, s mindent, ami ismeretlen, meg akar ismerni. Többek között ez a tudásvágy hajtja előre a megismerés útján, és valljuk be, eddig nagyon szép eredményeket ért el. E megismerési folyamatnak köszönhetően, az ember eljutott az űrkorszakba, a világ tovább tágult körülötte. Megismerte a Tejútrendszert, amely a földi méretekhez viszonyítva már szinte elképzelhetetlenül nagy képződmény, s amelyben mintegy 200 milliárd csillag van. Bolygónk, vagyis a Föld, a maga hatásszférájával is óriási, ha földi méretekkel mérjük. Elképzelni is nehéz, hogy a Föld hatásszférája a Nap és a Föld közötti távolság (149,6 millió km) hatvanezerszerese, vagyis közel 9 billió km. Ez már olyan fantasztikusan nagy szám, amelyet már a földi méretekhez szokott embernek elképzelni is nagyon nehéz. Ennek illusztrálására álljon itt egy példa. Tételezzük fel, hogy egy űrobjektumot a harmadik kozmikus sebességgel indítunk (16,6 km/s), s az objektumunk, ezzel a sebességgel 18 000 év múlva jutna el a Nap hatásszférájának a határára. Ez a sebesség ma még a lehetőségeink határa. A tér kitágult, és vele tágult az idő is. Tudomásul kell venni, hogy a mai eszközeinkkel a kitágult teret és időt még nem tudjuk követni. Mai eszközeink segítségével még sok ezer év alatt érhetjük el a Naprendszer dinamikai határát, s ennek is sokszorosa szükségeltetik ahhoz, hogy a szomszéd csillagig eljussunk.

A Naprendszer csak egy parányi része a Tejútrendszernek, amely a maga 100-130 000 fényévnyi átmérőjével ugyancsak parányi része a világmindenségnek. Az ember, ma már eszközei segítségével 12-13 milliárd fényévre is ellát, s ezzel egyelőre ugyan csak nagy vonalakban, de megismerheti, vagy inkább csak bepillantást kaphat az ősrobbanás utáni időszak titkaiba.

De most térjünk vissza a mába, és közvetlen világunk valóságába. Az igazság az, hogy az emberiség még nem készült fel arra, hogy a megismert távolságokat űreszközeivel viszonylag rövid időtartam alatt leküzdje, sajnos ehhez még jelentős fejlődésre lenne szükségünk. De az ember nem adja föl, próbálkozik, s e próbálkozásba nyújtunk lehetőséget, hogy bepillantást nyerjünk e kezdetleges próbálkozások titkaiba.

A Voyager-űrszondák útvonalszámításai

Köztudott, hogy 1977. augusztus 20-án, az Amerikai Egyesült Államok területéről útjára indították a Voyager–2 űrszondát, amelyet 16 nappal később követett a Voyager–1 is. E két szonda azzal a feladattal indult útjára, hogy elhagyva a Föld, majd a Nap hatásszféráját, kilépjen a csillagközi térbe és egy-egy közeli csillag felé vegye az irányt. A szondák fedélzetükön az emberiség üzenetét viszik az esetleges megtalálóknak, küldetésük célja tehát a közeli csillagok elérése, sőt azokon túlra is elmehetnek, s talán valamikor találkozhatnak olyan fejlett civilizációval, amely elolvashatja és meghallgathatja a Voyagerek által szállított üzenetet. Sajnos, ehhez — amint a továbbiakban majd látni fogjuk — sok ezer évre lesz szükség. A mai technológiával elérhető sebesség, még az esetenkénti, a bolygók által biztosított lendítőerők felhasználásával is kevés ahhoz, hogy akár egyetlen emberöltő alatt kijuttathassunk űrobjektumokat a csillagközi térbe.

A két űrszonda más-más sebességgel indult útjára. Az elsőként indított, de a 2-es jelzésű szonda indulási sebessége, a fellelhető adatok szerint, 16,08 km/s volt, és ezzel a sebességgel kezdte meg küldetését. A másodikként indított, de 1-es jelzéssel ellátott űrszonda indítási sebessége már meghaladta a harmadik kozmikus sebességégnek a Föld felszínére érvényes értékét (16,66 km/s), vagyis annak indulási sebessége elérte a 17,48 km/s értéket. Ennek köszönhetően, a Jupiter pályamagasságára már mintegy öt hónapos előnnyel, a Voyager–1 érkezett elsőként, bár az indítása 16 nappal a Voyager–2 után történt. Vizsgáljuk meg a megfelelő képletek alkalmazásával, mikor érkezhetnek ezek az űrszondák a Naprendszer dinamikai határára, amelyet a hatásszféra határának nevezünk, s ez a gravitációs szférahatár a Nap középpontjától 60 000 csillagászati egységre (CSE), vagyis közel kilenc billió, pontosabban meghatározva nyolcbillió-kilencszázhetvenhatmilliárd km-re van. Csak emlékeztetőül megemlítem, hogy egy égitest hatásszférája alatt azt a térrészt értjük, amelyben az adott égitest határozza meg minden abban mozgó kisebb égitest mozgását.

Első lépésként vizsgáljuk meg az indulási sebességből kiindulva — annak tudatában, hogy a Voyager–1-nél ez 17,48 km/s volt — milyen távolodási sebesség hozható létre a 930 000 km-re lévő hatásszféra határán? Ennek képlete a [3] és [4] forrásművekből ismert, és arra szolgál, hogy az erőcentrumtól távolodva, bármilyen r távolságon legyünk képesek meghatározni a távolodási sebességet. Ennek megfelelően, a Voyager–1 kiindulási adatai: v0 = 17,480 km/s; a KF =398 600 km^3/s^2; az r0 = 6371 km (vagyis a Föld közepes sugara); ahol a távolodási sebesség értékét kívánjuk meghatározni, az r = 930 000 km. Ezen adatokkal számolva tehát a Voyager-1 a Föld hatásszférájának a határán az alábbi sebességgel repült:

$$v^2 = {v_0}^2 - \frac{2K_F\ km^3/s^2}{r_0\ km}\left(1-\frac{r_0\ km}{r\ km}\right) = (17{,}480\,km/s)^2 - \frac{2\cdot 398600\,km^3/s^2}{6371\,km}\cdot$$

$$\cdot\left(1-\frac{6371\,km}{930000\,km}\right) = 305\,km^2/s^2 - \frac{797200\,km^3/^{s^2}}{6371\,km}\cdot(125{,}13\,km^2/s^2\cdot 0{,}993) = \qquad (14)$$

$$= 305\,km^2/s^2 - 124{,}254\,km^2/s^2 = 180{,}746\,km^2/s^2;$$

$$v = \sqrt{180{,}746\,km^2/s^2} = 13{,}444\,km/s.$$

A Föld középpontjától 930 000 km-re, a hatásszféra határán a Voyager–1 tehát még 13,444 km/s távolodási sebességgel rendelkezik. Ilyen sebességgel rendelkező űrobjektum heliocentrikus sebessége 13,444 km/s + 29,785 km/s = 43,230 km/s lesz. Ez a sebességérték már több, mint a Föld pályatávolságán a Napra vonatkozóan érvényes második kozmikus sebesség. Mivel a szonda indulása a Föld haladási irányába történt, értelemszerű, hogy a Nap hatásszférájába való beérkezés után, a megnövekedett centrifugális erő hatására intenzíven távolodni fog a Naptól és elindul a Mars, illetve a Jupiter pályája felé. A Jupiter pályamagasságára érkezés sebességét ugyanezzel a képlettel határozhatjuk meg, de a képletben most már nem a Földre, hanem a Napra vonatkozó adatokat szerepeltetjük. Így tehát, a Napra vonatkozó adatok a következők: v0 = 43,230 km/s; az r0 = 149 600 000 km; a KN = 1,32718 · 1011 km3/s2 (a sok nullát elkerülendő, 132718-cal számolhatunk, s akkor az r0 =149,6 km lesz.

A Jupiter hatásszférájába való belépés és kilépés közötti szög θ = 78° lesz, amelyet majd a Jupiter hatásszférájában való gyorsítási sebesség, vagyis a keresett Δv értékének meghatározásakor használunk. Az a távolság, ahol a távolodási sebességet keressük, vagyis a Jupiter pályatávolsága mínusz a hatásszférája határának a távolsága, vagyis az r = 778 – 48 = 730 millió km (ezen értékeket is, mint korábban, hat-hat nulla elhagyásával alkalmazhatjuk). Ekkor tehát:

$$v^2 = v_0{}^2 - \frac{2 \cdot K_N \; km^3/s^2}{r_0 \; km} \cdot \left(1 - \frac{r_0 \; km}{r \; km}\right) = (43{,}230\, km/s)^2 - \frac{2 \cdot 132718 km^3/s^2}{149{,}6\, km} \cdot$$

$$\cdot \left(1 - \frac{149{,}6\, km}{730\, km}\right) = 1868{,}833\, km^2/s^2 - 1774{,}3\, km^2/s^2 \cdot 0{,}795 = 1868{,}833\, km^2/s^2 - \qquad (15)$$

$$-1410{,}568\, km^2/s^2 = 458{,}265\, km^2/s^2; \quad v = \sqrt{458{,}265\, km^2/s^2} = 21{,}407\, km/s.$$

