HADMÉRNÖK

A ZMNE BOLYAI JÁNOS HADMÉRNÖKI KAR
ÉS A HADMÉRNÖKI DOKTORI ISKOLA
ONLINE TUDOMÁNYOS KIADVÁNYA

VI. Évfolyam 3. szám 2011. szeptember

ZMNE
BUDAPEST

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

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

Jelen számban megjelent írások szerzői:

Boldis Ottó – MH Dr. Radó György Honvéd Egészségügyi Központ

Csépainé Széll Pálma – ZMNE

Gachályi András – MH Dr. Radó György Honvéd Egészségügyi Központ

Faggyas Zoltán – Belügyminisztérium

Faragó László – Kaposvári Egyetem

Fleiner Rita – ZMNE HMDI doktorandusz

Dr. Földi László mk. alezredes – ZMNE BJHMK egyetemi docens

Horváth Tamás – MVM Zrt.

Karvaly Gellért – MH Dr. Radó György Honvéd Egészségügyi Központ

Kocsis György – MH Dr. Radó György Honvéd Egészségügyi Központ

Kuris Zoltán – ZMNE HMDI doktorandusz

Lasz György – ZMNE KMDI doktorandusz

Dr. Lázár Gábor – ZMNE

Mátyus Mária – MH Dr. Radó György Honvéd Egészségügyi Központ

Prof. Dr. Munk Sándor ny. mk. ezredes – ZMNE BJHMK egyetemi tanár

Dr. Resperger István ezredes – ZMNE

Pataki János – ZMNE HDI doktorandusz

Dr. Sulányi Péter – Suprex kft.

Répás József – ZMNE BJHMK hallgató (MSc)

Szatmári-Juhász Ditta – ZMNE

Tamási Béla mk. ezredes

Vízi Pál Gábor – ZMNE HMDI doktorandusz

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Horváth Tamás
tamhorvath@mvm.hu

KÁBELEK, HÁLÓZATOK, CCTV RENDSZEREK

Absztrakt

Biztonságtechnikai megfigyelő rendszerek egyik legfontosabb építőeleme a rendszer alapvető jeltovábbítását biztosító kábelhálózatok. A fizikai kábelek jelentősége a biztonságtechnikában továbbra sem csökken annak ellenére, hogy a vezetéknélküli megoldások újabb és újabb verziói jelennek meg, de az egyedi, dedikált kábelezéssel kialakított hálózatok biztonsági kockázata lényegesen kisebb, mind a rádiótechnikai megoldásoké. A kiemelt biztonsági kockázatú létesítményeknél, esetleg nehéz műszaki körülmények esetében az optikai kábelek jelentenek megoldást.

Cable network systems are the most important parts of the security surveillance systems which provide the essential signal transmission tasks. Values of cables them selves can not be decreased in spite of appearing new versions wireless solutions. Anyway the security risks of dedicated cable solutions are lower substantially comparing to implementations of radio technology based ones. At high security-risk facilities or in case of difficult technical conditions the fiber optic cables provide the proper solutions.

Kulcsszavak: *kábelhálózatok, dedikált kábelek, vezetéknélküli, optikai kábelek ~ cable networks, dedicated cables, wireless, fiber optic cables*

KÁBELHÁLÓZATOK, ÉS KÁBELNÉLKÜLI MEGOLDÁSOK

Az analóg CCTV rendszerekhez hasonlóan az IP alapú biztonságtechnikai CCTV rendszereknél a megépítendő kábelhálózat rendszertechnikailag alapvető fontossággal bír. Az analóg rendszereknél korábban az RG59U (75 Ω impedanciájú, árnyékolt kábel, sűrű szövésű réz árnyékoló harisnyával) kábel volt használatos, ma már szinte teljes egészében az csavart érpáras hálózati kábel (UTP kábel: 2x2x0,4) felhasználása terjedt el.

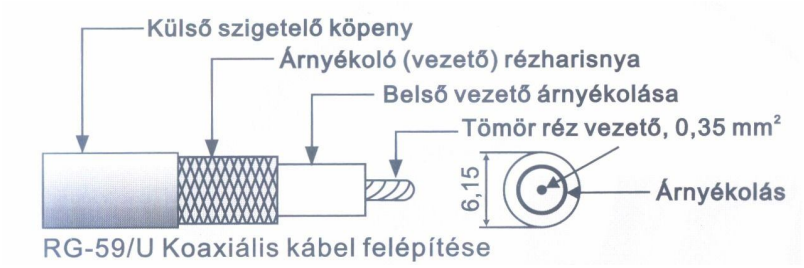
ANALÓG RENDSZEREKNÉL HASZNÁLHATÓ KÁBELHÁLÓZAT, ILLETVE KÁBELNÉLKÜLI MEGOLDÁSOK

Analóg biztonságtechnikai video megfigyelő rendszereknél használható kábelhálózatokat felépíthetjük [1]:

- Koax kábel
- UTP kábel
- Optikai kábel
- Kábelnélküli megoldások

Koax kábel használata

Az árnyékolt kábel használatának nagyon nagy múltja van a videó jelek továbbításban. A biztonságtechnikai videó rendszereknél néhány évvel ezelőtt szinte kizárólagos megoldás volt. Gondos csatlakozó szereléssel, jó minőségű BNC[1] csatlakozók esetén megbízható megoldás volt. (Megjegyzés: szakmai tapasztalatom szerint az elmúlt években, az árharc negatív hatása is megjelent a csatlakozók beszállítóinál, szinte használhatatlan BNC csatlakozók kerültek a piacra, melyek biztonságos, kontakthiba-mentes szerelése szinte lehetetlen volt.)



1. ábra. Árnyékolt kábel

Kisméretű rendszerek esetében még ma is alternatíva lehet a koax kábelek telepítése, bár napról napra szorul ki a telepítők kínálatából. Nagyméretű rendszereknél mér jelentős kábelköltségekről beszélhetünk, annak ára jelentősen befolyásolhatja a költségvetésünket. Napjainkban az UTP kábel ára, amely még a szükséges illesztőegységekkel is olcsóbb lehet nagyobb méretű rendszereknél, mint a hagyományos árnyékolt kábellel kivitelezett hálózat.

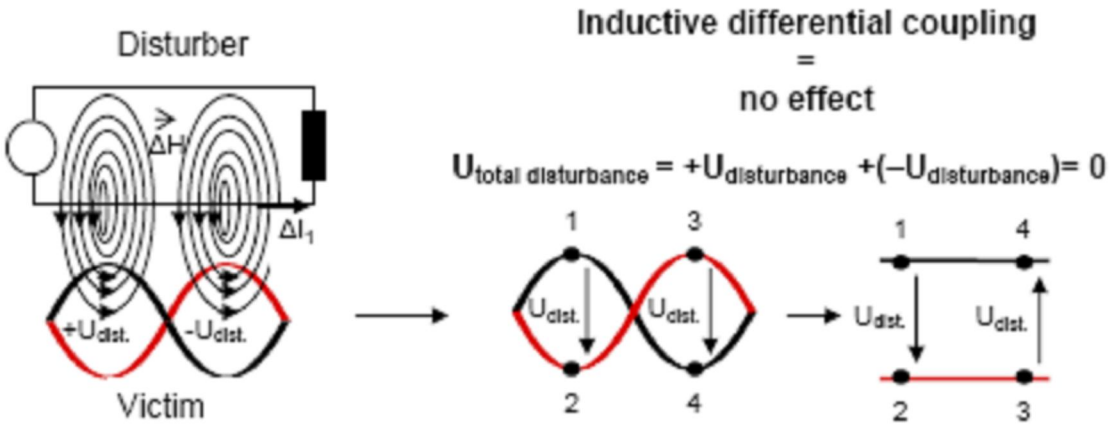
[1] BNC csatlakozó: a videotechnikában használatos csatlakozó fajta.

UTP2 kábelek az analóg CCTV rendszereknél

Csavart érpár [1] felhasználása a biztonságtechnikai CCTV rendszereknél rendkívüli módon elterjedt az elmúlt évtizedben. Az UTP kábel műszaki paraméterei, elsődlegesen az ér párak sodrási sűrűségétől függő sávszélesség, amely teljes egészében megfelel a videotechnikai igényeinek. A ma használatos kábelek több, általában 4 érpárból állnak, amelyek spirális formában meg vannak csavarva, ezáltal csökkentve az érpárok közötti esetleges interferenciát. Az erek mindegyike egyenként szigetelve van, de az érpárok lehetnek még páronként árnyékolva is, bár ez az analóg videotechnikai alkalmazásokban nem kívánatos (Az árnyékolás problémát okozó kapacitást vihet a hálózatba). A sávszélesség a huzalok vastagságától és az áthidalni kívánt távolságtól függ, de akár a Gbit/s-os nagyságrendű sebesség is elérhető.

2. ábra. UTP kábel érpáranként színezett kábelekkel

A kábelek zavarvédettsége működését magyarázó 3. ábra mutatja, hogy a kábel környezete által indukált zavarjelek a kábelpárok sodrás miatt, adott vizsgált pontokon ellentétes fázisban vannak, így azok egymást kioltják a kábelpár teljes hosszában.



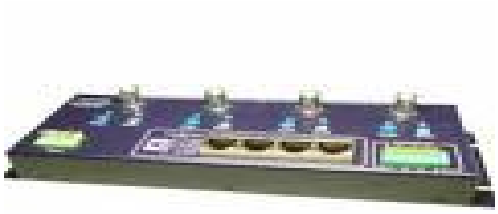
3. ábra. Sodrott érpáras kábel zavar elleni védettsége magyarázata[3]

Tekintettel arra, hogy sávszélesség probléma nem okoz műszaki nehézséget, az érpárak közötti interferencia sem nehezíti az átvitelt, így a helyes impedancia illesztést kellett megoldani, amely az erre a célra kialakított illesztő transzformátorokkal minden tekintetben kivitelezhető.

A konverterek [2] között passzív (az illesztő transzformátoron kívül egyéb elemet nem tartalmaz), és az aktív (az impedancia illesztés mellett erősítőket is tartalmaz) kialakítással is találkozhatunk, mely az UTP kábellel áthidalható távolság (1,0 - 1,5 km) megnövelésére szolgál. (Megjegyzés: természetesen ilyen méreteknél a tervező nem feledkezhet meg a

[2] UTP kábel: Unshielded Twisted Pair, azaz nem árnyékolt csavart érpár
[3] A. Klauser: WARP-The UTP technology 10GBASE-T, Letöltve: 2011.03.18.

túlfeszültség esetleges káros hatásairól, mivel egy ilyen méretű kábel antennaként képes működni egy-egy villámcsapás esetén, amely rajta indukálódott feszültség révén, mint másodlagos tranziens, a csatlakoztatott eszközöket tönkreteheti.)

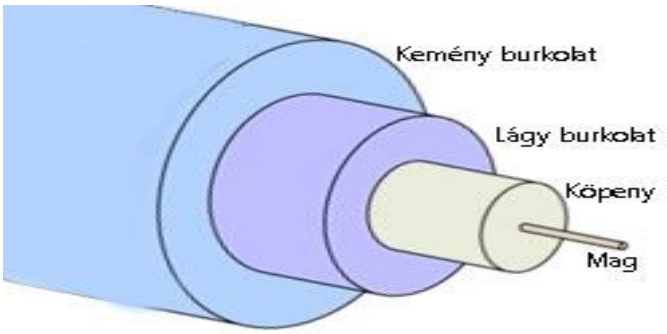


4. ábra. UTP konverter 4 koax kábelhez

Videojel átvitel optikai kábelen

Napjainkban legjobb, leginkább zavarvédett, legnagyobb sávszélességet biztosító átviteli forma, amely a biztonságtechnikában további előnyt garantál a felhasználók számára: az optikai szálon folyó kommunikáció a kábelen nem hallgatható le.

Optikai hálózat kiépítésére [1] akkor kerül sor, ha különösen nagy elektromágneses hatások érhetik a vezetékeket, vagy nagy távolságokat kell áthidalni.



5. ábra. Optikai kábel felépítése4

Mag: 62,5 µm; Köpeny: 125 µm; Lágy burkolat: 250 µm; Kemény burkolat: 400 µm

A továbbítandó információt fényimpulzusok szállítják az adó és vevő oldal között. Az áthidalható távolság 80 km lehet. Ennél a átviteli módnál a jelátviteli közeg alapvetően három részből áll:

- Optikai szál - Üvegszál, vagy szilikát szál
- Adó oldal - Fényforrás (LED, vagy Laser[5] dióda)
- Vevő oldal - Fényérzékelő elem (fotodióda)

Az optikai kábel fizikai működése lényege az, hogy a fénysugár különböző közegek határán más-más módon törik meg, illetve verődik vissza. A fénytörés mértéke a két közeg tulajdonságaitól függ. Amennyiben jeltovábbítást végző fény, az üvegszál belépési felületén, egy adott kritikus belépési szöget túllép, akkor a fénysugár az üvegszálból kilépve halad tovább. A kritikus szögnél kisebb beesési szöggel érkező sugarak a szálon belül maradnak. Az

4 Letöltve: http://netpedia.hu/optikai-kabel 2011.06.21.

5 Laser dióda: olyan félvezető elem, amely csak egy meghatározott hullámhosszúságú fényt bocsát ki.

optikai szálakban a gyakorlatban használatos átvitel módja: a *multimódusú* (átmérő: dm>10λ - gradiens, illetve lépcsős szál), és a *monomódusú* (átmérő: 2λ<dm<10λ)6 szál.