Ezzel meghatároztuk, hogy a Jupiter hatásszférájába való belépés előtt a sebességünk értéke 21,407 km/s értékű lesz. Érdemes itt megjegyezni, hogy mivel itt még eléggé jelentős a Nap vonzereje, a sebességcsökkenés értéke még igen nagy, vagyis eléri a 21,823 km/s értéket. A továbbiakban, a Jupiter hatásszférájába való belépési sebességet megkapjuk, ha kivonjuk az heliocentrikus érkezési sebességből a Jupiter közepes pályasebességét, vagyis vbe = 21,407 – 13,052 = 8,355 km/s. A bolygó általi gyorsítás értékét az alábbi képlet segítségével határozhatjuk meg, s a számítás eredményeként megkapjuk a bolygó segítségével elért gyorsítás értékét, amely tehát:

$$\Delta v = 2 \cdot v_{be} \cdot \sin\theta = 2 \cdot 8{,}355\, km/s \cdot \sin 39° = \\ = 16{,}71\, km/s \cdot 0{,}629 = 10{,}510\, km/s. \qquad (16)$$

Ha a 10,510 km/s értéket hozzáadjuk a heliocentrikus érkezési sebességhez, megkapjuk azt a sebességértéket, amellyel a szonda indul a Jupiter pályamagasságáról a Szaturnusz felé, vagyis vi = 21,407 + 10,510 = 31,917 km/s. A már ismert képlet segítségével meghatározhatjuk a Szaturnusz hatásszférájának a határára érkezés sebességét, vagyis:

$$v^2 = v_0{}^2 - \frac{2K_N}{r_0} \cdot \left(1 - \frac{r_0}{r}\right) = 1018{,}7\; km^2/s^2 - \frac{265436\, km^3/s^2}{778\, km} \cdot$$

$$\cdot \left(1 - \frac{778\, km}{1371 km}\right) == 1018{,}7 - 341{,}2 \cdot 0{,}433 = 1018{,}7\; km^2/s^2 - \qquad (17)$$

$$-147{,}74\, km^2/s^2 == 871 km^2/s^2;$$

$$v_{érk.} = \sqrt{871 km^2/s^2} = 29{,}512\, km/s.$$

31,917 km/s indulási sebesség esetén tehát a Szaturnusz hatásszférájának a határára már 29,512 km/s sebességgel érkezünk. Itt szemléltethetjük plasztikusan, hogy a Naptól való távolodással négyzetesen csökken a Nap vonzereje. Ennek köszönhetően tehát a Föld pályamagasságáról indulva, a Mars hatásszférájáig 580 millió km-t utazott a szonda, és 21,823 km/s sebességértéket vesztett, ami 51% veszteségnek felel meg, addig a Jupiter és a Szaturnusz között 593 millió km-t utazott, tehát 13 millióval többet, s a veszteség mindössze 2,4 km/s, ami már csak 7,5%-os sebességvesztést jelent. Ez konkrétan annak köszönhető, hogy a Naptól való távolság CSE-ben az elsőnél 1-ről 5,2-re növekedett, s a Nap vonzereje 1/27-ére csökkent, míg a második esetben a távolság 9,5-re növekedett, s a Nap vonzerejének a csökkenése már a Föld pályája mentén mértnek csak 1/90-ed része volt.

Megérkeztünk tehát a Szaturnusz hatásszférájának a határára, sebességünk pedig 29,512 km/s. A belépési sebesség tehát az érkezési sebesség mínusz a bolygó közepes pályasebessége, vagyis: vbe = 29,512 – 9,636 = 19,876 km/s-ra növekedett a bolygó által létrehozott gyorsítási sebesség értéke pedig:

$$\Delta v = 2 \cdot 19{,}876\, km/s \cdot \sin 22° = 39{,}752\, km/s \cdot 0{,}375 = 14{,}891\, km/s. \qquad (18)$$

A gyorsítás értéke tehát 14,891 km/s, így a szonda a hatásszféra felé az érkezési heliocentrikus sebesség és a gyorsítási sebesség összegével indul el, amelyek értéke 29,912 km/s + 14,891 km/s = 44,803 km/s. Megfigyelhető volt itt a θ szög hatása a gyorsítás értékére. A Jupiter hatásszférájában ez a szög 78° volt, a gyorsítás értéke pedig elérte a 10,5 km/s értéket. Itt jóval nagyobb volt a belépési sebesség, de a kisebb θ = 44° miatt, bár a belépési sebesség több mint a kétszerese volt az előzőnek, a gyorsítás értéke mégis csak 14,891 km/s volt. A Szaturnusztól tehát a távolodási sebesség a heliocentrikus érkezési sebesség 29,512 km/s és a gyorsítási sebesség értéke 14,891 km/s volt. Így tehát a Voyager–1 heliocentrikus távolodási sebessége, amellyel elindul a hatásszféra határa felé: 44,803 km/s lesz.

Ha a Nap hatásszférájának a határán a távolodási sebességet 42,45 km/s értéknek vesszük, akkor az indulási sebesség 44,58 km/s lesz, tehát minimális értékkel kisebb, mint a tényleges sebességérték, így az indulási sebesség kiszámításához ezt a sebességértéket használhatjuk. A szonda, ebben az esetben az indulási és a hatásszféra határára érkezési sebességek összegének a felével teszi meg az óriási távolságot, vagyis 43,626 km/s átlagsebességgel halad a hatásszféra határáig.

Ezután már csak azt az időtartamot kell kiszámítani, amely alatt a mintegy 59 990 CSE távolságot a szonda, ilyen átlagsebességgel fogja megtenni. Az átlagsebesség értéke tehát 43,626 km/s. A továbbiakban meghatározzuk, hogy a szonda, az átlagsebességével hány s alatt teszi meg az 59 990 CsE távolságot megszorozzuk 149 600 000-rel. Az így kapott értéket elosztjuk 3600-al és megkapjuk az időtartamot órában. Ha azt elosztjuk 24-gyel, majd 30,4-el, majd 12-vel, megkapjuk az eredményt évben. Elvégezve a jelzett számításokat, megkapjuk, hogy a Voyager–1 űrszonda az indulástól számított 6526,7 év múlva fogja elhagyni a Naprendszert. A ma elérhető legnagyobb indítási sebesség esetén tehát ilyenek a lehetőségeink, amelyek azonban jól jelzik, hogy ma még az ember ilyen távolságra való utazására még nincsenek meg a feltételek.

A Voyager–2 útvonalszámítása

Most végezzük el ugyanezt a számítást a Voyager–2-re. A kiindulási adatokban csupán annyi a változás, hogy változik, vagyis csökken az indulási sebesség: v0 =16,08 km/s; továbbá változnak a θ szögek, amelyeket jelezzük a képletek előtt. A Naprendszerre vonatkozó adatok ugyanazok, mint a Voyager–1-nél. Ennek megfelelően:

$$v^2 = v_0 - \frac{2K_F}{r_0} \cdot \left(1 - \frac{r_0}{r}\right) = 16{,}08^2\ km^2/s^2 - \frac{2 \cdot 398600\, km^3/s^2}{6371\, km} \cdot \left(1 - \frac{6371\, km}{930000\, km}\right) =$$

$$258{,}566\, km^2/s^2 - 125{,}13\, km^2/s^2 \cdot 1 - 0{,}0685 = 258{,}566\, km^2/s^2 - 124{,}254\, km^2/s^2 = \qquad (19)$$

$$= 134{,}312\, km^2/s^2; \qquad v = \sqrt{134{,}312\, km^2/s^2} = 11{,}589\, km/s.$$

A távolodási sebesség a Föld hatásszférájának a határán tehát 11,589 km/s, a heliocentrikus távolodási sebesség pedig vt = 11,589 + 29,758 = 41,347 km/s. Az indulási sebesség tehát 41,347 km/s, s a már ismert képlettel meghatározzuk a Jupiter hatásszférájának a határára érkezés heliocentrikus sebességét, vagyis itt már a Napra vonatkozó adatokkal számolunk. Tehát:

$$v^2 = {v_0}^2 - \frac{2K_N}{r_0}\cdot\left(1-\frac{r_0}{r}\right) = (41{,}347\,km/s)^2 - \frac{265436\,km^3/s^2}{149{,}6\,km}\cdot\left(1-\frac{149{,}6\,km}{730\,km}\right) =$$

$$= 1709{,}574\,km^2/s^2 - -1774\,km^2/s^2\cdot 0{,}795 = 1709{,}574\,km^2/s^2 - 1410{,}33\,km^2/s^2 = \quad (20)$$

$$= 299{,}244\,km^2/s^2; \qquad v = \sqrt{299{,}244\,km^2/s^2} = 17{,}298\,km/s.$$

A 41,347 km/s sebességgel a Föld pályamagasságról induló szonda tehát a Jupiter hatásszférájának a határára 17,298 km/s heliocentrikus sebességgel érkezik meg. Az útja során a sebességveszteség 41,347 – 17,298 = 24,049 km/s, vagyis kb. 59%. A heliocentrikus érkezési sebesség a Voyager–1-nél 21,407 km/s értéket képviselt, tehát mintegy 4,12 km/s volt a többletsebessége. A belépési sebesség ebben az esetben vbe =17,298 – 13,052 = 4,246 km/s, a θ = 88°, s ekkor a sin 44° = 0,695. Ennek megfelelően a gyorsítás értéke:

$$\Delta v = 8{,}492\,km/s\cdot\sin 39° = 8{,}492\,km/s\cdot 0{,}695 = 5{,}902\,km/s. \qquad (21)$$

Mivel az heliocentrikus érkezési sebességhez hozzáadva a gyorsítás értékét, a Jupiter pályamagasságáról a Szaturnusz felé az indulási sebesség vi = 17,298 + 5,902 = 22,639 km/s lesz. Elvégezve az érkezési sebességszámítást:

$$v^2 = 512{,}524\,km^2/s^2 - \frac{2\cdot 132718\,km^3/s^2}{778\,km}\cdot\left(1-\frac{778\,km}{1425\,km}\right) =$$

$$= 512{,}524\,km^2/s^2 - 341{,}177\,km^2/s^2\cdot 0{,}454 = 512{,}524\,km^2/s^2 - \quad (22)$$

$$-154{,}894\,km^2/s^2 = 357{,}894\,km^2/s^2; \quad v = \sqrt{357{,}630\,km^2/s^2} = 18{,}911\,km/s.$$

A Szaturnuszhoz tehát 18,911 km/s heliocentrikus sebességgel érkezik a Voyager–2. Mivel ott a θ = 90°, így a sin 45°= 0,707, a vbe = 24,867 – 9,636 = 9,275 km/s. A hatásszférában elért gyorsítás eredménye:

$$\Delta v = 2\cdot v_{be}\cdot\sin\frac{\theta}{2} = 18{,}550\,km/s\cdot 0{,}707 = 13{,}115\,km/s. \qquad (23)$$

Az érkezési sebesség plusz a gyorsítás eredményeként az indulási sebesség a Nap hatásszférájának a határa felé vi = 18,911 + 13,115 = 32,026 km/s. Ez mintegy 11,418 km/s sebességértékkel kisebb, mint amilyennel a Voyager–1 elindult. Ennek megfelelően, ha a számításokat elvégezzük, és a távolodási sebességet 29 km/s értékkel számoljuk, akkor az indulási sebesség 32,040 km/s, s ez az érték gyakorlatilag egyenlőnek vehető a korábban kapott 32,026 értékkel. Ekkor a közepes utazási sebesség 32,026 + 29 = 61,026, s ha ezt elosztjuk 2-vel, 30,5 km/s értéket kapunk.

Ezzel az értékkel számolva, a szonda utazási idejét a következő számításokkal kapjuk: Az indulási sebesség (32,026 km/s) és a hatásszféra átlépésekor megmaradó 29 km/s a sebesség összegét kettővel osztjuk, akkor megkapjuk a közepes utazási sebességet, amely vköz = 32,026 +29 = 61,026 km/s, osztva 2-vel 30,5 km/s átlagsebességet kapunk. Ha az 59990 csillagászati egységet átszámítjuk s-ra, vagyis osztjuk az átlagsebesség értékével, megkapjuk: 8,959842 x 1011 km értéket. Ha ezt elosztom 3600 s-al, 24-gyel, majd 30,4-gyel, aztán pedig 12-vel, megkapom az utazási időt évben, amelynek értéke 9335,6 év.

Így tehát a Voyager–1 6523 év múlva, a Voyager–2 pedig 9335 év múlva hagyja el a Nap hatásszférájának a határát. A számítás helyességét még úgy is igazolhatjuk, hogy a két szonda közepes távolodási sebességének a viszonya 30,5 : 43,65 = 0,698, továbbá az utazási időtartam-értékek viszonya, vagyis a 6523 : 9335 = 0,698, tehát a hányadosok is megegyeznek. A két szonda útvonal-számítási táblázatában megadtuk a legfontosabb részadatokat, amelyek alapján a két szonda útvonalát nyomon követhetjük:

Részadatok	**Voyager–1**	**Voyager–2**
Indulási sebesség a Föld felszínéről	17,48 *km/s*	16,08 *km/s*
Távolodási sebesség a Föld h.h.-n	13,444 *km/s*	11.589 *km/s*
Heliocentrikus sebesség a Föld pályáján	43,444 *km/s*	41,347 *km/s*
Érkezési sebesség a Jupiter h.h-ra	21,407 *km/s*	17,298 *km/s*
Indulási és érkezési sebességkülönbség	21,823 *km/s*	24,049 *km/s*
Gyorsítás a Jupiternél (Δv)	10,510 *km/s*	5,341 *km/s*
Indulási sebesség a Jupitertől	31,917 *km/s*	22,639 km/s
Érkezési sebesség a Szaturnusz h.h.-ra	29,512 *km/s*	18,911 km/s
Indulási és érkezési sebességkülönbség	2,400 *km/s*	3,428 km/s
Gyorsítás a Szaturnusznál	14,891 *km/s*	13,115 km/s
Indulás a Nap hatásszférájának a hat.-ra	44,630 *km/s*	32.040 km/s
Távolodási sebesség a Nap h.h-n	42,500 *km/s*	30,500 km/s
Utazási idő a hatásszféra határáig	**6523 év**	**9335 év**

Mindezek után, a számítások útján kapott értékek alapján egyértelműen levonhatjuk a következtetést, hogy ma még az emberiség, az ilyen nagy távolságok áthidalására — amelyek pedig még a Tejútrendszer viszonylatában is elenyészőek — nincs felkészülve. Ahhoz, a mai rakétákénál sokkal nagyobb kiáramlási sebességre lenne szükség, vagy új rakétatípusokat kellene alkalmazni, amelyekkel meglehetne közelíteni a fotonrakéták teljesítményét. Ilyen rakéták ma még csak a fantázia szintjén léteznek. Ugyanakkor nem szabad elfelejteni, hogy a mai eredményeink is, alig 100 éve, ugyancsak a fantázia birodalmába tartoztak, ma pedig több mint 600 űrhajós járt a világűrben, s az elmúlt alig 60 éve tartó űrkorszakban, már sok ezer rakétaindítást végezett az emberiség. Mindez — a jövőt illetően —, bizakodással tölthet el bennünket.

Még két adatról kell megemlékezni, éspedig arról, hogy az adott indulási sebességértékek birtokában, a két szonda mikor érheti el a legközelebbi csillagot. Feltételezzük, hogy a Voyager–1 célcsillaga, amely felé az irányát vette, s amely tőlünk mintegy 4,3 fényévre van. Ugyanakkor a Voyager–2 a mintegy 4,6 fényévnyire lévő csillag felé fog haladni. A távolodási sebességek figyelembe vételével a Voyager–1-es a célcsillag közelébe mintegy 30 000 év múlva érkezik, míg a Voyager–2 érkezési ideje, mintegy 50 000 évre tehető. Bizony, ezek óriási távolságok, amelyek áthidalásához, ma még nem rendelkezünk megfelelő eszközökkel. Még ha képesek lennénk is a fénysebesség 90%-ával haladni a kozmikus térben, akkor is, amint az alábbi táblázat adatai mutatják, az oda-vissza utazás időtartama mintegy 13 év lenne. Ehhez azonban számos olyan problémát kellene megoldani, amilyenről még csak elképzelésünk sincs, vagy legfeljebb csak az van.

Még egy kérdésről röviden. Napjainkban a csillagászok szerint már a csillagközi térben haladnak a Voyagerek. Nos, nekik is valószínűleg igazuk van, mert ahol e két szonda halad, már több a csillagközi anyag, mint a Napból kiáramló részecskék mennyisége. Mi azonban dinamikai szemléletünk okán azt mondjuk, hogy a két szonda a Naprendszerben halad és még fog is haladni több ezer éven át. Ha egyszer a hatásszféra határán belül a Nap határozza meg a mozgásokat, akkor jogos a kijelentés, mivel a Naprendszer határa 60 000 CsE távolságon van. Akkor a még attól messze haladó mindkét égitest ugyan már a csillagközi tér anyagát észleli

maga körül, de még mindketten a Naprendszer határán belül vannak, és még lesznek is sok ezer évig. [12]

Fantázia szülte a gondolatot, de most induljunk el a legközelebbi csillag felé mintegy 0,9 fénysebességgel. Einstein kimutatta, hogy a sebesség növekedésével az idő múlását lassúbbnak észleljük. Ennek megfelelően, az utazás alatti földi időt, valamint az űrhajóban eltelt időt feltüntetjük, s látni fogjuk, hogy egy ilyen utazás alatt mennyi lesz az időkülönbség. A legközelebbi csillagig és vissza, az út szakaszaira adjuk meg az időkülönbségeket.[3]

	Földi időtartam	Az űrhajóban
Gyorsítás egy négylépcsős űrhajóval	1,45 év	1,14 év
Utazás a célcsillag felé	3,33 év	1,85 év
Fékezés a csillag elérése előtt	1,45 év	1,14 év
Ott-tartózkodás a csillag valamelyik bolygóján	1.00 év	1,00 év
Gyorsítás vissza a Naprendszer felé	1,45 év	1,14 év;
Utazás az elért sebességgel (270 0000 *km/s*)	3,33 év	1,85 év;
Fékezés a Naprendszer elérése előtt	1,45 év	1,14 év
Összesen	**13,46 év**	**9,26 év**

A fentiekből kiderül, hogy míg a Földön 13,46 év telt el, mialatt az űrhajóban az utasok mindössze 9,26 évet öregedtek, tehát a földieknél 4,2 évvel maradtak fiatalabbak. Ebből következik, hogy az ilyen utazásnak is lenne valami haszna. Meg kell itt jegyezni: az ilyen utazás ma még csak vágyálom, amelytől ma még nagyon messze vagyunk. Az elképzelések szerint ilyen sebesség elérésére a fény felhasználásával lenne lehetőség. Ehhez az ún. annihilációs folyamatra lenne szükség, amely tulajdonképpen anyag és antianyag egyesítése, és amelynek eredményeként fény jön létre. Persze arra ma még, hogy a keletkező magas hőmérséklet kezelésére milyen módon lenne lehetőség, ma még elképzelés sincs. Az azonban tény, hogy ezzel a módszerrel roppant erős hajtóművet lehetne üzemeltetni, s ezt az állítást egy rövid számítással igazoljuk.