Monomódusú jelátvitel

A monomódusú optikai szál (fizikai mérete 9/125 μm) mérete az átvitelre használt fény hullámhosszával összemérhető, akkor a fényhullám nem képes az optikai szál teljes hosszában kilépni a fényvezetőből, így az visszaverődések nélkül, egyenes vonalban (követve az optikai szálat a telepítés vonalában) és egy módus alakul ki.

Monomódusú optikai szál meghajtásához az ehhez a rendszerhez tervezett, és gyártott eszközök szükségesek, melyek ára jelentősen meghaladják a multimódusú rendszerekhez gyártott interfészekét. A kábel meghajtásához laser-dióda kell. Nagytávolságú átvitelre (50-80 km) zavarvédett, nagy sávszélességet biztosító megoldás. A biztonságtechnikában ezt a fajta átvitelét igen ritkán, vagy soha nem használjuk, helyette a lényegesen olcsóbb, és kisebb, de az igényeknek teljes egészében megfelelő multimódusú optikai átvitelt alkalmazzák.

Multimódusú jelátvitel

A multimódusú szál (fizikai mérete: 50/125 μm, illetve 62,5/125 μm) több frekvencián is képes a jeltovábbításra. A jelenleg kapható multimódusú optikai szálak az igen gyakran használt 850 nm-es hullámhossz esetén 1 km-es távolságon, 4-5 dB-t csillapítanak.

„Multimódusú optikai szál jelátvitele esetében az egyik legfontosabb csillapítást előidéző jelenség a diszperzió. A tökéletes optikai szál kimenetén teljesen ugyanazt a jelformát kapnánk vissza, mint amit a bemeneten rákapcsoltunk. A valóságban azonban az optikai kábel hosszától és egyéb paramétereitől függően a beadott jel kissé "elkenődik", sávszélessége megnő, hossza bizonytalanná válik. Ez a jelenség a diszperzió, ami leginkább gátat szab az alkalmazható frekvencia magasságának és az áthidalható távolságnak. A diszperzió három fő forrásra vezethető vissza. Az egyik a módus diszperzió, ami multimódusú szálakban lép fel és a különböző hosszúságú terjedési utakkal magyarázható. A másik az optikai kábel anyaga által okozott diszperzió, mely az eltérő frekvenciákon jelentkező eltérő késleltetési paraméterekből adódik. A harmadik a hullámvezetési diszperzió, ami abból adódik, hogy az optikai kábel magrésze mellett a magot körülvevő borítás is vezeti a fényt az egymódusú szálak esetében…”[7]

A biztonságtechnikai video megfigyelő rendszernél a multimódusú optikai kábelek telepítése a gyakorlat, mivel az egy objektumon belüli kábelhossz ritkán haladja meg a 4-5 km hosszúságot. A kábel hálózat kiépítése során az egyes toldások, hegesztések, csatlakozók mind-mind az Optikai Budget (a rendelkezésre álló optikai keret[8]) terhére mennek, azaz csillapítják az átvinni kívánt optikai jel szintjét. Az optikai szál hegesztése okozza a legkisebb veszteséget, amely gyakorlatilag 0 dB csillapítást jelent, míg egy-egy csatlakozó (főként a szerelési technológia nem pontos betartása esetén) már jelentősebb, mintegy 0,25 dB csillapítást okoz, de a csillapítás akár 2-3 dB is lehet, amennyiben a szerelés nem szakszerű a hálózaton.

A tervezés során az egyes rendszer elemek katalóguslapjából pontos adatokat kaphatunk az adott egység optikai kimenete teljesítményére, így az átviteli lánc teljes ismeretével az optikai kábel vevőoldalán megjelenő jelszint számítható.

---

[6] Átvéve: http://www.mht.bme.hu/~lenart/Vill_A344/Op.pdf (Letöltve: 2011.06.11.)

[7] Szövegszerűen átvéve: dr Bartolits István: Optikai kábel alapfogalmak (Modern kor kisszótár LIX) Letöltve: http://e-times.hu/01szept/kisszot.htm

[8] Optikai keretnek nevezzük azt jelszint tartalékot, melyet a hálózatépítés során a rendszer még jelveszteség nélkül elvisel.

Kábelnélküli átvitel

Analóg biztonságtechnikai CCTV rendszereknél a kábel nélküli jelátvitel [1] természetesen létező megoldás. A piacon több gyártó, különböző átviteli metódust (analóg, digitális, diversity[9] analóg, vagy digitális, stb.) alkalmazó berendezése megtalálható. A használható megoldások nem olcsóak, mivel a sávszélesség biztosítása mellett a rádiótechnikai zavarmentességet is meg kell oldani. Ezen felül a biztonságtechnikai szakmában dolgozóként megjegyzem, nem kedveljük azokat az átviteli módokat, amelyek nem nehezítik a lehallgatás lehetőségét, ezért csak a megfelelő titkosítással rendelkező rádiótechnikai átvitelt lehet elfogadni, mind átviteli megoldást. Tekintettel a fejlődési irányokra, néhány kivételtől eltekintve, a kábelnélküli jelátvitel a digitális jeltovábbítás nagy jelentőségű módszere.

A rádiófrekvenciás kábelnélküli megoldások[2] mellett léteznek infra tartományú, valamint lézeres kivitelű jelátviteli rendszerek. Mindkét rendszer esetén adó-vevő oldalak kiépítése szükséges. Az előnyük a nehéz lehallgathatóság, de igen nagy hátrányuk az időjárási körülmények (köd, szennyezett légkör, csapadék) zavaró hatása nehezen kompenzálható.

DIGITÁLIS RENDSZEREKNÉL HASZNÁLHATÓ KÁBELHÁLÓZAT, KÁBELNÉLKÜLI MEGOLDÁSOK

Digitális, IP alapú biztonságtechnikai video megfigyelő rendszereknél használható kábelhálózatokat felépíthetjük:

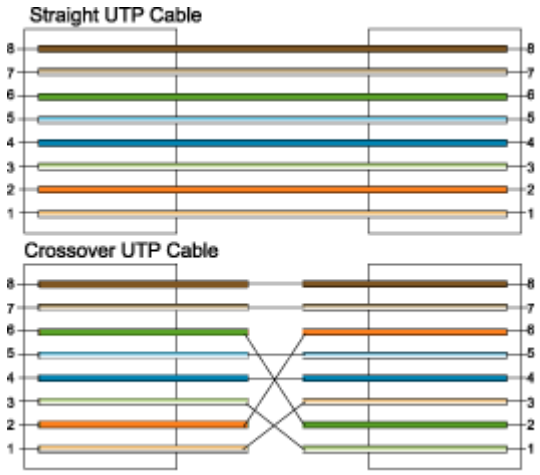
- UTP kábel
- Optikai kábel
- Kábelnélküli megoldások

UTP kábelek IP alapú CCTV rendszereknél

UTP kábelek felhasználása az IP alapú CCTV rendszereknél semmiben nem különbözik a számítástechnikában alkalmazott hálózatokban felépítettetektől, mivel a kábelhálózat telepítésekor informatikai hálózatot kell telepíteni. Ennek megfelelően az adatátvitelre használt kábelezés, topológia, a felhasznált rendszer-elemek a számítástechnikában használt elemek. Nagy épületeknél, irodaházaknál önálló kábelhálózatot nem is kell kiépíteni, mivel az informatikai végpontok az egyes épületek gyakorlatilag valamennyi helységében megtalálhatóak.

Az egyes kamerák bekötésénél a szabványos soros Ethernet kábel bekötést [3] kell alkalmazni. Az *IEEE 802.3* szabványgyűjtemény, ami az IEEE szabványokkal meghatározott, és Ethernet kábelezést használó fizikai rétegnek és adatkapcsolati rétegnek a megvalósításait írja

[9] Diversity kábelnélküli rendeszek esetében a vevők (a diversity rendszer adója jeleit figyelve) több vevőegységet, ennek megfelelően több antennát használnak, és a legjobb vételt biztosító antennára kapcsolnak át automatikusan.



6. ábra UTP kábelek bekötése[10]

Biztonságtechnikai CCTV rendszerek esetében a kameraoldali bekötés megfelel az ún. „ Straight UTP Cable" egyenes UTP kábel bekötésnek, mivel az Ethernet által használt érek (1,2,3,6) egy aktív eszközre csatlakoznak. (Megjegyzés: A „Crossover UTP Cable" – fordított kábel bekötés ismerete is fontos a szakember számára, mivel egy-egy informatikai aktív eszköz, így az IP kamera is, közvetlenül egy számítógépre csak így kapcsolható. A szakmában igen gyakran kell az egyes elemeket beállítani, mielőtt azt rendszerbe kötnénk. A dolgozatomnak nem témája az informatikai hálózatok konfigurációja, de azt a biztonságtechnikai szakembernek ismernie kell, mivel az egyes rendszerelemek csak azonos IP tartományban látják egymást, azaz képesen a kommunikációra egymás között.)

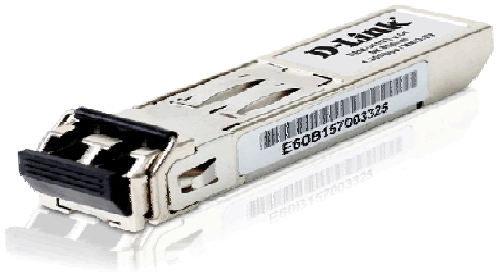
Digitális IP alapú kamerák videojelei átvitele optikai kábelen

Az IP alapú biztonságtechnikai rendszer telepítése egyik nagy előnye éppen az, hogy meglévő számítógépes hálózat (Ethernet) használata során semmilyen különbség nincs arra tekintettel, hogy az átvitt jelek milyen információtartalommal bírnak. Így ebben a témakörben az informatikai hálózatok optikai építőelemiről szeretnék szólni néhány mondatban.

Némiképp más megoldásokat találunk az informatikai hálózatok optikai adatátviteli egységei kialakításánál, mint az analóg eszközöknél. Az optikai interfész igen gyakran opcionális része az ún. Gigabit-es hálózati kacsolónak [3] (valamennyi port 1000BASE-T, azaz 1 Gbit/sec adatátviteli sebességre képes), melynél 1, vagy 2 portot egy, vagy két ún. combo SFP (Small Form-factor Pluggable - Optikai Átviteli Modul) mini GBIC (**G**iga**B**it **I**nterface **C**onverter) modul segítségével „full duplex"[11] üzemmódú (2 db LC[12] csatlakozós optikai kábel szükséges) optikai port-tá lehetséges átalakítani. (Megjegyzés: Természetesen létezik ún. Média Interface[13], amely 1 Gbit/sec ún. „réz" és egy full duplex optikai prottal rendelkezik. Ez akkor használható, ha nincs szükségünk egy komplett hálózati kapcsolóra.)

Az egyes mini GBIC egységeknél, a kisebb távolságoknál, nem mindig adják meg az ún. Optikai keret értékét, mint az adott modul kimeneti jelszintjét, hanem a felhasználási lehetőségét határozzák meg a katalógusokban. Ennek megfelelően létezik többek között mini GBIC modul (D-Link DGS-700 sorozat):

10 Letöltve: http://www.wahsiu.com/network/sharing/utp.gi f 2011.03.19.
11 „Full duplex" üzemmód egy adatátviteli eljárás, mely során egy időben, teljes sávszélességgel, mind a adás és vétel irányban működhet az átvitel.
12 Optika átviteli egységekben használt speciális csatlakozók egyike.
13 Media Interface: egy olyan átalakító, amely az átviteli közegek közötti kapcsolatot biztosítja.



7. ábra. Mini GBIC optikai modul

- MM (Multi Modusú) modul 100 m-ig
- MM (Multi Modusú) modul 550 m-ig (Optikai keret: 7,5 dB)
- SM (Singe Modusú) modul 10 km-ig (Optikai keret: 10,5 dB)
- SM (Single Modusú) modul 30 km-ig (Optikai keret: 18 dB)
- SM (Single Modusú) modul 70 km-ig (Optikai keret: 23 dB)

A biztonságtechnikai gyakorlatban az a kívánatos, ha az optikai kábel teljes hosszán 1-2 hegesztés, és 1-2 csatlakozó felszerelésére kerül sor. Ezek a modulok ezeket a veszteségeket gond nélkül elviselik. Minden egyéb toldást, csatlakozó felszerelést már számítással ellenőrizni kell a szükséges optikai tartalékot az üzembiztos működéshez.

Biztonságtechnikai alkalmazásnál célszerűen használható olyan optikai kábel, amely az optika patch modulban a kifejtésnél közvetlenül ST14 csatlakozó szerelhető, így mérsékelve a további hegesztési költségeket, illetve az optikai keret további csökkenését.