Amint korábban már meghatároztuk, egy rakéta legjellemzőbb adata az ún. fajlagos impulzus, az Ifajl., amely megmutatja, mekkora tolóerő hozható létre, pl. 1 kg hajtóanyag 1 s alatti elégetésekor. A fotonrakéta esetében: Ifajl. = c m/s /g m/s2 = 3,056 · 107 s = 30 560 000 kg·s/kg; (mai rakéták ≈ 300 s). Ez 100 000-szerese a mai kémiai energiával létrehozható tolóerőnek, azonos mennyiségű anyag felhasználása esetén. Ha tehát másodpercenként fél-fél kg anyagot és antianyagot egyesítve, a létrehozott fényt kiáramoltatjuk, akkor az kb. 30 560 t tolóerő hozható létre, ami elképzelhetetlenül nagy érték. Természetesen ez csak elméleti érték, ma még a megoldás, amely ilyen teljesítményhez vezetne, csak a fantázia szintjén létezik.

Érdekességként megemlítjük: 1t tömegű űrobjektum v = 11,2 km/s-ra való felgyorsításához ma 41 t hajtóanyag szükséges. Ilyen eredményhez, fotonrakéta esetén 410 g, vagyis ½ kg-nál kevesebb anyagra lenne szükség ugyanazon eredmény eléréséhez, vagyis 1 t tömegnek a második kozmikus sebességre való felgyorsításához.[7]

BEFEJEZÉS

Ezt a rövid fantázia szülte anyagot azért mutatjuk be, hogy lása az olvasó, milyen messze vagyunk még a csillagközi utazás reális lehetőségétől. Ugyanakkor nem szabad elfelejteni, hogy alig 100 évvel ezelőtt még senki nem tudta megmondani, hogy az ember mikor juthat ki a világűrbe. Eltelt 41 év, s megjelent a világűrben a Szputnyik–1, még eltelt 3,5 év és az első ember 108 perc alatt megkerülte a Földet. Még egy évtized sem kellett ahhoz, hogy az első ember a Holdra lépjen. Akkor gyorsan jöttek az egymást követő eredmények. Ma azonban kissé csökkent a tempó, s az első ember Marsra lépését, bár az 1960-as 70-es években még az

ezredfordulóra jósolták, ez már 16 éve elmúlt. Jelenleg egy ilyen utazás lehetőségével 15-20 év múlva, vagyis 2030-2035 körülire számolnak, mivel néhány, az emberi élet biztosításával kapcsolatos probléma még nem jutott el a megoldás stádiumába. Mivel e repülés során is a gyenge láncszem az ember, az odautazó űrhajósok életének mindenoldalú biztosítására kell fordítani a fő figyelmet. (Folytatjuk.)

Felhasznált irodalom

[1.] Almár Iván főszerkesztő, Horváth András szerkesztő: *Űrhajózási Lexikon,* Akadémiai Kiadó, Zrínyi Katonai Kiadó, Budapest, 1981.

[2.] V. I. Levantovszkij: *Mechanyika koszmicseszkogo poljota v elementarnom izlozse-nyii*, Izdatyelsztvo „NAUKA", Glavnaja Redakcija Fiziko-matyematyicseszkoj Lityeraturi, Moszkva, 1974.

[3.] A. P. Razigrajev: *Osznovi upravlényija poljotom koszmicseszkih apparatov i korab-lej,* Izdatyelsztvo Masinosztrojényije, Moszkva, 1977.

[4.] V. I. Bazsenov, M. I. Oszin: *Poszadka koszmicseszkih apparatov na planyeti,* Izdatyelsztvo Masinosztrojényije, Moszkva, 1978.

[5.] I. B. Afanaszjev: *Nyeizvesztnie korabli,* Izdatyelsztvo Znanyije, Moszkva, 1991.

[6.] A. Sternfeld: *Vvegyenyije v koszmonavtyiku,* Izdatyelsztvo „NAUKA", Moszkva, 1947.

[7.] Szabó József: *Az ember és a világűr, Űrdinamika, bővített előadásvázlat,* Zrínyi Miklós Nemzetvédelmi Egyetem Távoktatási Központ kiadványa, Budapest, 2010.

[8.] K. Ciolkovszkij: *Izszledovanyije mirovih prosztransztv reaktyívnimi priborami,* Tyipografija Sz. A Szemjonova, Kaluga, 1914.

[9.] K. Ciolkovszkij: *Koszmicseszkije raketnie pojezda,* Kollektyiv szekcii naucsnih rabotnyikov, Kaluga, 1929;

[10.] K. Ciolkovszkij: *Celi zvezdoszplavanyije,* Gosztyipografija OSZNH, Kaluga, 1929.

[11.] Oriana Falaci: *Ha meghal a Nap,* Európa Könyvkiadó, Budapest, 1984;

[12.] Szabó József: *A Voyager szondák útvonalszámításai,* Saját számítások.

HADMÉRNÖK

XI. Évfolyam 2. szám – 2016. június

Tóth József
toth.jozsef@uni-nke.hu

A REPÜLŐ MŰSZAKI TISZTEK SZAKMAI KOMPETENCIÁINAK KUTATÁSA

Absztrakt

A szervezet működésének, és az elvárt minőségű feladat-végrehajtás biztosításának egyik alapfeltétele a megfelelő számú, jól képzett szakember. A képzési szerkezet, az infrastruktúrák, a humánerőforrás fenntartása és folyamatos fejlesztése érdekében fontos ismerni, hogy milyen kompetenciákkal rendelkező műszaki szakemberekre van szükség a Magyar Honvédségben. A katonai repülőműszaki feladatokat ellátó szervezetek működésének, és az elvárt minőségű feladat végrehajtásnak alapfeltétele a megfelelő számú, jól képzett tiszt, műszaki szakember. Az elvárt tudással rendelkező tiszti utánpótlás érdekében fontos ismerni, hogy milyen kompetenciákkal rendelkező műszaki szakemberekre van szükség a Magyar Honvédségben. A tervezési/előrejelzési és aktuális megrendelői tendenciákat elemző kutatás olyan információkat biztosít, amelyek hozzájárulhatnak az oktatási és képzési portfólió, valamint a szakokon végzett diplomások felkészültsége és a munkaerő-piaci elvárások összehangolásához. Egy ilyen kutatás folyamata, és eredményeinek bemutatása olvasható a cikkben.

A precondition of the proper functioning of our organizations is a sizeable body of well-trained professionals. The ongoing development of educational content and structure, the changing needs of the labour market, and the novelties of the technological environment make it necessary to conduct regular research to clear what competencies military engineers should possess. Military aviation organizations should dispose over well-trained, professional personnel. In order to enable their work and qualifying them for their tasks, they receive schooling following particular standards of education as well as those of final results. The provision of ongoing supply of new generations of military aviation specialists requires an understanding of competencies requested by the various air force jobs. Research and assessment concentrating on present requirements on the side of the employer and proper analysis for the sake of forecasting and planning may add value to the education and training portfolio development. The present article presents some results of such a research.

Kulcsszavak: *repülőmérnök, katonai műszaki oktatás, kompetenciák, modell, minőség, vezetés, fejlesztés, kvantitatív kutatás ~ aviation engineering, military engineer education, competency, modelling, quality, management, development, quantitative research*

BEVEZETÉS

Az elmúlt évtizedekben a felsőoktatásban bekövetkezett változások jelentős hatást gyakoroltak a védelmi szektor felsőoktatási intézményeire, ezen belül is a repülő műszaki tisztképzésre. A képzések kimenetén követelményként jelentek meg a kompetenciák, melyek a képzés tantárgyi struktúrájának, belső idő (kredit) arányainak, más tartalmi és módszertani elemeinek átalakítását tették szükségessé.

Ezekkel a változásokkal parallel módon a Magyar Honvédség Légierejénél is a repülőtechnika tekintetében jelentős, a szervezetek és folyamatok alapvető, lényegi elemeit érintő változások zajlottak. A már meglévő légi járművek mellé új harcászati repülőtechnika jelent meg, míg más eszközök kivonásra kerültek az üzemeltetés rendszeréből.

Az új repülőtechnika új üzemeltetési stratégia, és filozófia bevezetését követelte, mely új kihívásokat jelentett a repülő műszaki üzembentartó szervezetek vonatkozásában, és az abban tevékenykedő szakemberekkel szemben támasztott követelmények szempontjából is. A változás az infrastruktúra elemein át a műszaki üzembentartó szervezetek felépítését, a szervezeten belüli munkamegosztást, a szakszemélyzetekkel, a repülő műszaki tisztekkel szembeni szakmai elméleti és gyakorlati követelményeket is átalakította.