Kábelnélküli - WLAN – átvitel [3]

Informatikai hálózatok esetében az egyik legfontosabb hálózatkialakítási, illetve kapcsolódási forma a ma már közismert WLAN[15] (Wireless Local Area Network). Biztonságtechnikai CCTV rendszerek esetén a WLAN hálózatok használta igen nagy rugalmasságot biztosít mind a tervező és kivitelező, mind az üzemeltető részére. Meglévő hálózat bővítése egy jól megtervezett helyen telepített Access Point-tal[16] a meglévő IP alapú CCTV rendszerünk bővítése megoldható. Ezen a ponton a hálózatfejlesztéshez szükséges sávszélesség számítás igen nagy jelentőségűvé válik. Nem pontos, vagy helytelen kalkuláció esetén előfordulhat, hogy a telepítésre szánt kamera (annak paramétereitől, és beállításától függően) által biztosított video stream nem lesz képes, nem lesz képes folyamatosan, eljutni a DVR-hez, mert a hálózat túlterheltsége miatt egyre több, és több lesz az ún. csomagütközés, amely jelentősen lelassítja a hálózat adatforgalmát.

A gyakorlati tapasztalatom az, hogy 35-40%-os hálózati terheltség már képes csomagütközésekkel lelassítani a hálózatot. Különösen nagy figyelmet kell fordítani a sávszélesség számításra abban az esetben, ha több megapixeles kamerát, teljes felbontásban szeretnénk használni.

A tervezőnek kiemelt figyelmet kell fordítani arra tényre, hogy biztonságtechnikában nem képzelhető el a titkosítás nélküli adatforgalom. A titkosítás, mind hozzáadott csomagoló protokoll további sávszélesség igénnyel lép fel, tehát az adott IP kameránk elhelyezése, a

14 Az ST (Straight Tipp) csatlakozó egy optikai csatlakozót használó egy dugasz és foglalat, amely egymáshoz egy fél csavar fordulattal működő bajonett zárral kapcsolódik.

15 WLAN – kábel nélküli helyi hálózat, mely lehetőséget ad arra, hogy a helyi hálózatunkhoz kábelezés nélkül csatlakozhassunk.

16 Access Point – Hozzáférési Pont -: ahova a WLAN kompatibilis eszközök csatlakozhatnak a hálózatra.

WLAN kapcsolat kialakítása, a megfelelő titkosítás beállítása mellet is a hálózatunk sávszélessége elegendő legyen. (Megjegyzés: Ez a probléma nem akkor következik be, ha van egyetlen egy kameránk egy hozzáférési ponton, hanem akkor, mikor egy Access Point-ra több IP kamrát regisztrálunk be, és nem számítjuk ki pontosan igényeket, a rendelkezésre álló sávszélesség nagyon gyorsan elfogy.)

ÖSSZEGZÉS

A video megfigyelő rendszerekben használható jelátviteli megoldásokat áttekintve ismét megbizonyoshadtunk arról, hogy komplex rendszerek, komplex megoldásokat igényelnek. Kábelek használatát nem lehet megkerülni sőt, egyre inkább az optikai szálas megoldások kerülnek előtérbe, melyek napjainkban már gazdaságossági szempontokból is kiváló lehetőséget biztosítanak.

Egy másik szempont, amely kiemelt szerepet kell, hogy kapjon: a szakmai továbbképzés, amely nem megkerülhető a biztonságtechnikai iparban tevékenykedők számára sem. Ehhez elegendő a kábel hálózatok fentebb felvetett műszaki paramétereire gondolni.

Felhasznált irodalom

[1] Tóth Levente: CCTV magyarul (Kiadó: BM Nyomda Kft., 2004)

[2] Herman Kruegle: CCTV Surveillance Video Practice and Technology Second Edition (Kiadó: Elsevier Butterwoth-Heinemann, 2007)

[3] Andrew S. Tanenbaum: Számítógép hálózatok

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Horváth Tamás
tamhorvath@mvm.hu

KORSZERŰ KERÍTÉSVÉDELEM

Absztrakt

Az elektronikus behatolás-jelző rendszerek egyik legtöbb figyelmet, leggondosabb kiválasztást, és telepítést igénylő eszközei a kerítésvédelmi rendszerek. Kiemelten fontos a megfelelő jelzéstechnológia kiválasztása egy adott kerítéshez készített vagyonvédelmi terv elkészítésekor. A biztonságtechnikai piacon több kerítésvédelmi rendszer megtalálható, melyek érzékelő technológiákban, jelfeldolgozásban, és nem utolsó sorban szelektivitás tekintetében igen eltérőek.Az elektronika, a jelfeldolgozás gyors fejlődése a kültéri védelemben is jelentős változásokat hozott, így a nagybiztonságú kerítésvédelmi megoldások jelentős támogatást képesek biztosítani akár a nagy biztonsági kockázatú létesítmények, objektumok védelmében, miközben alkalmazásukkal lehetőség nyílik a gazdaságosabb védelmi rendszerek telepítésére.

The perimeter protection systems are the essential parts of electronic intrusion systems which do require the most attention and carefully selection. The highly important activity is to sort out the proper signal processing technology for the security perimeter protection plan. A few of fence protection system can be found in the security market which do contrast strikingly with sensor technology, signal processing and at last but not at least in signal selectivity.
The rapid development of electronics and signal processing have brought significant changes in all parts of the security industry so the high-secure-requirement facilities and objects can be supported by the most sophisticated perimeter protection systems while the economy point of views could be taken in to consideration.

Kulcsszavak: *kerítésvédelmi rendszer, szelektivitás, nagy biztonságú, gazdaságos ~ perimeter protection system, selectivity, sophisticated, economy*

SZELEKTIVITÁS A KULCS

A rendszer szelektivitása igen fontos paraméter a kerítésvédelmi rendszerek esetében is, mivel az egyes jelzések kialakulásának pontos helye ismerete, főként egy integrált rendszer esetén, amikor a területvédelemre telepített biztonságtechnikai CCTV rendszer adott Speed Dome kamerái a jelzést adó érzékelőkre tudnak fókuszálni (pontosan konfigurált un „preset" állapotok), jelentősen befolyásolhatja az élőerős védelem létszámát, felszereltségét, és nem utolsó sorban az adott védett objektum biztonsági szintjét.

Egy esetleges rosszindulatú behatolás pontos helyének meghatározása, megfelelő képkivágás előzetes beállítása („preset" programozások) mind az élőerős védelem, valamint a nyomozóhatóságok részére rendkívül hasznos lehetőség. A megfelelő szelektivitás az un vakriasztások értékelése szempontjából is kiemelkedően fontos műszaki paraméter.

Biztonsági vállalkozások megrendelők által generált igényei, a piaci verseny, és nem utolsósorban különböző állami feladatok a technológiai fejlesztésekre nagyszerű hatással vannak. Többek között ezen kihívásoknak akartak megfelelni a fejlesztők, amikor megalkották a „jel visszaverődéses technológiára" alapozott kerítésvédelmi rendszerüket, mely alkalmazásával, a napjainkban beszerezhető berendezések tekintetében kiemelkedően jó +- 10 m-es jelzés szelektivitás érthető el.

A BERENDEZÉS KIALAKÍTÁSA

A gyártó, az izraeli EL-FAR [1] részvénytársaság, elsősorban speciális állami igényeknek megfelelően kialakított rendszere tervezésekor a legfontosabb peremfeltétek az alábbiak voltak:

- Egyszerű, és hosszú élettartamú érzékelők gyakorlatilag bármilyen időjárási körülményekre
- Kiemelkedően jó jelzés szelektivitás
- Lehető legkevesebb vakriasztás
- Bővíthető legyen
- Önállóan, és hálózatban is működésképes legyen
- Meglévő, jó minőségű kerítések esetében is használható legyen
- Rendkívül kis fogyasztás

A tervezés eredményeképpen megalkotott rendszer a VIPER (**VI**bration **PER**imeter Fence Sensor System) elnevezést kapta, mely valamennyi fentebb felsorolt követelménynek eleget tesz.

Érzékelők (Sensor Line)

Az érzékelők a gyártó saját fejlesztése eredményeképpen jöttek létre. Rendkívül egyszerű, megbízható működést az érzékelőbe integrált négy darab aranyozott elem egymástól független módon került elhelyezése, melyek a legkisebb mozgás esetén az érzékelő un transzfer karakterisztikáját megváltoztatja. Az érzékelő tokozata az UV sugaraknak ellenálló műanyagból készül, melyekre a gyártó 15 éves garanciát vállal. Bővítési igény esetén a bővítés helyén az érzékelő kábel bontható és a szükséges toldat beépíthető. A gyár egy teljesen megszerelt érzékelő vonalat szállít, az előzetes megrendelés alapján.

1. ábra. Felszerelt vibrációs érzékelő

Működési hőmérséklet tartomány:	-45OC - +85OC
Relatív páratartalom:	100%
Működési feszültség:	5 - 35 V
Áramfelvétel:	5 – 50 mA
Tokozás:	UV védett műanyag burkolat

Más típusú érzékelőkkel (ultrahangos, szeizmikus érzékelők, infra-sorompókkal a rendszer probléma nélkül bővíthető, javítva a kerítésvédelmi rendszer hatékonyságát.

Vezérlőegység (EF2000)

A vezérlőegység képes 2X750 m érzékelő vonal ellenőrzésére gyakorlatilag bármilyen időjárási körülmények között. Az elektromos fogyasztása 2,5 W. A kommunikációs interfésszel (EF1500) kábeles, optikai, vagy kábelnélküli technológiával tartja a kapcsolatot.

Működési feszültség:	12 V
Áramfelvétel:	0,2 A
Kimeneti impulzus amplitúdója:	5 V

Elektromos fogyasztás

A fejlesztés eredeti célja volt a rendkívül kis áramfogyasztás, mivel nem minden esetben könnyű az központi egységek tápellátása. A berendezés elektromos teljesítmény igénye 2,5 W. Az izraeli határvédelmi kerítés esetében a tápellátását un szolár cellákkal, valamint kisteljesítményű szélkerekekkel oldják meg, biztosítva a berendezés működését, valamint a szünetmentes tápegység akkumulátora töltését.

Interfész egység (EF1500)

A csatolóegység (kommunikációs interfész) biztosítja a kommunikációt a vezérlőegység (-ek) és a számítógépen futó program között, valamint biztosítja az érzékelő hálózat villámvédelmét 6,5 KA terhelésig. Kommunikációs protokoll RS232.

Működési feszültség:	90 – 230 Vac
Kommunikációs protokoll:	RS232
Kommunikáció az I/O egységgel:	szinkron (0,5 KHz)
Villámvédelem:	6.500 A max tranziens impulzus
Reagálási idő:	35 nsec

Működés – jelzésszelektivitás

A berendezés működése tekintetében az un jelvisszaverődésen (Reflected Wave Technology) alapul, azaz a központi egység minden ezred másodpercben (msec) egy un teszt

jelet küld végig a kiépített érzékelő vonalon, melynek az utolsó eleme ellenállással van lezárva, biztosítva a jól ellenőrizhető hurokáramot, illetve a szabotázsjelzéseket. Amennyiben az érzékelő rezgést észlel, megváltozik az átmeneti ellenállása, a tesztjel részben visszaverődik a megváltozott transzfer karakterisztika miatt, így a központi egységbe egy „válaszjel" érkezik, mely jel beérkezése, és a tesztjel kibocsátásának időkülönbsége a visszaverődéshelyéről ad meglehetősen pontos információt. A jelenleg alkalmazott technológia ± 10 m pontossággal képes megkülönböztetni a visszaverődések helyét, azaz a jelzésszelektivitás ± 10 m.

Az alkalmazott számítógépes program segítségével a teljes rendszer az adott helyszínre adaptálható. A software képes a védett terület térképét beillesztve a kezelőfelületbe, térképen jelezni a jelzett behatolás helyét a ± 10 m pontossággal.

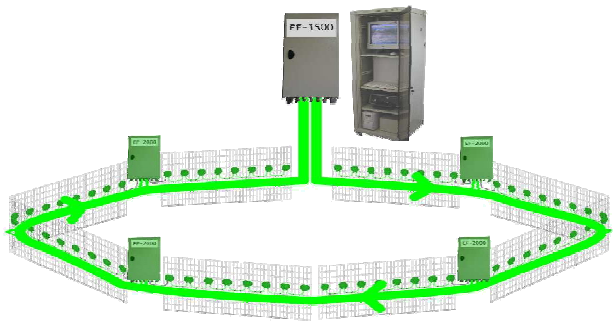
A központi egység a speciális csatolófelületen keresztül kapcsolódik a kiértékelő programot futtató számítógéphez. A kapcsolat lehet hagyományos módon kialakított rézkábeles, optikai, vagy a biztonságtechnikában csak korlátozott módon használható kábelnélküli.

Vakriasztások minimalizálása

A rendszer vakriasztásai minimalizálását a kerítéssel kell kezdeni. A kerítéselemeket nagy figyelemmel meg kell vizsgálni, és valamennyi meghibásodást (hegesztés elengedése, törések, stb.) ki kell javítani, a kerítésszerkezet állékonyságát, feszességét helyre kell állítani. Az így megjavított kerítésre (amennyiben erre egyáltalán szükség volt) már gond nélkül telepíthető a rendszer. A vakriasztások további minimalizálását a központi egységben telepített mikroszámítógép által végrehajtott algoritmusok végzik. Ezzel a módszerrel a széllökések (kb. 100 km/h sebességig) 80-90 százaléka probléma nélkül kiszűrhető.

Önálló és hálózatos működés

Egy berendezés telepítésekor a műszakilag még jól kezelhető jelzővonal hossz 2x750 m. Amennyiben ennél hosszabb kerítésvonal védelme szükséges az egyes központi egységek hálózatba köthetőek, így akár több tíz kilométer hosszú kerítésvédelmi rendszer is kiépíthető. A jelenleg ezzel a berendezéssel megépített, és üzemeltett leghosszabb kerítésvédelmi rendszer 12 km hosszú, határvédelmi feladatokat lát el Izrael területén.



2. ábra. Hálózatos működés

Telepíthetőség

A berendezés rendkívül könnyen telepíthető. Az adott, védeni szándékozott kerítéshez meg kell határozni az egy kerítéselemre felszerelni szükséges érzékelők számát, majd elkezdhető a munka. A jó műszaki állapotú kerítésre történő felszerelés probléma mentes. Amennyiben a védeni kívánt kerítés igen merev – kovácsoltvas kerítés -, az egy kerítéselemre 2 érzékelő felszerelése szükséges. Hasonló módon épületek homlokzatai is védhetőek a felmászás ellen,

melyhez hordozóként hegesztett rész kerítéselemek felszerelése szükséges a falakra, majd azokra kerülnek az érzékelők.

ALKALMAZÁS ELŐNYEI

- Meglévő, és új telepítésű kerítéseknél is használható
- Speciális konfigurálással műanyagból készült hálókerítés esetén sem kizárt a használat
- ± 10 m jelzés szelektivitás
- Rendkívül kevés alkatrész felhasználásával készült a rendszer
- Kiértékelő algoritmus biztosítja a rendkívül alacsony számú vakriasztást
- Bármilyen időjárási körülmények között használható ($-45^{O}C$ – $+70^{O}C$)
- Felhasználóbarát grafikus kezelői felület
- Egyszerű telepítés, és alacsony karbantartási költségek
- VIPER integrálható más, meglévő biztonsági rendszerekben

Minősítések

- ISO 9001:2000
- CE
- FCC
- Israeli Hadsereg minősítése (Israeli Army Certification)

ÖSSZEHASONLÍTÁS MÁS KERÍTÉSVÉDELMI RENDSZEREKKEL

	EL-FAR technológia	Mikrofon kábeles technológia	Optikai kábeles technológia	Feszített kábeles technológia	Piezo-elektromos technológia
Rendszer	TDR aktív	Passzív	Aktív	Passzív	Passzív
Telepítés és karbantartás	Egyszerű, de jól képzett telepítő szakember szükséges	Bonyolult	Nagyon bonyolult	Nagyon bonyolult	Bonyolult
Pontosság	±10 m	100-250 m	100 m	100-200 m	100-200 m
Élettartam	Nagyon hosszú	Közepes	Közepes	Közepes	Alacsony
EMI és RFI	Védett	Nagyon érzékeny	Közepesen védett	Közepesen védett	Nagyon érzékeny
Időjárásállóság	Program algoritmus	Meteorológiai egység	Ellenálló	Érzékeny	Meteorologiai egység
Költségek az élettartam alatt	Alacsony	Közepes	Magas	Magas	Közepes

1. táblázat. Összehasonlító táblázat

ÖSSZEGZÉS

Az EL-FAR által gyártott VIPER kerítésvédelmi berendezés a jelenleg kapható berendezés közül a legjobb, leghatékonyabb eszköz korszerű, magas biztonsági szintet igénylő behatolás-jelző berendezések kialakításhoz. Kiemelkedően jó a jelzéspontosság, mely a vezérlő és kiértékelő program segítségével akár térképes, akár fényképes felületen is megjeleníthető. Megbízhatósága, pontossága magas fokú integrálhatósága, speciális érzékelőkkel történő kiegészíthetősége a legjobb kerítésvédelmi megoldássá teszi.

ALKALMAZÁSI PÉLDÁK

1. kép. Határvédelmi kerítés (12 km)

2. kép. Kereskedelmi létesítmények védelme

3. kép. Repülőterek védelme (JFK)

4. kép. Nukleáris létesítmények védelme (Csehország)

5. kép. Athéni Olimpiai falu védelme

Felhasznált irodalom

[1] Advances Perimeter Security Systems
http://www.elfar.co.il

[2] VIPER – Advanced Perimeter Security System
http://www.elfar.co.il/index.aspx?id=3087

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Lasz György
georgelasz@gmail.com

TÖMEGRENDEZVÉNYEK ÉS BIZTOSÍTÁSUK
VÉDETT SZEMÉLY A TÖMEGBEN

Absztrakt

Korábbi publikációm és előadásaim során hitet tettem amellett, hogy: a legjobb gyakorlatot csak fejlesztéssel és fejlődéssel alakíthatjuk ki. Ez igaz az technikai innováció meghonosítására éppúgy, mint a tömegrendezvények gyakorlatának kialakítására.
A tömegek kezelése jelentős, nagy kockázattal járó feladat. A biztonság megőrzése, a megbomlott rend helyreállítása különösen azzá teszi. Az pedig, ha egy védett személy biztonságát kell garantálnunk egy tömegrendezvényen igazán kiemelkedő, de nem teljesíthetlen feladat elé állít minket.
Ezért is - cikkemet az elmélet és gyakorlat egyaránt írta.

In my previous publications and presentations I have expressed my belief that: the best practice could be formed by development and progress only. It is true in establishment of technical innovations, as well as in forming best practice.
The management of crowds is an important, high-risk task. Preserving safety and restoring breached order make the task especially so. And if we have to ensure the safety of protected person, it assigns a really big, but not impractical task to us.
My article - for this reason also, is written by both the theory and practice.

Kulcsszavak: *tömegrendezvény, magánbiztonság, rendezvénybiztosítás, védett személy ~ large-scale event, private safety, event security, protected person*

TÖMEGEK ÉS EGYÉNEK

Korábban is írtam arról, hogy a rendezvények biztosítása világos és követhető szabályozáson alapul. Ez azonban csak az egyik oldal. Ha a tömegrendezvény biztosításában résztvevő, az azt végző magánbiztonsági szolgáltató nem rendelkezik megfelelő humánerőforrással és infrastruktúrával, s ami a legfontosabb: helyzetre akklimatizált standardekkel, az komoly problémát jelenthet. Ezek az elméleti partíciók. S ekkor még nem szóltunk a biztosítások eredőjéről, a rendezvény apropójáról, az azon résztvevők intellektuális és szociális hátteréről, irányultságukról. E két oldal szerencsétlen találkozása vezethet a rendezvényen konfliktushoz, hiszen ha a rendezvény szélsőséges csoportjainak, személyeinek szándéka sikerre vezetett, mert a rendezvény nyugalmát megzavarva részben vagy egészben -célt ért szándékuk. Ez azonban még nem a biztosítás kudarca s nem is elméleti probléma...[1]

A rendezvények alatt a tömeg a százastól a százezres nagyságrendig változhat, de mindegyik esetben javasolt a tömeg menedzsment és annak biztosítása, hogy a biztonsági őrök állandóan ott legyenek, és a tömegben rejtőzködő lehetséges elkövetők elrettentőiként működjenek, vagy tartsák fenn a rendet, ahol a fenyegetés vagy verekedés fordulhat elő. A rendőrök kötelességei között van a tömeg menedzsment, az olyan elektronikus biztonsági rendszer működtetése, mint a zártláncú videómegfigyelés vagy a belépési ellenőrzés, a parkolás kezelése és általános ellenőrzési feladatok. A biztonsági személyzet fizikai jelenlétet is nyújt, és fontos része a segítséget és információt igénylő közönség felhívásának. Emellett alapvető szerepet töltenek be a rendezvény egészségének és biztonságának biztosításában és irányítják a sokaságot a vészhelyzetekben.[2]

Nemrég e folyóirat hasábjain is írtam róla, hogy a rendezvények bizonyos, nem elhanyagolható csoportjánál a tömegek lélektana meghatározó, a konfliktusok[3] alapja, a biztosítás oka a tiltakozás, az ellenvélemény különböző energiájú közlése. Ismeretesek „Ulrich Beck[4] gondolatai is korábbról, aki úgy véli, hogy az anonim rizikóeloszlás struktúráinak változásai nyomán a modern "rizikótársadalmakban" a civil társadalom éltre hívja a "blokád" jelenségét, amelyben ugyan nem képes rá, mégis megkísérli a struktúrák kedvezőtlen alakulásának korrigálását, vagy legalábbis a problémák tiltakozásként szignalizált közvetítését a modern társadalmak szükségképpen átpolitizált struktúráiban "mindenhatóvá" és "mindenütt jelenvalóvá" váló politikai centrumokhoz.[5] Azonban a biztonsági intézkedéseknek az ilyen rendezvényeken határozottnak és komolynak, de nem túlságosan beavatkozónak kell lenniük, hogy biztosítsák a rendezvény résztvevőinek és a személyzet védelmét, anélkül, hogy tönkre tennék a nézők élményét. A BSIA területei mindegyikének - mint a tömeg menedzsment (Crowd Management), a Rendőrségi és Közszolgálatok (Police and Public Services), a Biztonsági Őrködés (Security Guarding), Belépési Ellenőrzés (Access Control), Személyvédelem (Close Protection) és a CCTV (Closed-circuit Television)-

[1] GYENES Levente (2003): Biztonságvédelmi kézikönyv. KJK-KERSZÖV Jogi és üzleti kiadó Kft., Budapest, 2003. ISBN 9632245539

[2] KELLY, JAMES, a Brit Biztonsági Ipari Szövetség (Britsh Security Indusrty Association-BSIA) vezetője, a nagy létszámú rendezvények biztonsági stratégiájának kihívásairól és szervezőiről adott riportotjban. Forrás itt: http://www.counterterrorbusiness.com/features/93-event-security/481-bringing-home-the-gold-in-event-security

[3] LE BON, Gustave. (1920): Psychologie des foules. A tömegek lélektana, Frankin. Az eredeti kiadásban még nincs ISBN szám.

[4] BECK, Ulrich, (1986): Risikogesellschaft. Frankfurt am Main: Suhrkamp, 121-161, 205-220.o.

[5] SZABÓ Máté (1995): Tiltakozási kultúra Magyarországon a rendszerváltozás után a sajtó tükrében (1989-1995) Forrás: Szabó Máté oldala, és forrás itt: www.adata.hu/_.../Tiltakozási%20kultúra%20Magyarországon%20a%20rendszerváltás%20utá...

széleskörű tapasztalata van a biztonsági feladatok valamennyi típusú rendezvényen való véghezvitelének.[6]

Fontos lehet, - bár a hatályos szabályozás rendelkezik erről –, hogy minden tömeges rendezvény szervezője tartalmas felelősséggel bírjon a rendezvény minden körülményét, részletét érintően. Látható, hogy a rendőrség energiái is végesek, és számos olyan eset adódott a közelmúltban is, ahogy az egyébként értékesebb és nagyobb felhatalmazással bíró rendőrök szerepeltetése helyett speciális magánbiztonsági szolgálatok igénybevétele indokolt.

A jogi szabályozás neuralgikus pontja a bejelentések körül rajzolódik meg, mi tekinthető spontánnak, s persze, hogy milyen időszakban zajlanak az események. A szabályok pontos finomhangolása még hátravan, az azonban nyilvánvaló, hogy jelentős társadalmi konszenzussal elfogadott, hosszútávon vállalható és követhető szabályozás szükséges.

Időnként felüti még a fejét hibás elgondolás, amely indokolatlanul (nagyobb) szerepet szán az államnak, a rendőrségnek a tömegrendezvények biztosításában. „A tömegrendezvények biztosítása alapvetően rendőri feladat, amelyben más rendészeti szervek vagy magánbiztonsági szolgáltatók nem vehetnek részt. A tömegmegmozdulások kezelésének jogi hátterével, így különösen a gyülekezési jog alkalmazásával, egyes a rendbontások során elkövetett jogsértések pönalizálásával, illetve azok felderítésének, elbírálásának joggyakorlatával kapcsolatos feladatokat a Kormány jogpolitikai tevékenységének körében részben elvégezte, illetve azokat a Parlament elé terjesztette.”[7] Nyilván a közterületen megvalósuló politikai típusú rendezvényekre vonatkozik a megfogalmazás, ám tárgyunk szempontjából ez most kevésbé fontos.