Az új üzemeltetési technológia az eddigiektől eltérő, újfajta rendszerismeretet és rendszerszemléletet követel, amely a repülő eszköz rendszereinek más típusoktól eltérő üzemeltetési rendszerfelosztásából is adódik. Ez azt jelenti, hogy a repülőgép rendszereinek felosztása a hagyományos gépészeti (sárkány, hajtómű), elektromos, fegyverzeti rendszerekre való bontás helyett, olyan funkcionális egységekre történik, amelyek egyaránt tartalmaznak mechanikus, elektronikus, és/vagy fegyverzeti elemeket is. Ez a rendszerfelosztás az üzemeltetésben tevékenykedő szakemberek szempontjából egyrészt a meglévő tudásuk, tapasztalataik átértékelését, másrészt új szemléleti, és tudáselemek megszerzését jelentette.[1][14][26][27][28]

KOMPETENCIA

A kompetenciakutatások milyen nézőpontból, vonatkoztatási rendszerből kiindulva végzik vizsgálataikat. A releváns szakirodalom alapvetően két megközelítést tárgyal. [3][4]

„Income” megközelítés; ebben az értelemben a kompetencia [6] megközelítéséből indul ki, vagyis ide tartozik az egyénnek minden olyan viselkedéses jellemzője, amely oksági összefüggésbe hozható a kiváló és/vagy átlagos munkahelyi teljesítménnyel. Fókuszában azok az inputok (személyes tényezők) állnak, amelyek segítenek a hatékony munkateljesítmény elérésében. Ezek gyakran viselkedéses kompetenciákként („behavioural competencies”) vannak leírva. Az egyén hatékonyságát akkor tudjuk értékelni és fejleszteni, ha nem a munkakör egyes aspektusait, hanem a legjobban teljesítők személyiségjegyeit vesszük alapul [5]

„Outcome” megközelítés abból a definícióból indul ki, amely olyan aktivitások végrehajtásának képességére vonatkozik egy foglalkozáson, munkaköri feladaton belül, amelyek megfelelnek az adott munkakör előírt követelményeinek.. Ebben a megközelítésben, a középpontban a kimutatott kompetenciaigények, mint outcome-ok (munkaköri követelmények végrehajtására való képesség) állnak. Ezek gyakran munkaköralapú kompetenciákként/kompetencia-igényként írhatók le, akár a sztenderd munkakörökre vonatkoztatva. Az outcome szemlélet képviselői úgy vélik, hogy a hatékony teljesítményt nem az egyén viselkedései, hanem a munkaköréhez tartozó feladatok hatékony ellátása bizonyítja, és a szervezet számára ezeknek a teljesítéseknek van valójában értéke. Nyilván itt a hatékonyság a tevékenység, munkafeladat elvégzéséhez kapcsolódó teljesítmény szinthez kötődik.

Az elmúlt években újabb megközelítések jelentek meg a kompetenciákkal kapcsolatban, amik a hangsúlyt a dolgozó munkával kapcsolatos átélt tapasztalataira helyezik a hangsúlyt.

Sandberg tanulmánya [8] azt sugallja, hogy az, ahogyan a dolgozó értelmezi, felfogja, megérti a munkáját, az jelenti a kompetenciát, és előbbre való a készségeknél és tudásnál, amivel rendelkezik. A szerző úgy véli, hogy az, ahogyan értelmezzük a munkát, szervezi megkülönböztető kompetenciákba tudásunkat, készségeinket. Habár ez a megközelítés viszonylag még új keletű, szemléletmódjában az „income" megközelítésekhez áll közel. A repülő műszaki tiszti kompetenciákkal kapcsolatban is ezt a megközelítést alkalmaztam a kutatás során.

Figyelembe véve a kompetencia fogalommal kapcsolatos bőséges irodalmat, és elemzést, illetve a fogalom sokszínűségét munka-definícióként a Spencer&Spencer [7] által közzétett meghatározást alkalmaztam a kutatás során. Eszerint tehát a kompetencia „Egy személy alapvető, meghatározó jellemzői, melyek okozati kapcsolatban állnak a kritériumszintnek megfelelő hatékony és/vagy kiváló teljesítménnyel." A fogalmat némileg finomítva úgy értelmezem, mint egy foglalkozás, szakma adott feladatának az elvégzéséhez szükséges ismeretek, magatartásformák (attitűdök) és képességeket összessége. [7][8][17][18][19] [20][21][22][25][26][28]

KVALITATÍV KUTATÁS

A kutatás a felsőfokú repülőműszaki végzettséggel betölthető munkakörök kompetencia térképének megalkotásához szükséges megalapozott ismeretek elemzése volt. A szervezet igényeihez igazított kompetenciamodell (az átfogó modellekben a kompetenciák előre elkészítetten rendelkezésre állnak) megalkotásához nyújt segítséget, hogy meghatározható legyen, hogy mely kompetenciák milyen mértékben fontosak az adott beosztásokhoz, illetve hogy akár teljesen új modell legyen összeállítható.

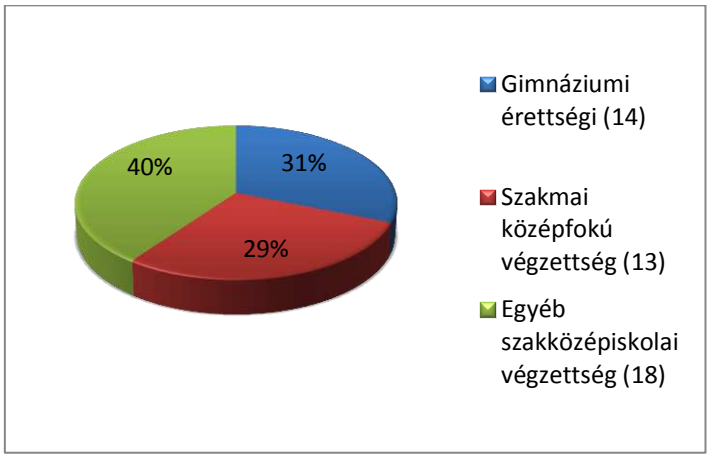
A kutatás célcsoportját tehát a repülő műszaki beosztásban jelenleg is aktívan dolgozó, vagy huzamosabb időn át a katonai repülésben műszakiként tevékenykedő tisztek (vagy annál magasabb rendfokozatúak), és a civil, illetve nyugdíjas repülő műszaki szakemberek képezték. A célcsoport jellemzője, hogy létszámát tekintve kicsi (a marketing, a szociológiai vagy más kutatásban megszokott szegmensekhez képest), és egy igen szűk szakmai területre koncentrálódó közösséget jelent. Ezek a jellemzők határozták meg és egyben indokolták is az alkalmazott mintavételi módot.

A mintavételezés során határoztuk meg a vizsgált sokaságból, azokat a személyeket, akik reprezentálni képesek (mély, információban gazdag ismeretei vannak, a megértéshez érdemben hozzá tud járulni, és a keresett információ veszteség nélkül kinyerhető) a felsőfokú végzettséggel rendelkező repülőműszaki ismeretekkel (elméleti és/vagy gyakorlati tudással, gyakorlattal bíró) személyeket, és ismerhetik a repülőműszaki katonákra jellemző kompetenciákat. Kihasználva a korábbi ismeretségeinket, illetve a hólabda–mintavétel módszert alkalmazva léptünk kapcsolatba olyan emberekkel, akik releváns ismeretekkel rendelkeznek a kutatott témával kapcsolatban, és segítségünkre lehettek a kutatási feladat elvégzésében.

A mintába bekerült interjúalanyok középfokú iskolai képzettségük a tekintetében az 1. ábrán látható módon oszlottak meg. A diagramból kitűnik, hogy a résztvevők közel kétharmada repülő szakmai, illetve szakközépiskolai végzettséggel került a pályára. A felsőfokú végzettség tekintetében a megkérdezettek összetétele a következőképpen alakult (2. ábra). Az interjúalanyok alig több mint fele a szolnoki főiskolán (illetve annak utód intézményében) szerzett szakmai felsőfokú végzettséget. A megkérdezettek mindössze 2%-a rendelkezett nem szakirányú egyetemi végzettséggel, ami rendkívül jó aránynak mondható.

A szakmai tapasztalatok tekintetében néhány kivételtől eltekintve rendelkezett legalább 5 éves repülőgép üzemeltetési tapasztalattal. A megkérdezettek közül átlagosam 3 év üzemeltetési gyakorlattal rendelkeztek a Gripen üzemeltetése kapcsán, de az ilyen kollégák közül egyikőjük sem szerzett 4 évnél kevesebb szakmai tapasztalatot. Az egyéb típusokon

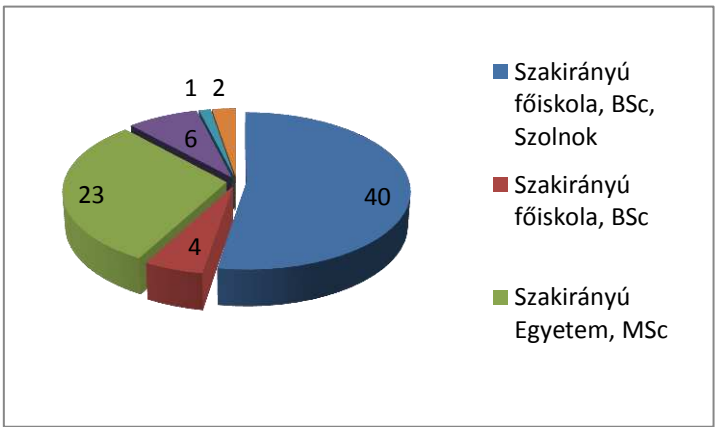
szerzett szakmai gyakorlat vonatkozásában az átlag 8 évre adódott, az ingadozás pedig 3 év és 25 év kötött alakult.



1. ábra Az interjúalanyok középfokú végzettség szerinti megoszlása (Saját szerkesztés)

Az interjúk felvételére 2015. november, december hónapokban került sor, és végeredményként 45 interjú felvétel készült el.

A felvett interjúk alapján az elvégzett tartalomelemzés eredményeként a következő kompetenciákat azonosítottam. A kompetenciákat, melyek itt jellemző tulajdonságok formájában jelentkeztek a tudás két komponense, (a „Tudni mit?” és a „Tudni hogyan?”), a képességek, készségek, valamint az elvárt magatartás (attitűd) kategóriái szerinti csoportosításban rendszereztem.[1]



2. ábra Az interjúalanyok felsőfokú végzettség szerinti megoszlása (Saját szerkesztés)

Ez teremtett alapot a kutatás kvalitatív részéhez, melynek módszereként a kérdőíves lekérdezést alkalmaztam. [15][23][24][26][27]

A KVANTITATÍV KUTATÁS LEÍRÁSA, EREDMÉNYEI

A kérdőíves kutatás kettős célt szolgált. Az egyik cél a kvantitatív kutatás során nyert információk, vagyis a kapott kompetenciák validálása, megerősítése volt. A másik cél pedig olyan új információk megszerzése, melyek az interjúk során csak közvetetten, vagy egyáltalán nem álltak rendelkezésre. Ilyen új tartalom és információ, az egyes kompetenciák fontosságának megítélése, valamint annak megállapítása, hogy a vezetői (parancsnoki) munkakörök kompetenciái mennyiben térnek el a beosztottakétól. A másik alapvető

[1] A kvalitatív kutatás leírását és eredményeit részletesen lásd: [23] irodalomban

fontosságú információ az üzemeltetett repülőeszközökkel kapcsolatos, vagyis, hogy melyek azok a kompetenciák, melyek a két egymástól elkülönült üzemeltetési stratégiákkal hozható összefüggésbe. összefoglalva tehát olyan új információt jelentő kérdésekre kerestem a választ, hogy:

- Mely kompetenciákat (tulajdonságokat) tartják fontosnak, illetve kevésbé fontosnak?
- A kompetenciák (tulajdonságok) közül melyek fontosabbak vezetői munkakörökben?
- Melyek azok a kompetenciák (tulajdonságok), amik kizárólag a Gripenek üzemeltetési rendszerében nagyobb, esetleg kizárólagos jelentőséggel bírnak?

Az előzőekből is kitűnik, hogy a kérdőívben az életút interjúk elemzése alapján kapott kompetenciákra vonatkozó kérdések szerepeltek alapvetően, az egyes kérdéscsoportok végén lévő nyitott kérdésben biztosítottam a válaszadó számára újabb tulajdonságok megjelenítését.

Az elkészített kérdőív első részében a felkérő levelet követően a kutatáshoz szükséges általános adatokra vonatkozó kérdések szerepeltek.

I. rész Általános adatok:

1. Jelenlegi beosztásához előírt iskolai végzettség (Egyetem, főiskola)

- Legmagasabb szakmai iskolai végzettség
- Főiskola,
- Egyetem,
- PhD,
- szakirányú továbbképzés,
- szakmai tanfolyamok,
- speciális képzések)
- Egyéb:

2. Szakmai életútja során milyen típusú munkakörökben, mennyi ideig dolgozott: *(jelölje X-el a betöltött munkaköröket,)*:

3. Főiskolai végzettséghez kötött, beosztott
    - 1-5 év
    - 6-10 év
    - 10-nél több
- Főiskolai végzettséghez kötött, vezető (parancsnok)
    - 1-5 év
    - 6-10 év
    - 10 -nél több
- Egyetemi végzettséghez kötött, beosztott
    - 1-5 év
    - 6-10 év
    - 10-nél több
- Egyetemi végzettséghez kötött, vezető (parancsnok)
    - 1-5 év
    - 6-10 év
    - 10-nél több
- Felső vezető:
    - 1-5 év
    - 6-10 év
    - 10-nél több

4. Szakmai pályafutása során munkaköri feladatai milyen légi járművekhez kapcsolódtak? *(Válaszát jelölje X-el,)*
    - JAS-39 (Gripen),
    - minden más típus (legalább egy)

Ez a kérdéscsoport arra irányult, hogy a válaszadókat el tudjam különíteni iskolai végzettségük, vezető, vagy beosztotti munkakörük, valamint az üzemeltetett (vagy a munkaköréből adódó feladatai vonatkozásában releváns) repülőgép típus alapján. Ez lehetőséget biztosított számomra, hogy a kérdőív további részében a válaszadókat különböző csoportokra bontsam, és az egyes csoportok a számukra releváns kérdéseket kapják. Az információszerzés szempontjából az alábbi csoportokat különítettem el:
beosztott, Gripent és más típust is üzemeltetett;
beosztott, minden más típust üzemeltetett;
vezető, Gripent és más típust is üzemeltetett;
vezető, minden más típust üzemeltetett.

A kérdőív további részében a korábban említett, és az interjú elemzés eredményeként kapott tulajdonságokkal kapcsolatos kérdések szerepeltek. A kérdések annak megítélésére vonatkoztak, hogy a válaszadó mennyire fontosnak tartja az adott tulajdonságot a repülő műszaki tiszti tevékenység kapcsán általában, ezen kívül vezető beosztású tisztként, valamint a különböző üzemeltetési endszerekkel összefüggésben.

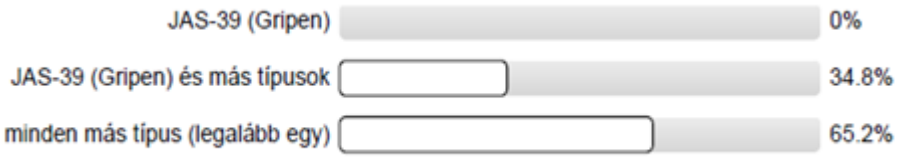
A kérdőíves kutatásba 152 főt vontunk be. A kutatásba való bekerüléshez szükséges e-mail címeket személyes ismeretségek felhasználásával és a már alkalmazott hólabda-mintavétel módszer újbóli alkalmazásával gyűjtöttem össze. A kérdőíveket az EvaSys rendszer segítségével elektronikusan az internet nyújtotta lehetőségek kihasználásával e-mailes felkérő levélben küldtük el a célcsoporthoz. A felkérő levélben tájékoztattuk a megkérdezetteket a vizsgálat tárgyáról, céljáról, a kutatásban való részvétele fontosságáról, az anonimitásról, az önkéntességről és megköszöntük a segítségét. A levél végén találták a címzettek azt a linket, amelyen keresztül elérhető volt a kérdőív. A kérdőíves lekérdezés 2016. 03. 03. és 2016. 03. 16. között történt. A kiküldött 152 elektronikus levélre 89 kitöltött kérdőív érkezett vissza, ez 58,55%-os részvételi aktivitást jelentett. A válaszadók felsőfokú végzettséggel és repülőműszaki tudással/végzettséggel rendelkeztek. Egyértelműen megállapítható, hogy a kutatáshoz való hozzáállás igen jónak tekinthető. Az 58,5% azt is bizonyítja, hogy a repülőműszaki szakma ilyen irányú vizsgálatának fontosságát még inkább belátják a repülőműszaki szakemberek.

A kérdőívek értékelése az EvaSys rendszer nyújtotta lehetőségek kihasználásával történt.

Az általános kérdésekre adott válaszokból kiderült, hogy a válaszadók 46%-a főiskola elvégzése után 5 éven belül valamilyen parancsnoki beosztásba került. Az életpálya csúcspontját jelentő egyetemi végzettséghez kötött vezető beosztással a megkérdezettek 45,3 %-a rendelkezett, és abban legalább 1 évig dolgozott. öt évnél több tapasztalattal a válaszadók 22%-a rendelkezett, ami meghatározó, releváns szakmai tudást igazol.

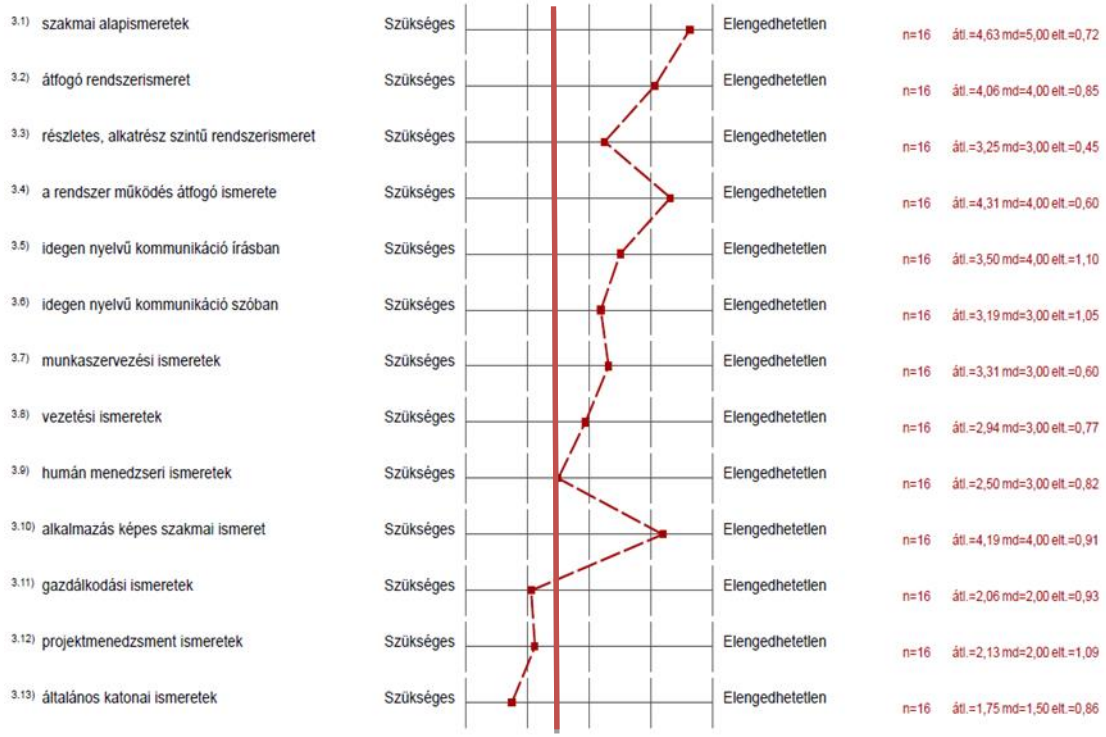
A megkérdezettek között nem volt olyan szakember, aki csak a Gripen üzemeltetésében dolgozott volna, ami az üzemeltető szervezetbe való bekerülés kapcsán (svédországi képzés, előírt üzemeltetési gyakorlat) érthető, és indokolt.