Természetesen arra gondolok, hogy a legnagyobb tömegrendezvényeket az elmúlt években (Balaton Sound, Sziget, stb.) magánbiztonsági szolgálatok biztosították, nagyon magas szinten, nemzetközi elismerést kiváltva. Ugyanerről a korábban hivatkozott brit biztonsági vezető az alábbiak szerint fogalmaz: "A közhatalmak gyakran vesznek részt a jelentősebb eseményeken, ahol követelmény a nagyszámú rendőr jelenléte. Amikor azonban a források a határaikat feszegetik, a magán biztonsági ipar nagyszerű segítség a rendőrségi erőkön való nyomás enyhítésében és néhány, az események biztosításában szükséges feladat átvállalásában." Példaként, a 2012-es Olimpiai és Paralimpiai Játékokat említi, a Rendőrség nagy erőkkel fogja támogatni a magán biztonsági szektort, és még a legnagyobb magán biztonsági vállalatok is együtt fognak működni a kisebb cégekkel a hatékony biztonság szolgáltatása érdekében. A BSIA már korán kapcsolatba lép a Rendőri Vezetők Szövetségével (Association of Chief Police Officers-ACPO), ahogy a kormány minisztériumaival -mint az olimpiai biztonsági igazgatóság, avLondoni Szervező Bizottság az Olimpiai Játékokért (London Organising Committee for the Olympic Games- LOCOG) -, hogy biztosítsa a hatékonyan működő munkakapcsolatot az Olimpiai Játékokig fennmaradó időben.

Disszertációmban már hangot adtam vélekedésemnek, hogy bár a rendőrség vonatkozásában Kacziba a tárgyunk szempontjából arról is ír, hogy átfogó korszerűsítési intézkedések történtek a rendészeti csapaterőként működő Készenléti Rendőrség személyi állományának képzése, továbbképzése és felszerelése tekintetében, s intézkedtek arra nézve is, hogy a tömegrendezvények terén alkalmazható rendészeti taktika zárkózzon fel a nyugat-európai rendészeti gyakorlat követelményeihez. Meggyőződésem, hogy a magánbiztonsági szolgálatok e tekintetben egy kicsit már előrébb járnak, s rugalmasabb, meggyőzőbb felkészülést mutattak az elmúlt évek során. E megjegyzésemnek nem mond ellent, inkább

[6] KELLY, JAMES, a Brit Biztonsági Ipari Szövetség (Britsh Security Indusrty Association-BSIA) vezetője, a nagy létszámú rendezvények biztonsági stratégiájának kihívásairól és szervezőiről adott riportotjban. Forrás itt: http://www.counterterrorbusiness.com/features/93-event-security/481-bringing-home-the-gold-in-event-security

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

árnyalja a későbbiekben, a személybiztosítást végző magántestőrök felkészítése oktatása kapcsán megfogalmazott véleményem.

RENDEZVÉNYBIZTOSÍTÁS A NEMZETKÖZI GYAKORLATOK ASPEKTUSÁBÓL. A HÁROM KÖR

Jelen fejezetben számos távol-keleti, és európai példát áttekintve főbb pontokba szedve igyekszem interpretálni, melyek a legfontosabb teendők a nagyon jelentős tömegeket feltételező rendezvények magas szintű biztosításakor.

Kezdjük egy szomorú, esettel. Egy tinédzser meghalt, kilenc pedig megsérült abban az összecsapás sorozatban, amely a hosszú ideje egymással rivalizáló amerikai futball csapatok egymást követő meccsein történt Dallas külvárosában. Számtalan verekedés szakította félbe a futballmeccseket Richmondban (Virginia), három rendőr sérülését okozva és közel egy tucat letartóztatást vonva maga után. Két tinédzsert kaptak el lőfegyverrel, miután a sheriff megbízottak fémdetektorokat állítottak fel a Walterboro, S.C., futball stadionnál. Számos biztosítást, eseményt lehetne még citálni, azonban a problémák ezen keresztül is láttathatóak.

Több tervet kell készíteni a professzionális biztosítás elé, amelyek tartalma és száma a helyi gyakorlatokhoz és normákhoz igazodik, ám a Biztosítási tervtől nem térhetünk el. Ennek legfontosabb elemeit emelem ki. A biztosításért felelős személy köteles ilyen tervet készíteni. A tervnek tartalmazni kell a biztosításban résztvevő szerveket, szervezeteket, a feladatmegosztást pontosan cizellálva.

feladatmegosztás például a rendőrség és a civil biztonsági szolgálat feladatait választja szét. Rendőrségi biztosítás esetén a vagyonvédelmi vállalkozás feladata lehet:

- megfelelő létszám biztosítása,
- beléptetés, jegykezelés, biztonsági ellenőrzés,
- intézkedés esetén segítségnyújtás a rendőrségnek,
- a nézők irányítása, a szektorok lezárása (amennyiben van), a nézők vándorlásának megakadályozása,
- a nézők magatartásának folyamatos figyelése,
- a résztvevők védelme,
- a menekítési útvonalak biztosítása,
- jogsértések megelőzése,
- szabálysértésen vagy bűncselekményen tetten ért személy(ek) visszatartása, átadása a rendőrségnek,
- külső és belső parkolók biztosítása, védelme,
- helyiségek, technikai eszközök, felszerelések őrzése,
- rendkívüli események bekövetkezésekor segítségnyújtás.

Ezen kívül tisztázni szükséges a rendőri jelenlét minőségét, mennyiségét, elhelyezkedését.

Több nemzetközi példát is látva tapasztalhatjuk, hogy ezen elemek minden terv részét kell képezzék bárhol a világon, akárcsak a védelmi körök, saját erő-, eszközigény előzetes végiggondolásának. Mi a "hármas koncentrikus kor" védelmének elvét követjük. Miről szól ez? Mindegyik körnek megvan a maga funkciója, amely a másik feladatait egészíti ki vagy készíti elő.

A védelmi körök típusai:

- külső,
- középső,
- belső védelmi kör.

A külső kör magába foglalja a rendezvények helyszínének közvetlen környezetében és a megközelítési útvonalakon megoldandó biztosítási feladatokat, a helyszín külső határának biztosítása, illetéktelen személyek behatolásának megakadályozásának céljából. A beléptetési pontokon túl ellenőrizni, védeni kell az egyéb bejáratokat, kapukat. Ez épület esetében a kerítés, a beléptetési pontok, a kerítésen belüli terület, környezet, az épület saját parkolója alkotja. Kültéri rendezvények esetében a szervező által telepített kerítések, illetve az általa kijelölt parkoló alkotja. A szervező embereinek az érkezőket kell útbaigazítania, a rendezőknek, a gyanúsnak látszó személyeket, csomagokat már a épületbe, területre való belépés előtt át kell vizsgálniuk. Nagy létszámú rendezvény esetén alkalmazhatnak a tömegben a tömeg mögött elhelyezett megfigyelőket, akik folyamatosan tájékoztatják a vezetőt a hangulatról, esetleg a gyanús eseményekről. Nagy terület esetében (a beengedési pontokat kivéve) kutyás területőrzést is alkalmazhat a rendező a kerítések mentés, a jogosulatlan behatolás megakadályozása érdekében, illetve a parkoló őrzését is meg lehet valósítani ilyen típusú őrzéssel. A parkolást irányítók esetében (amennyiben belépési korlátozás van) a parkolható autók rendszámát is le kell adni, hogy a jogosultságot ellenőrizni lehessen.

A középső kör az a terület, ahol, a rendezvényt megtartják, és ahová az érdeklődők meghívójukkal, belépőjegyeikkel ellenőrzötten bejuthatnak. E kör tartalmazza a beléptetést, a területen belüli tájékoztatást és a rendezvény belső rendjének biztosítását. A beléptetés jogosultságát a szervező emberei ellenőrizhetik, a csomag-, illetve felsőruházat átvizsgálást a biztosítók végezhetik. Sportrendezvény esetében a beléptető kapuknál érdemes egy kapura 3-4 főt számolni, a gyors haladás, illetve a segítségnyújtás érdekében. A biztonsági személyzet munkáját nagyban segíti, ha a rendezvény szereplőinek, azok segítőinek jól elkülöníthető színösszeállítású kitűzőket osztanak ki. A kitűzők színe egyben a használójának a mozgásterét vagy más jogosultságát is behatárolja. A beléptetésnél az őrök kiemelt figyelmet kell, hogy fordítsanak az ilyen kitűzővel rendelkező személyekre (pl.: átvizsgálást nem igényelnek). Egy őrzött objektum megrendezésre kerülő rendezvény esetén a feladatok kiegészülnek az objektum bejárata és a rendezvény helyszíne közötti területen végrehajtandó biztosítási feladatokkal, például az épület lezárt területeken nem tartózkodhatnak illetéktelenek, illetve nem állhatják el az épület üzemeltetéséhez szükséges bejáratokat. Esetleg a résztvevők a helyszínre való kísérését is meg kell valósítani.

A belső körben kell elhelyezni a szereplők és a segítő személyzetük igazolását végző, illetve az öltözőkbe, tartózkodási helyekre vezető útvonalat ellenőrző személyeket. Ebbe az övezetbe csak a szereplők és azok személyzete, illetve a rendezvény lebonyolítását végző személyzet kaphat belépési engedélyt. Az itt alkalmazott beléptetésnél a jogosultság ellenőrzését előnyben kell részesíteni a ruhaátvizsgálásnál. Minden körnél a pontőrzést és a járőrözést is meg kell valósítani. A vezetési pont felállítása, ennek kijelölése minden biztosításunk során nagyon figyelemmel megválasztott.

A biztosítást végző vezetőnek ennél a pontnál kell megállapítania a biztonsági személyzet létszámát, kijelölni felállítási helyeiket, megszabni a feladataikat, szolgálati rendjüket, ruházatukat, megkülönböztető jelzéseiket, felszereléseiket. Rendkívül fontos, hogy a túlzott létszámban vagy feleslegesen látványosan felszerelt biztonsági személyzet legalább akkora hiba, mint a feladat ellátásához nem megfelelően felszerelt, alacsony létszámú személyzet. Míg az első feleslegesen ingerelheti a tömeget, a második képtelen feladatait ellátni.

A személyzet kiválasztásánál, beosztásánál figyelembe kell vennie, a biztosítók képzettségét, tapasztalatait, viselkedésformáit, ismereteit, modorát. Amennyiben a rendezvényen kiemelt fontosságú külföldi személy is részt vesz, úgy a biztosítására természetesen az adott idegen nyelvet beszélő biztosítót kell megbíznia.

A vezetőnek ennél a pontnál kell az időpontokat meghatározni. Időpontok:

- a rendezvény biztosításának kezdeti és befejező időpontját;
- a területi átvizsgálások időpontjait;
- a szolgálati pontok felállításának időpontját;
- a beléptetés kezdetének időpontját.

Lényeges, hogy a vezető személy szerint felelős az egyes tevékenységekre kijelölt rendezvénybiztosítók és általánosságban az egész személyzet viselkedéséért. Ennél a pontnál kell a biztosítás során használni kívánt eszközöket tételesen felsorolni, felállítási pontjaikat meghatározni és az elhelyezésükkel kapcsolatos mindenféle feladatot meghatározni. Meg kell határozni a várható közönségszámot, a kapcsolattartás rendjét, a rádió hívóneveket és hívószámokat, rendkívüli esemény bekövetkezése esetén a magán biztonsági szolgálat teendőit.

Elsősorban a fiatalokkal kapcsolatos tömegrendezvényeken megjelenő erőszakról ír[8] Kenneth S. Trump, aki (nem csak ezekre érthetően) három lépést emel ki. Az első az előre tervezés, amely egyeztetéseket, pontos információszerzést, a korábbi esetek, gyakorlatok megismerését egyaránt feltételezi. A második - szerinte - a megfelelő személyzet, vagyis a legjobb biztosítás kiválasztása - erről korábban már írtam. A harmadik lépés pedig a folyamatos készenlét, vagyis mindig készen állni a veszélyhelyzetek elhárítására.

VÉDETT SZEMÉLY A TÖMEGBEN. A BIZTOSÍTÁS NÉHÁNY SPECIFIKUMA

A személyvédők olyan, az eseményen megjelenő VIP személyek védelménél szükségesek, mint híresség, politikusok, különösen a közhírré tettek vagy sokat vitatottak. A 2012-es Londoni Játékokon és nemrég Londonban, a hercegi esküvőn látott híresség részvétele az eseményen megjelenő tömegben, úgymint nemzeti és nemzetközi politikusok, híresség, a királyi család tagjai és jól ismert sportolók - ezek a legújabb, a biztosítást jól kifejezeő események.

A személyvédők munkája az esemény előtt kezdődik a helyszín részletekbe menő vizsgálatával annak érdekében, hogy minden sarok biztosítva legyen. A legtöbb forgatókönyv szerint a biztosítani kell, hogy a VIP látogatók végezni tudják napi ügyeiket, körülöttük egy majdnem láthatatlan buborékkal, csak akkor reagálva, amikor szükséges. Minden egyes, VIP személyre vonatkozó biztonsági követelménynek integrálva kell lennie az eseményre vonatkozó, szélesebb biztonsági stratégiában, nyomást gyakorolva ezzel a szervezőkre oly módon, hogy meg kell bizonyosodniuk, valamennyi nézőpontot figyelembe vettek. Azonban a különböző biztonsági teamek és résztvevő segítők közötti kommunikációnak pontosnak és eredményesnek kell lennie az esemény alatt és után.[9]

---

[8] TRUMP, Kenneth S. – a Nemzeti Iskolai Biztonság és Biztonsági Szolgáltatások, Cleveland-i, nemzeti konzultációs, iskolai biztonságra és vészhelyzetekre felkészítő tréningre és konzultációra specializálódott cég elnöke in: American school Board journal/February 2007, p. 26-29.