A légi járművekhez kötődő üzemeltetési tapasztalatok a következőképpen alakultak:



3. ábra A válaszadók üzemeltetett repülőeszközök szerinti megoszlása (Feldolgozott kérdőív részlet)

A repülő műszaki tisztek kompetenciáival kapcsolatos véleményeket, az összegzett, vagyis a teljes mintára vonatkoztatott profilgörbén követhetjük, mely az egyes válaszok átlagait mutatja. A kérdőívek részletes érékelését az első kérdéscsoport példáján mutatom meg. Az első kérdéscsoport az elvárt tényszerű, szakmai tárgyi tudásra vonatkozott.



4. ábra az első kérdéscsoportra adott válaszok profilgörbéje (Az Eva Sys rendszer generálta profilgörbe)

A kutatási céllal összefüggésben azokat a kompetenciákat kell kiemelni, amelyek legalább 3-as osztályzatot kaptak, tehát legalább fontosnak ítélték a válaszadók. Ilyen 8 tulajdonság adódott.

A feldolgozás során kapott eredmények alapján a repülő műszaki tisztek kompetenciái kapcsán néhány igen fontos következtetés vonhatók le.

A kemény idős üzemeltetési stratégia szerint történik a második generációs repülő eszközök műszaki üzemeltetése, úgymint a Mi-8, Mi-17 helikopterek, és az An-26 szállító repülőgépek műszaki kiszolgálása. Ezen légi járművek rendszereit szakágak szerint csoportosítva üzemeltetik, és ennek megfelelően gépészeti, elektromos műszer és oxigén, rádió, lokátor, valamint fegyverzeti rendszerek ismeretével rendelkező műszaki szakembereket igényel. A műszaki tisztek alapvető tudása is ehhez kell, hogy igazodjon, míg más szakágak ismerete szükségtelen.

A javítási, karbantartási eljárások megbízható végzése alapjaiban mély rendszerismeretet, és rendszerben való gondolkodást igényel. A repülő eszközök diagnosztikai fejlettsége nem teszi szükségessé a számítógépek, és a kapcsolódó alkalmazások mély ismeretét.

A szakmai tapasztalatoknak a hibafeltárás során van nagy jelentősége. A tapasztalat itt a meghibásodás okának gyors megtalálásában jut döntő szerephez, amely mély, átfogó rendszerismeretet és akár alkatrész szintű tudáson alapul. Különösen fontossá válik ez a tudás a javító osztály szakembereinél, hiszen az időszakos munkák mellett itt történik azoknak a hibáknak a feltárása, és javítása, amelyeket az üzemben tartó századoknál nem végezhetnek el.

A vezetési, vezetői (leadership) ismeretekre a szervezeti hierarchiának megfelelő parancsnoki (csoport- műhelyparancsnok, századparancsnok és helyettese, hangárparancsnok és helyettese s.í.t.) van szükség. A repülések műszaki kiszolgálásánál a szolgálati személyek a kiszolgálási folyamatok irányításáért felelősek, így vezetői funkciót ebben a szerepkörben nem töltenek be. [12][13][14]

A műszaki munkák dokumentálása ebben az esetben dominánsan papír alapon történik, ennek pontos, szakszerű vezetése alapvető fontossággal bír.

A Gripen, mint negyedik generációs repülő eszköz építési elvéből következezően rendszereinek nagyfokú elektronizáltsága okán az előbbitől lényegesen eltérő rendszercsoportosítással rendelkezik. Így az üzemeltetésben dolgozó műszaki tiszteknek magas szintű gépészeti, elektronikai és elektrotechnikai ismeretekkel is rendelkezniük kell.

A JAS-39-re érvényes, és fentebb bemutatott üzembentartási rendszerben egyértelműen megvalósul az a számítógéppel támogatott, és valós idejű állapotinformációkra épülő üzembentartás, ami alapja a mai modern, negyedik generációs repülőgép üzembentartási stratégiának. Mind a földi kiszolgáló személyzet, mind pedig a hajózó állomány számára rendkívül nagy segítséget nyújt a fedélzeti önellenőrző rendszer. A folyamatosan működő monitorig és adatrögzítő rendszer pedig nem csak a repülések kiszolgálásához, de az időszakos javítások gyors és hatékony elvégzéséhez is segítséget ad.

A fentiektől lényegeses eltérő vonás a rendszerismeret szintjében van. A fent ismertetett elektronizált rendszerek nem igénylik az alkatrész szintű rendszerismeretet, különösen igaz ez a műszaki üzembentartó századnál tevékenykedő tisztek esetében. A meghibásodások okainak feltárása lényegileg szükségtelen, lényegében javítási feladatok nem adódnak. A mélyebb rendszerismeret elsőként a hangár, kiemelten azonban a rendszermérnökök szintjén jelenik meg.

Szintén lényeges eltérés a hagyományos technikához képest az, hogy az üzemeltetési folyamatban létrejövő információk elektronikusan keletkeznek, és jelennek meg, így azok feldolgozása, és értelmezése egy másfajta, az eddigitől eltérő szemléletet, és gondolkodás módot igényel.

A Gripen üzemeltetési rendszerében azonban a számítástechikával kapcsolatos hardver, és szoftver ismeretek jelentősége is kiemelt.

A hibajavítás vonatkozásában megállapítható, hogy bizonyos javítási feladatokat (például forrasztás, kompozit elemek javítása) csak az ezekre vonatkozó jogosultsággal rendelkező szakemberek végezhetnek, mely jogosítványokat külföldön elvégzett tanfolyamok keretében szerezhetnek meg a szakemberek.

Ezzel összefüggésben az idegen nyelvű kommunikáció, és annak minden formája felértékelődik nemcsak a javítások, hanem a repülőgép technológiai dokumentációjának használata kapcsán is.

Az eredmények alapján igazolható, hogy a vezetni tudás hasonló szervezeti szinteken jelentkezik itt, mint a kemény idős üzemeltetési rendszerben. A rendszermérnökök különlegesen fontos helyzetben vannak, ugyanis a repülőgép műszaki kiszolgálása során jelentkező döntési helyzetek ezen a szinten összpontosulnak. [2][9][10][11][14][16][29][30]

ÖSSZEGZÉS

A társadalomtudományokban alkalmazott kutatási módszerek felhasználásával, a cikkben ismertetett módon, a repülő műszaki tisztek szakmai kompetenciái meghatározhatók. Az

alkalmazott kombinált, azaz a kvalitatív, és kvantitatív kutatási módszer egymásra épülő alkalmazása alkalmas azon szakmai kompetenciák megtalálására, amelynek segítségével a repülő műszaki szakemberek elvárt explicit és implicit tudáselemei meghatározhatók.

A kutatás alapján megállapítható, hogy a repülő műszaki tisztek képzése eredményeként megjelenő tudás kompetenciákként értelmezhető, és azok megfeleltetése a katonai repülőeszközöket üzemeltető szervezetek szakmai elvárásának biztosítja megfelelő szakemberek kibocsátását fegyverzetváltás esetén is.

Az ismertetett kutatási módszer felhasználásával meghatározott kompetenciák az eltérő üzemeltetési stratégiák elvárásainak megfeleltethetők.

Az alkalmazott kutatási modell figyelembe veszi a kimeneti elvű szabályozás elvét, és lehetőséget biztosít a tanulási eredmények meghatározásán alapuló programok kialakítására, amely a repülő műszaki tisztek kompetencia alapú képzési programjainak, és azok alapját képező Képzési és Kimeneti Követelményeinek adekvát meghatározásához biztosíthat módszertani alapot.