[9] Tapasztalom, hogy a professzionális személybiztosítást ellátó cégek nem szívesen osztják meg saját személyvédő technikáikat és tapasztalataikat a szélesebb publikummal, amelynek okai érthetőek. A kutatásaim során tett beszélgetéseket (amelyeket Európában éppúgy mint tengeren túlon folytattam) követően engem is szigorú ígéret köt, hogy csak azon információkat tegyem publikussá, amelyek nem jelenthetnek egy később, akár általunk vállalt biztosításnál kockázatot. Erről itt: http://www.counterterrorbusiness.com/features/93-event-security/481-bringing-home-the-gold-in-event-security

Amennyiben védett személy vesz részt tömegrendezvényen, az rendkívül szoros, ám a védett felé nyitott, a tömegrendezvény felé zárt információáramlást feltételez. Szerencsés esetben ugyanaz a cég biztosítja a rendezvényt és a védett személyt, ám ha nem, ezen alaptételnek nem szabad változnia. Azt jelenti mindez, hogy a védett személy biztosításában résztvevőknek valamennyi információt ismerniük kell (menekülő útvonalak, kapuk, kapcsolatok, stb.) amelyet a rendezvénybiztosításért felelős személy ismer, a rendezvénybiztosítási dokumentáció tartalmaz. Fordítva ugyanez azonban nem igaz. A védett személlyel kapcsolatos információk közül csak a legszükségesebbeket kell megosztanunk a rendezvénybiztosítás vezetőjével, hiszen ez fontos biztonsági kockázat lehet.

BIZTONSÁGI ŐR, TESTŐR

Szögezzük le: a biztonsági őr nem testőr, a személyvédő (testőr) pedig elsősorban nem biztonsági őr, s a védett személyre koncentrál. A közvélemény gyakran tekinti a személyvédőket úgy, mint egy jól-ismert és/vagy fenyegetett személy védelmezőjeként.

Egy világ láthatta, amint az Amerikai Titkosszolgálat (U.S. Secret Service-USSS) eltávolította a demonstrációkat Bush elnök beszéde alatt, vagy épp ahogy az elnököt húzta testőre a "harcoló" testőrök kordonján keresztül Chilében, egy állami fogadáson. De a védelem az egyetlen dolog, amit a USSS ügynökök vagy a (magán) személyvédők (close protection officer- CPO; close protection jelenti valamely személy védelmét, vagy az itt is használt bodyguarding, de ez utóbbi kifejezést használják inkább újságokban etc. a 'close protection officer' pedig maga a személyvédő. megj. tőlem) tesznek?

Jerome Jacobs egyértelmű választ ad: szerencsére nem, mivel néhány helyzetben a kimenetel drámai lett volna! A CPO-k nem csak a védelemre kiképzettek, hanem elsősegélynyújtásra is. Ezenkívül kiképzik őket objektumok védelmére is, mint rezidenciák, irodák, etc. Az önvédelem, a lövészet és a speciális vezetési tanfolyamok szintén részét képezik kemény kiképzésüknek. Mondhatjuk, hogy a CPO egy sokoldalú személy, aki otthon van minden területen és egy specialista.

Nem mindenki válhat testőrré. Még egy "hétköznapi" biztonsági őr (security officer) számára is majdnem lehetetlen -amerikai terminus technicussal- CPO-vá válni. Hogy egy testőr a múltban biztonsági személyként (őrként) dolgozott, előny, de nem feltétlenül követelmény. Egy vérbeli testőrnek meg kell felelnie néhány speciális követelménynek - fogalmaz Jacobs[10]. A képességek 3 típusával kell rendelkeznie:

1. tanulható kézségek
2. nem tanulható kézségek
3. használható kézségek

Mit is jelent tulajdonképpen az a három kézség- teszi fel a kérdést Jacobas?

1. amely kézségek főként megtanulhatóak
2. ezen kézségek nem taníthatók, rendelkezni kell velük

Tehetségnek is hívhatjuk ezeket.

3. mindent elmond, használható kézségek.

10 JACOBS, Jerome, ©27-01-2009. Forrás: http://www.iacpo.org/index.php?option=com_k2&view=itemlist&layout=category&task=category&id=5&Itemid=130

A TESTŐRREL SZEMBEN TÁMASZTOTT PSZICHOLÓGIAI KÉSZSÉGEKRŐL

Ha valaki személyvédővé akar válni, rendelkeznie kell Jacobs szerint legalább a nem tanulható kézségekkel. A tanulható kézségek a második legfontosabb, melyekkel rendelkezni kell, bár néhány használható kézség is jó, ha van. Ám a pszichológiai készségek követelménye szélesebb.

"Kemény" képességek szükségesek a személyvédő specialistáknak, akiket gyakran tekintenek úgy, mint akik rendőrként vagy (elit) katonaként viselkednek. Noha lehetnek bizonyos hasonlóságok, pl a fegyverhasználat, a pusztakezes küzdelem vagy a járműkezelés tekintetében, a legtöbb ember, aki dolgozott mindkét területen, visszautasítja, hogy a kézségek hasonlóak. Talán hasonlónak tűnnek, de a módszertanuk részről részre más. A pszichológiai képességeknek azonban majdnem azonosnak kell lenniük. A pszichológiai jártasság ismerete alapvető ezen a területen, ahogy a rendvédelmi vagy katonai küzdelemben is. Bármely személynek, aki felelősséget vállal másvalaki életéért, figyelemmel kell lennie a pszichológiai adottságainak alkalmazhatóságára a különböző helyzetekben. Ezek magukban foglalják a kellemetlen szituációkban való alkalmazhatóságot (a pszichológiai állapotnak az egyszerűtől az ellentmondást nem tűrő állapotig változása), különböző munkakörnyezetben alkalmazhatóságot (a testet és az elmét nyugodt állapotban tartani az ügyfélre várakozás közben és hirtelen magas stressz szintre változik) és az örök, olyan közkedvelt, élet-vagy-halál szituációk figyelembevételének kérdését (megölhetem vagy ne mozduljak?), de nem korlátozódik ezekre.

Tudni és nyíltan elfogadni, hogy egyes fizikai vagy pszichológiai korlátok léteznek, életet mentő. Nemcsak egyesek életét menti meg, hanem a csapattársak és ügyfelek életét is.[11]

Kormányzati szinten a CPO különösképpen foglalkoztatott ezekkel a képességekkel. a privát szektorban gyakran különböző, részben mert néhány kézséget vagy válogatott tulajdonságot nehéz ellenőrizni. Ennek oka, hogy a magánszektor nincs felhatalmazva ezek leinformálására. Ahogy a hivatkozott forrás korábban említette, a testőröket kizárólag védelmi személynek tekintik, pedig sokkal többet tesznek annál. Vannak testőrök, akik nagyon jó autóvezetők vagy gyermekvédők, és vannak női személyvédők is, akik kizárólag nőket védenek.

Mivel a személyvédő nagyon közel áll a VIP személyhez, lehetséges, hogy céltáblájává válik a VIP érzelmeinek, különösen, ha valami rosszra fordul. Néha a CPO a VIP személyi asszisztense (VIP Personal Assistant =PA), mert éttermi vagy utazási foglalásokat tesz. A sokoldalú védelmi személyen kívül a CPO egy "mindenes", bizonyos mértékig.

Érdekes kérdés e téren a biztonság. A hivatkozott dániai igazgató véleményét magam is osztom, aki szerint a képzés ezen a területen a magánszektorban majdhogynem nem létezik. Ezért is fordítunk magunk is különösen sok időt aktív állományunk képzésére, amely rendszeres és visszatérő, s tartalmazza a legújabb tapasztalatok átültetését a gyakorlatba, s a kötelező vizsgálatokon túl a rendszeres és állandó vagy épp változó ismeretek frissítését. Brambsborg egy "könnyen követhető tréning" forgatókönyvét is megosztja a biztonsági menedzserek/csapatvezetők számára, amelyből kettőt osztok meg ezúttal, amelyet mi is alkalmazunk az éves képzési tervünk során:

---

[11] BRAMSBORG, Henrik, *Forrás:* By Henrik Bramsborg *(társtulajdoosa egy exkluzív biztonsági cégnek Dániában. Számos biztonsági könyv szerzője. Személyvédő instruktor, NATO S-FOR erők kiképzését is végezte, rendőrökét, büntetésvégrehajtási szakemberekét és magán testőrőkét.* International Association of Close Protection Officers-*IACPO (Személyvédők Nemzetközi Egyesülete) dániai igazgatója.*
http://www.iacpo.org/index.php?option=com_k2&view=itemlist&task=category&id=7:necessary-psychological-skills-when-working-in-executive-protection&Itemid=132

1. Egy diákot vagy egy újonc testőrt vigyünk egy partyba és jelöljük ki egy VIP személy mellé. Ez lehet a saját privát partyn és a VIP bárki lehet, akit választunk, de győződjünk meg arról, hogy a VIP tudja, a testőrök azért vannak ott, hogy figyeljenek rá. A testőr értékelésétől függően a VIP lehet egy nagyon attraktív nő (lehetséges problémák: féltékenység, vagy számtalan imádó) vagy egy férfi, ivásra való hajlammal (lehetséges problémák: helytelen vagy vakmerő viselkedés). Most figyeljük meg a testőrt az éjszakán keresztül. Ha szükségesnek tartjuk, vegyünk igénybe valakit, aki segít jelenetet rendezni, mint a helyes viselkedés provokálásaként a VIP személytől és remélhetőleg a testőrtől.

A forgatókönyv elődleges célja, hogy megtalálja a bizonytalanság és/vagy a zavar jeleit abban az időpontban, amikor a személyvédőnek el kell döntenie, hogy közbelépjen vagy ne. A másodlagos cél lehet a testőr által írásos jelentés készíttetése rögtön a kikérdezés után, leírandó bármely hibát a saját érzelmi viselkedésében. Ennél fogva segíteni saját önbecsülésük és a kapcsolódó megismerő képességek megértését.

2. Munkakörnyezet. Helyezzünk el diákot vagy egy új testőrt egy olyan munkahelyen, ahol alacsony színvonalú a menedzsment/igazgatás. A 3-5 napra kijelölés a preferált. Tegyük a teljes tervezés és személyi kíséret osztály résztvevőjévé (mutassuk be tanítványként az igazgatónak/menedzsernek, ha szükséges). Bármely és minden meetingnél ezt a meghatározott diákot állítsuk az ajtók előtti posztra a folyosókon, irodákban, etc. Had tapasztalja meg a várakozás örömét. Biztosítsuk, hogy végül minden információt megkapjon. Változtassa a járásmódját, bármikor, amikor ez lehetséges. Nem sokkal ezután figyeljük meg a "lecsillapodás-sietség" ("relax-hurry" syndrome) szindróma beütését. A diák stresszhormonok növelésének és csökkentésének képességétől függően fáradtnak fogja érezni magát egy idő után, majdnem egy depresszív állapot felé hajolva. Ha alacsony a stressz-tűrése, az előbb említett állapot nyilvánvaló. Amennyiben nem, ez alig látható. Hasznos lehet leméri a tanulót a kezdés előtt és rögtön utána. Alacsony stresszkontrollal rendelkező személyek hajlamosak több súlyt veszíteni, még rövid idő alatt is, mint azok, aki jobb stressz állapotban vannak. Megint készítessünk írásos jelentést a tanulóval a pszichológiai és érzelmi komfortjáról rögtön a kikérdezés után.

A megmagyarázott képességeken kívül minden testőrnek fejlesztenie kell a jó jellem megítélését, közvetlen/közvetett támadás felismerő kézségét, képesnek kell lennie a manipulálás felismerésére és magabiztos fellépéssel kell rendelkeznie az emberek felé. Nem lehet mindenkinek kimagasló vagy akár szerényebb pszichológiai végzettsége, de bárkinek, aki a személyvédelem területén dolgozik, részt kell vennie néhány rövid pszichológiai tréningen. E tréningeknek rendszeresnek kell lenniük, cégünknél magunk is így teszünk. Ez a fajta tréning a normál rendőrtiszti képzés része is kell legyen, ahogy része az általános e területen dolgozók (pl. katonák) felkészítő oktatásának, és Bramsborggal egyező véleményem szerint, kötelezően része kellene, hogy legyen a személyvédők képzésének. Így tehát, ezen utolsó mondattal már célokt is tűztünk a honi magánbiztonsági képzés elé.