Felhasznált irodalom

[1] KAVAS LÁSZLÓ – ÓVÁRI GYULA: A katonai repülőgépek korszerű üzemeltetési eljárásainak elvi alapjai és gyakorlati hozadéka, Repüléstudományi Közlemények, XXV. évfolyam 2013.1. szám, Available at: http://www.repulestudomany.hu/index_rtk.html (2016.05.04)

[2] DR. SZEGEDI PÉTER: A pilóta nélküli repüléshez kapcsolódva... Tanulmány a pilóta nélküli légijárművek működésével és üzembentartásával kapcsolatban, p.: 80, ISBN 978-963-12-5224-8, 2016, Available at: https://ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10148/Tanulmany_Szegedi_P%C3%A9ter.pdf?sequence=2&isAllowed=y (2016.05.04)

[3] PATÓ GÁBORNÉ SZŰCS BEÁTA: Kompetenciák, feladatok logisztikai rendszerekben. Doktori (PhD) értekezés. Pannon Egyetem, Szervezési és Vezetési Tanszék, Gazdálkodás-és Szervezéstudományok Doktori Iskola, Veszprém 2006, Available at: http://konyvtar.uni-pannon.hu/doktori/2006/Pato_Gaborne_Szucs_Beata_dissertation.pdf (2016.05.04)

[4] DR. GŐCZE ISTVÁN: A tudományelmélet és kutatásmódszertan alapjai, A tudományos kutatás és publikálás, Tanulmány, ZMNE, KLHTK, Katonai Stratégiai Tanszék, Budapest, 2010, Available at: http://www.lib.pte.hu/csomag/FEEK/MA-Lev/01felev/ Kocsis_M. Tudomanyelmelet/GOCZETUDELM_KUTMODSZT_TANULMANY.PDF (2016.05.04)

[5] SZEGEDI PÉTER: Gondolatok a magyar honvédség szervezeti kultúrájának fontosságáról, Véget ért a MIG-korszak, Repüléstudományi Konferencia, 2011, Szolnok, Available at: http://www.repulestudomany.hu/kulonszamok/2011_cikkek/Szegedi_Peter.pdf (2016.05.04)

[6] VASS VILMOS: A kompetencia fogalmának értelmezése, válogatás dr. Vass Vilmos publikációiból http://www.petsul.hu/dokumentumok/valogatas.pdf (2016.05.04)

[7] SPENCER, L. M. – SPENCER, S. M. JR.: Competence at Work: Models for Superior Performance. Boston: Wiley. p. 384 (1993)

[8] SANDBERG J.:Understanding Human Competence At Work:An Interpretative Approach, Academy of Management Journal, 2000, Vol. 43. No. 1: 9–25.

[9] KORONVÁRY PÉTER: TQM a közszférában?: Veszélyek és lehetőségek Hadmérnök 9:(3) pp. 281-289. (2014) http://hadmernok.hu/143_23_koronvary_1.pdf (2016.05.04)

[10] LÁZÁR EDE: Kutatásmódszertan a gyakorlatban az SPSS program használatával, Sapientia Erdélyi Magyar Tudományegyetem Gazdaság- És Humántudományok Kar, Csíkszereda Üzleti Tudományok Tanszék, Scientia Kiadó, Kolozsvár 2009, http://ghtk.csik.sapientia.ro/data/cvk/Lazar%20Ede%20Kutatasmodszertan%20jegyzet.pdf (2016. 04. 27)

[11] HÉRA GÁBOR – LIGETI GYÖRGY: Módszertan Bevezetés a társadalmi jelenségek kutatásába, Osiris Kiadó, Budapest, 2006, p. 371., (ISBN 963 389 788 2)

[12] KORONVÁRY PÉTER: Gondolatok a vezetéstudomány feladatáról, Hadmérnök 3:(2) pp. 161-168. (2008) Available at: http://hadmernok.hu/archivum/2008/2/2008_2_koronvary.pdf (2016.05.04)

[13] KORONVÁRY PÉTER: Kicsoda a vezető?: Gondolatok a vezetői felelősségről, Hadmérnök 9:(3) pp. 290–295. (2014) Available at: http://hadmernok.hu/143_24_koronvary_2.pdf (2016.05.04)

[14] HÜLVELY LAJOS – KORONVÁRY PÉTER: Some Thoughts on 21st Century Challenges of Management Education and Practice, Hadtudományi Szemle 5, pp. 190–195. (2012)

[15] DR. SZEGEDI PÉTER: Egy non-profit szervezet értékeinek közvetítése tömeg kommunikációs csatornákon keresztül, tanulmány a magyar honvédség hagyományainak, jelképeinek, tradícióinak, értékeinek közvetíthetőségéről, 2016 p.:80 ISBN 978–963–12–5258–3 Available at: https://ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10149/tanulmany2_szegedi_peter.pdf?sequence=1&isallowed=y (2016.04.20)

[16] KORONVÁRY PÉTER – SZEGEDI PÉTER: Repülőgép üzembentartó szervezetek humán erőforrásának tudásalapú fejlesztése, In: Békési Bertold, Szegedi Péter (szerk.), Repülőműszaki üzembentartó szervezetek működésével, fejlesztésével kapcsolatban Tanulmánykötet a BSc, MSc hallgatók számára. 82 p. Szeged: Magánkiadás, 2016. pp. 49-63. (ISBN:978-963–12–5621–5)

[17] BÉKÉSI BERTOLD – SZEGEDI PÉTER – SZABÓ VIVIEN – TÓTH JÓZSEF: How Terrorism Can Affect Technologycal Aspects of the Airport Security. Proceedings of 19th International Scientific Conference Transport Means 2015. Kaunas, Technologija, 2015.10.22-23., pp. 112-115. (ISSN: 1822–296X)

[18] BÉKÉSI BERTOLD – KORONVÁRY PÉTER – SZEGEDI PÉTER: Terrorism and Airport Security Some Technological Possibilities to Reduce Exposure, Deterioration, Dependability, Diagnostics International conference, Univer-sity of Defence, Brno, 2015. pp. 279–288. (ISBN: 978–80–7231–431–7)

[19] DR. KORONVÁRY PÉTER – DR. SZEGEDI PÉTER: Tudásalkalmazás és tudásgondozás, Hadmérnök, X. Évfolyam 2015/4, pp. 217–226. Available at: http://www.hadmernok.hu/154_20_koronvaryp_szp.pdf (2015.08.06)

[20] KORONVÁRY PÉTER– SZEGEDI PÉTER – TÓTH JÓZSEF: Kutatás és képzés – módszertani felvetések az elvárások és a képzési portfólió összehangolására a repülőműszaki képzésben, Hadmérnök, X. Évfolyam 2015/4, pp. 237–246 Available at: http://www.hadmernok.hu/154_22_koronvaryp_szp_tj.pdf (2015.08.06)

[21] KORONVÁRY PÉTER – SZEGEDI PÉTER: Thoughts on understanding our organizations, Hadmérnök X. 4. (December 2015) p. 227 Available at: http://www.hadmernok.hu/154_21_koronvaryp_szp.pdf (2016.04.29)

[22] SZEGEDI PÉTER: „ÖTLET! ... ROHAM!" egy „csináld és tanítsd" folyamat elindításához, a katonai felsővezető képzés lehetséges fejlesztési iránya, Hadmérnök,

IX. Évfolyam 2. szám - 2014. június pp.:400–408 Available at: http://hadmernok.hu/142_35_szegedip.pdf (2016.04.29)

[23] TÓTH JÓZSEF: A repülő műszaki tiszti kompetenciák kvalitatív vizsgálata. In: Békési Bertold, Szilvássy László (szerk.), Repüléstudományi Szemelvények, Nemzeti Közszolgálati Egyetem Katonai Repülő Intézet, Szolnok, 2016. pp. 177–196. (ISBN: 978-61-5057-70-0) Available at: http://www.repulestudomany.hu/kiadvanyok/RepSzem-2016.pdf (2016.03.29)

[24] TURCSÁNYI KÁROLY – SZEGEDI PÉTER – TÓTH JÓZSEF: A katonai repülőműszaki tiszti kompetenciák felmérése integrált kutatási módszerrel Repüléstudományi Közlemények, XXVIII. évf. 2. sz. pp.: 153–164 Available at: http://www.repulestudomany.hu/index_rtk.html (2016.04.29)

[25] TÓTH JÓZSEF: Компетентностный подход модернизации образования инженеров по эксплуатации современных летательных аппаратов, Repüléstudományi Közlemények, XXVIII. évf. 1. sz. pp.: 49–53 Available at: http://www.repulestudomany.hu/index_rtk.html (2016.04.29)

[26] SZEGEDI PÉTER – TÓTH JÓZSEF: Repülőgép üzembentartó szervezetek humán erőforrásának kompetencia vizsgálata kvalitatív módszerrel, In: Békési Bertold, Szegedi Péter (szerk.), Repülőműszaki üzembentartó szervezetek működésével, fejlesztésével kapcsolatban Tanulmánykötet a BSc, MSc hallgatók számára. 82 p. Szeged: Magánkiadás, 2016. pp. 64–82. (ISBN:978–963–12–5621–5)

[27] TÓTH JÓZSEF: Considerations On Modernization And The Competencies And Education Of Aircraft Maintenance Engineers, Hadmérnök XI:(1) pp. 294–299. (2016) Available at: http://hadmernok.hu/161_28_tothj.pdf (2016.04.29)

[28] TURCSÁNYI KÁROLY – SZEGEDI PÉTER – TÓTH JÓZSEF: Определение компетенций офицеров авиационных инженеров, Repüléstudományi Közlemények (1997-től) (3) pp. 7–14. (2016) Available at: http://www.repulestudomany.hu/index_rtk.html (2016.04.29)

[29] TOMCSÁNYI PÁL: Általános kutatás módszertan, Szent István Egyetem, Gödöllő, Bp. 2000, ISBN: 963 86097 0 2

[30] KORONVÁRY PÉTER: Az amerikai „military leadership” elmélet rendszertana (PhD értekezés) Zrínyi Miklós nemzetvédelmi Egyetem, Hadtudományi Doktori Iskola, Budapest, 2008.