Felhasznált irodalom

[1] GYENES Levente (2003): Biztonságvédelmi kézikönyv. KJK-KERSZÖV Jogi és üzleti kiadó Kft., Budapest, 2003. ISBN 9632245539

[2] KELLY, JAMES, a Brit Biztonsági Ipari Szövetség (Britsh Security Indusrty Association-BSIA) vezetője, a nagy létszámú rendezvények biztonsági stratégiájának kihívásairól és szervezőiről adott riportotjban. Forrás itt: http://www.counterterrorbusiness.com/features/93-event-security/481-bringing-home-the-gold-in-event-security

[3] LE BON, Gustave. (1920): Psychologie des foules. A tömegek lélektana, Frankin. Az eredeti kiadásban még nincs ISBN szám.

[4] BECK, Ulrich, (1986): Risikogesellschaft. Frankfurt am Main: Suhrkamp, 121-161, 205-220.o.

[5] SZABÓ Máté (1995): Tiltakozási kultúra Magyarországon a rendszerváltozás után a sajtó tükrében (1989-1995) Forrás: Szabó Máté oldala, és forrás itt: www.adata.hu/_.../ Tiltakozási%20kultúra%20Magyarországon%20a%20rendszerváltás%20utá...

[6] KELLY, JAMES, a Brit Biztonsági Ipari Szövetség (Britsh Security Indusrty Association-BSIA) vezetője, a nagy létszámú rendezvények biztonsági stratégiájának kihívásairól és szervezőiről adott riportotjban. Forrás itt: http://www.counterterrorbusiness.com/features/93-event-security/481-bringing-home-the-gold-in-event-security

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

[8] TRUMP, Kenneth S. – a Nemzeti Iskolai Biztonság és Biztonsági Szolgáltatások, Cleveland-i, nemzeti konzultációs, iskolai biztonságra és vészhelyzetekre felkészítő tréningre és konzultációra specializálódott cég elnöke in: American school Board journal/February 2007, p. 26-29.

[9] http://www.counterterrorbusiness.com/features/93-event-security/481-bringing-home-the-gold-in-event-security

[10] JACOBS, Jerome, ©27-01-2009.

[11] Forrás: http://www.iacpo.org/index.php?option=com_k2&view=itemlist&layout=category&task=category&id=5&Itemid=130

[12] BRAMSBORG, Henrik, Forrás: By Henrik Bramsborg (társtulajdoosa egy exkluzív biztonsági cégnek Dániában. Számos biztonsági könyv szerzője. Személyvédő instruktor, NATO S-FOR erők kiképzését is végezte, rendőrökét, büntetésvégrehajtási szakemberekét és magán testőrőkét. International Association of Close Protection Officers-IACPO (Személyvédők Nemzetközi Egyesülete) dániai igazgatója. http://www.iacpo.org/index.php?option=com_k2&view=itemlist&task=category&id=7:necessary-psychological-skills-when-working-in-executive-protection&Itemid=132

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Lasz György
georgelasz@gmail.com

A BIZTONSÁGTECHNIKA ALAPJAINAK MEGJELENÉSE AZ OBJEKTUMVÉDELEM GYAKORLATÁBAN

Absztrakt

A rendezvénybiztosítás mellett az objektumvédelem a legnagyobb felségterülete a magánbiztonsági szolgálatoknak. A biztonságtechnika tudományos alapjainak ismerete nélkül azonban hosszabb távon nem létezhet magas szintű (objektum)védelem, nem lehet professzionális szolgáltatás, de facto: nem lehetnek elégedett ügyfelek.
Az információtechnológia mellett a védelmi szolgáltatások során használt eszközök és technikák fejlődése is jelentős, amelyek sokszor nem megfizethetőek a magánbiztonsági piacon, sokan kizárólag az állandó élőerős őrzés elkötelezettjei, noha a távfelügyeleti szolgáltatások rejtette protokollok - amelyek egyszerre tartalmazzák az elektronikus jelzőrendszerek kiszámíthatóságát és az élőerős védelem garantálta jelenlétet - többre érdemesek.

Besides the event security, the biggest area of private security services is the physical security. But high-level (physical)security cannot exists through a long term without knowledge of the scientific basis of security technology, it can't be a professional service, de facto clients can't be satisfied.
Besides the information technology, also the development of techniques and appliances used in protection services is important, whiches are often not affordable in the private security market, many people are committed to the permanent, manpower guarding, though protocols in distance surveillance - whiches include both computability of the electronic indicator systems and attendance ensured by manpower protection - are more worthy.

Kulcsszavak: *biztonságtechnika, objektumvédelem, magánbiztonság ~ security technology, physical security, private security*

BIZTONSÁG ÉS TUDOMÁNY

A biztonságtudomány nem régi keletű fogalom, így elemeinek meghatározása, cizellálása minden, ezzel foglalkozó kutató számára izgalmas kérdés. Publikációm bevezetőjében a második Biztonságtudományi Világkonferencián elhangzott elméleti koncepciókból és gyakorlati megismerősekből egyaránt merítettem. A biztonság nélkülözhetetlen eleme életünk minden részének, prioritás: bolygónk biztonságától, családunk, személyes biztonságunkon át lakóhelyünk nyugalmáig. Ebből is következik, hogy a biztonságtudomány az élet minden területét átfogja s tanulmányozza a rendszerek, közöttük a termelési rendszerek változásainak alapjait. Fejlődése cáfolja, hogy a biztonság a termelési rendszertől függ, s fejlődése a technológiai fejlődés mögé kényszerülne.[1] A biztonságtudomány célja a rendszerek biztonsági funkció központú elemzése, a rendszerbiztonság tervezése, részletes kidolgozása.

Ezekből fakadóan a biztonságtudomány az egészségmegőrzés egyik eszköze és az objektív valóság létező állapotának egyik aspektusa is egyben. A biztonság iránti igény, akár a biztonsággal kapcsolatos problémák az emberi gondolkodással egyidős. A megismerés a kisebbtől a nagyobb felé, vagyis a kevésbé ismerttől a bonyolultabb megismerése felé halad, amelyben több kutató szakaszokat azonosít (ártatlanság, felfedezés, rendszer biztonság, biztonságtudomány). A biztonságtudomány rendszere horizontálisan a filozófia mellett a biztonság és biztonságtechnikai tudományra figyel, vertikális rendszerében a biztonsági filozófia és az egyes horizontális elemek helyezkednek el. Ismernünk kell azonban a biztonság tervezésére vonatkozó két legfontosabb törvényt: teljes biztonságra törekedni kötelező, azt megvalósítani azonban nem lehet,[2] s minden biztonsági tevékenység eltérő hatékonysággal bír.

A biztonságtudomány számos vizsgálati módszerrel rendelkezik (HAZOP - hazard and operatibility studies, azaz veszély és működőképesség vizsgálat; ETA - event tree analisy, eseményfa elemzés; AEA - activity error analysis; TA - task analyis, feladat aanalízis; IEA - intital event analysis, kezdeti eseményelemzés; stb.) - ám ezek közül, munkám gyakorlatára figyelemmel hármat veszek nagyító alá. Az objektumvédelmet megelőző kezdeti eseményelemzésről, a feladat, valamint a végesemény elemzésről szólok.

Kezdeti eseményanalízis (IEA - inital event analysis), feladat- (TA - task analysis) és végesemény elemzés (PFA - post factum analysis) az objektumvédelemben[3]

A kezdeti eseményanalízis minden vállalást megelőző feladat. Ennek során összevetjük, hogy a rendelkezésre álló vagy elérhető erő, humán és infrastruktúra alkalmas-e a feladat végrehajtására, a megbízói igény teljesíthető-e? Ennél az eljárásnál a rendszert elemenként vizsgáljuk. Nézzük a jogi környezetet, a helyi normákat, ezek akklimatizálhatóságát, a lehetséges kockázati tényezőket. Szükséges ehhez minden dokumentáció, tervrajzok, biztonsági útvonalak, az objektum teljes műszaki és egyéb dokumentációja. Figyelnünk kell a számítógépes, felügyeleti rendszerekre, ezek programjaira, javítási és karbantartási utasításokra, korábbi veszélyhelyzetekre.

A feladat elemzés[4] megkerülhetetlen módszer, gyakorta használjuk a távfelügyeleti rendszerekben is, hiszen az emberi, felügyelői hibák elemzését nagyban segíti. A legelső lépés

[1] KISS Sándor: Biztonságtechnika alapjai. Főiskolai jegyzet, Budapest, 2004. Zrínyi Miklós Nemzetvédelmi Egyetem, Bolyai János Katonai Műszaki Főiskolai kar.

[2] A tételek innen: Hans A. Merz és Hans Bohnenblust megállapításai itt: Cost/Effectiveness Analyses and Evaluation of Risk Reduction Measures, 2-nd World Congress on safety Science Budapest, 1994.

[3] SOUKAS, Iuko: On the reliability and validity of safety analysis (Espoo, 1989). Innen: Kiss Sándor im. 20. p. A terminológiát Gál Csaba használja először, lásd ugyanitt

[4] McCLAY, R. E.: Using Task Analysis to Estimate the Risk of Human Error (2-nd WCOSS Budapest, 1994)

hogy egy hasonló, optimálisan és biztonságosan működő rendszer modelljét az új objektum védelmére átültetjük, vagy ha nincs ilyen, kidolgozzuk az optimális működési feltételeket, vagyis az általunk, az In-Kal-nál az úgynevezett szuper biztonsági protokollt. Minden részfeladatot is alaptevékenységekre bontunk, ugyanezt tesszük a lehetséges veszélyekkel. Tesszük mindezt azért, hogy a felmerülhető, potenciális hibák beazonosíthatóvá váljanak. Alapegységnek azt a legkisebb azonosítható és célszerű elemet választjuk, amely már megjeleníti az emberi tevékenységet, az érintett munkafeladattal és az ahhoz vezető folyamattal együtt.

A végesemény elemzést ezeket követően dolgozzuk ki, immáron a vállalás tudatában. A tipikus munkafolyamatok áttekintése és megtervezése mellett a krízishelyzetek modellezését, a rendszerelemek csoportosítását is optimalizáljuk, s a hierachia és értesítési, kommunikációs rendszert is fel kell állítanunk. Munkacsoportban dolgozunk, az esetleges eltérő véleményeket rendszeresen modellezzük, átnézzük a korábbi ellenőrzések, viszgálatok tapasztalatait is. Komplett rendszerleíró védelmi dokumentáció készül.

BIZTONSÁGELEMZÉS, KOCKÁZATFELFOGÁS

Minden biztonsági tevékenységet a feladat sajátosságaitól függően tervezhető kockázat kísér. A technikai eszközök jelentősen segítik az adott objektumvédelmi biztosítási feladatatokat, ám meghibásodásukat nem mindig lehet kizárni, ezért azok működtetése újabb kockázat lehet. Ekként tehát a kockázat az objektumvédelem során lehet:

- tervezhető, kiszámítható feladatkockázat;
- kiszámítható (azonnal pótolható) vagy váratlan (nem azonnal korrigálható) technikai kockázat;
- személyi kockázat.

Noha minden megbízás során a kockázat minimalizálására kell törekedni, e fentieket nem szabad figyelmen kívül hagyni. A biztonsági elemzés során megrajzolódnak a kockázatok összetevői, ezek természete és összefüggéseik, ekként nyílik lehetőség azok csökkentésére. Az elemzések során mindenképpen meg kell válaszolni:

- optimális humán és infrastruktúra elosztást feltételezve azt, hogyan található meg az optimális kockázatcsökkentési stratégia - harmóniában a megbízással és a tevékenység jellegével;
- a kockázati szintek meghatározását követően mekkora kockázatcsökkentés szükséges, milyen kritériumok vállalhatók, de facto: mi a kiszámítható kockázat?!

A kockázati tényező egy olyan számérték[5] amely egy meghatározott helyi értékű skálán megmutatja, hogy az adott kockázatra vetített számérték hol helyezkedik el. Ebből a kockázatvállalás mértékére is következtetünk, amelyet a környezet, a felszereltség, s a végrehajtásban részt vevők személye határoz meg. A kockázat mértéke fordítottan arányos a megbízhatósággal, vagyis minél inkább kiszámítható egy rendszer működése és felügyelete annál inkább csökkenthető a kockázat. Ehhez azonban tennék egy megkötést. Minden rendszer üzemeltetésénél fontos, hogy ne alakuljanak ki egészségtelen automatizmusok, amelyek növelik a kockázatot. A humánerőforrások cseréjével, képzésével ezt magabiztosan ki lehet szűrni.

A kockázati tényező meghatározásánál figyelembe kell venni annak valószínűségét, hogy az valóban bekövetkezik-e, erre SWOT elemzéssel is törekszünk. E tényező értékét a technikai, felügyeleti eszközök minden, legkisebb elemére is meg kell határozni. A kockázati határérték azt fejezi ki, hogy az adott közeg (egyén vagy környezet) milyen mértékben képes

[5] KISS Sándor i.m. 47. p.

tolerálni egy kockázat vagyis egy rendszerzavar bekövetkezését. A határ ott húzódik, ahol az adott közeg (már) hajlandó szellemi, és anyagi erőfeszítéseket tenni a kockázat elkerülése érdekében.

AZ OBJEKTUMVÉDELEM SZINTJEI – ÁLTALÁBAN

Az objektumvédelem azon tevékenységeket jelöli, amelyeket az épületek, ingatlanok és más vagyontárgyak betolakodók elleni védelme érdekében tehetünk. A védelmi rendszer megtervezésekor a három védendő szint a külső és a belső terület valamint a belső tér. Ha két vagy inkább három biztonsági formát tudunk létrehozni mindegyik szinten, több mint valószínű, hogy rendszerünk optimalizált, vagyis: hatékony objektumvédelmi rendszerrel rendelkezünk. William Deutsch ennek kapcsán három szintről ír.[6]

Az ingatlan külső területét a határai jelölik ki. Ezen terület védelmében célunk annak ellenőrzése, ki közelít belépési szándékkal. A védelem egyik legextrémebb formája a magas fal, zsilipes kapu, szögesdrótkerítés fegyveres őrrel védett kapuval. Más esetekben egy egyszerű sövény is elegendő. Annak eldöntésekor, hogy milyen biztonsági formát hozzunk létre, mérlegelni kell egy betolakodó belépésének kockázatát és az elérhető biztonsági intézkedések költségét. Két biztonsági elgondolást jelent a terület védelmében a Természetes Belépést Ellenőrzés (Natural Access Control) és a Területi Megerősítés (Territorial Reinforcement). Más és más teendőink vannak üzleti objektumok vagy magánlakóingatlan(ok) esetében.

A Natural Access Control[7] egyike a CPTED (Crime Prevention Through Environmental Design - bűnmegelőzés az épített környezet tervezése által) négy alapelvének. Az alapelvek az elkövetők gondolatainak előrelátásán és egy, a véghezvitelt elriasztó környezeti klíma létrehozásán alapulnak. Amikor a CPTED-et a gyakorlatba ültetik át - hívja fel a figyelmet többek között Deutsch -, olyan környezetet eredményez -magában foglalva az épületét és az azt körülvevő területet-, amely akadályozza a kriminális viselkedést, és ugyanakkor ösztönzi a polgárokat, hogy szemfülesek legyenek. Bár ezen elveket az új épületek terveihez, konstrukcióihoz fejlesztették, a koncepció alkalmazható a már meglévőknél is.

Az első megfontolandó dolog a Natural Access Control esetében a terület megközelítése. Be tudnak-e hajtani a járművek észrevétel nélkül a területre? Ha igen, fontolóra kell venni kapuk, sorompók és járdaszegélyek, irányító táblák, természetes épített környezeti tárgyak használatát, melyek irányítják a járműforgalmat az egyes ellenőrzött területekhez. Fontos, hogy ezek áttekinthetőek legyenek, és ne teremtsenek lehetőséget elrejtőzésre! Ezen ellenőrzött bejáratok biztonsági személyzethez vezessenek! Amikor a jármű belép a területre, a vezetőt a jól körülhatárolt parkolóhoz kell irányítani. Vizsgálnunk kell a gyalogosforgalmat. Ha illetéktelenek be tudnak jönni az épületbe, akkor nyilvános kaput kell felállítani. Ideális esetben ez a kapu az őrséghez vagy a recepcióhoz vezet, ahol fogadják a látogatókat. A tető a másik problémás terület. Koncentráljunk arra, hogy minden bejutást innen is korlátozzunk, megakadályozzunk. Ha a tető menekülési útvonal, helikopter leszállópálya is, akkor felügyelnünk kell a forgalmat.

Az elkövetők az észrevétel nélküli bejövetelnél még inkább igyekeznek gyorsan eltűnni. Azonban a kijáratok korlátozása még nehezebb, mint a bejáratoké az élet biztonságának fontossága miatt. A tűzvédelmi előírások nem mindenütt engedik bezárni az épület kijáratait, még ha ezen kijáratok a raktárépület távoli területén vannak is. A problémát ellensúlyozhatjuk, ha a kijáratok körülötti területeket nyitottá és láthatóvá tesszük, amennyire csak lehet. Amíg nem kerül alkalmazásra a rendszer (Natural Access Control), késleltető kijárati hardware-t szerelhetünk a vészkijáratokhoz. Ez a hardware riaszt és kb. 15

[6] http://bizsecurity.about.com/od/physicalsecurity/a/What_is_physical_security.htm
[7] Uo.

másodpercig zárva tartja az ajtót azután, hogy valaki megnyomja azt a kinyitás érdekében. A hang figyelmeztet arra, hogy valaki megpróbál észrevétel nélkül kijutni, illetve ad egy rövid időt a reagálásra. A késleltetett kijárati ajtókat egyértelműen jelezni kell, hogy bárki tudja, az ajtó kinyitásának megkísérlése esetén a riasztó riasztani fog. Ahogy a bejáratoknál, itt is ideális, ha a kijáratok a gyalogosokat és a járműveket az őrséghez vagy a recepcióhoz vezetik.

A fegyveres őr kérdése gyakorta vitatott kérdés. A külön tanulmányt megérő pro és kontra állításokat jelen alkalommal nem részletezem, ám a honi gyakorlat szerint erre leginkább csak jelentős pénzforgalmú, vagy kiemelt kockázatú objektumok esetén alakult ki gyakorlat. Noha az ügyfél kérése és igénye e szempontban is meghatározó, a fegyveres őr alkalmazása nagyon gondos megfontolást, körültekintő felmérést igényel, s persze a költségek emelkedését is feltételezi.

A Territorial Reinforcement célja az illetéktelen belépés és kilépés megelőzése, és a magán- és köztulajdon közötti világos különbségtétel. Ez a különbségtétel két okból fontos: a jogos tulajdonosnak a tulajdonlás érzése és az általa a nem oda tartozók figyelmeztetése miatt, másrészről, hogy a betolakodók nehézségekbe ütközzenek a bejutásnál. A Territorial Reinforcement nem ugyanaz, mint a területi védelem, de a célja mindkettőnek ugyanaz: a betolakodók távoltarása az ingatlantól.

A CPTED négy alapelve:

- Természetes felügyelet
- Natural Access Control
- Territorial Reinforcement
- Karbantartás.

Egyértelmű különbséget tehetünk a köz- és magánterületek között természetes és mesterséges módon is. Élő sövények és a terep adottságai hatékony módjai lehetnek az ingatlan határvonalainak meghúzásához. A derékig érő kerítéseket ugyan könnyű átmászni, de ezek hatékonyak a határok létrehozásában. Az ingatlan határainak megszabásánál a kerítéseket és tereptárgyakat kellően alacsonyan kell tartani, minthogy ezek láthatóan tarják az oldalvonalakat nem engedve teret a rejtett területeknek. Riasztó vagy kamerarendszer alkalmazása esetén táblák és ablak matricák hozzá tudnak járulni az előbbiek elriasztó erejéhez. Ezen jelek feltűnő helyeken való kirakása figyelmezteti a lehetséges elkövetőket, hogy a kriminális tevékenységet rögzítik, illetve reagálnak arra.

A belső terület az épület nyílászárói és falait által határolt terület. Erre legalább olyan figyelemmel kell lennünk, mint a külső területekre. A belső terület védelmét általában zárakkal, kapukkal, zsiliprendszerrel, kamerával és riasztó rendszerekkel valósítjuk meg. A zárak és kulcsok használatának célja a betolakodók kívül tartása. Egy elektronikus belépést felügyelő rendszer szintén hasznos eszköze a belső terület felé irányuló forgalom ellenőrzésének. Végül, a riasztó rendszer figyelmeztet, amikor a területet megsértették.

A kamera fontos kontroll lehet, események esetén pedig bizonyíték erejű. Ha illetéktelenek a tulajdonos tudomása nélkül tudnak másolatot készíteni a kulcsokról, az a biztonság komoly gyengeségét jelenti.

A belső tér a biztonság utolsó szintje, amely az épület belső terét foglalja magában. A biztonsági kamerák hatékony eszközei a belső tér ellenőrzésének, melyek felvételei bizonyítékai lehetnek a későbbi nyomozásnak. Védhető a belső tér mozgásérzékelőkkel, melyek érzékelik a betolakodók, őrök jelenlétét. Elektronikus belépést ellenőrző rendszer szintén alkalmas a forgalom ellenőrzésére és az illetéktelenek védett területre való belépésének megelőzésére.

ÚTMUTATÓ AZ OBJEKTUMVÉDELMÉHEZ

Szögezzük le: megkerülhetetlen védelem nincs, de a kockázat minimalizálható akkor, ha követünk egy elfogadott sémát. Javaslataim az alábbiak:

- Professzionális magánbiztonsági szolgáltatót válasszunk, referenciával, gyakorlattal!
- Alkalmazzunk zsiliprendszeres beléptetést, különösen az üzleti objektumoknál!
- Kizárólag biztonsági ajtókat és reteszzárakat alkalmazzunk!
- Használjunk kulcs-felügyeleti stratégiát! Abban az esetben, ha nem tudjuk, kinél vannak kulcsaink, vagy akiknél találhatóak, lemásolhatják-e azokat a beleegyezésünk nélkül, komoly rés van a biztonsági tervben. Elsőként fizikailag védeni kell az ajtókat, majd biztonságban tartani a kulcsokat egy felügyeleti stratégia kialakításával.
- Építsünk ki rendőrségre, vagy a biztonsági felügyeleti céghez bekötött riasztórendszert!
- Egy ellenőrzött riasztórendszer két alapvető célt szolgál: beindítja a szirénát, mely a betolakodót elijeszti, másodszorra riasztja a rendvédelmi szakembereket, akik reagálni tudnak a betörésre.
- A hivatkozott W. Deutsch ajánlása: "Floor Marshall" kijelölése.
- Erre leginkább akkor kerülhet sor, ha nem használunk biztonsági szolgálatot. A Floor Marshall egy olyan önkéntes a szervezetben, akinek feladata az ismeretlen látogatók megközelítése és az arról való meggyőződés, hogy legális céljuk van-e a területen tartózkodásra. Illetve ugyanő más alkalmazottak részére olyan személyeket biztosít, akik jelentik a gyanús egyéneket. Ez társasházaknál is megszervezhető.
- Elektronikus belépést ellenőrző rendszert telepítsünk!
- Ez az üzleti objektumoknál ma már megkerülhetetlen. A mechanikus zárak "nem hazudnak". Az ajtózárak elektronikus belépést ellenőrző rendszerrel való javításával azonban rögzíthetjük azt, aki kinyitja, vagy megpróbálja kinyitni az ajtót. Ez az információ hatalmas segítség, ha nyomozásra van szükség a biztonság megsértése miatt. Emellett a rendszer lehetővé teszi elektronikus kulcsok azonnali hozzáadását vagy elvételét. Ez kiküszöböli az elvesztett vagy ellopott kulcsok miatti védtelen állapotot, és megengedi az időn, dátumon vagy jogosultsági szinten alapuló testre szabott belépési privilégiumok kijelölését.
- Videófelügyelet használata.
- Nem csak a terület ellenőrzésének képességét javítják a kamerarendszerek, hanem hasznos bizonyítékot és információt szolgáltatnak, ha nyomozásra van szükség egy balesetnél, támadásnál vagy lopásnál. Az alkalmazottaknak titokban kell tartaniuk a felügyeleti rendszerek alkalmazását.
- Ismeretek szerzése a bűncselkemények megelőzéséről.

KIEGÉSZÍTÉSÜL

Amíg a terület és a belső rész védelmében vannak átfedések (pl. őrök és kamerák, melyek meg tudják védeni a kettőt), ezen három szintnek, és mindegyik szinten két vagy három objektumvédelmi intézkedés létrehozásának jegyében való gondolkodás segít végrehajtani az alkalmas objektumvédelmi intézkedéseket.

Az angol irodalomban a Crime Prevention Through Environmental Design (CPTED) a bűncselekmények végrehajtását bátortalanító gátló elvek sora. A koncepció egyszerű: Az épületeket és ingatlanokat a természet erőinek és a természeti csapások károsító hatásának

megelőzésére tervezték; a bűn megelőzésére is megtervezettnek kell lenniük. Ezen elveket használhatjuk az otthoni irodák, és felhőkarcolók esetében is. A megelőző felmérés, tanácsadás cégünk szolgáltatásai között is elérhető, s keresett.

A Natural Access Control rendszer olyan elemeket használ, mint a járdasziget, járda vagy ajtók, melyek a gyalogos- és a járműforgalmat irányítják az ingatlanunkon. A rendszer célja a kockázat észlelésének előidézése a lehetséges elkövetők gondolataiban az ellenőrzés érzésének kiiktatásával.

A Territorial reinforcement szándéka nem annak megelőzése, hogy valaki területünkre belépjen, a betolakodók kívül tartásához őrökre, kapukra, szögesdrót-kerítésekre és hasonló dolgokra van szükség. Ennek célja inkább a lehetséges elkövetők számára annak az üzenete, hogy az adott terület máshoz tartozik. A CPTED más elveinek kombinálásával hatékony lehet a kriminálprevencióban.

Felhasznált irodalom

[1] KISS Sándor: Biztonságtechnika alapjai. Főiskolai jegyzet, Budapest, 2004. Zrínyi Miklós Nemzetvédelmi Egyetem, Bolyai János Katonai Műszaki Főiskolai kar

[2] MERZ, Hans A. és BOHNENBLUST, Hans megállapításai itt: Cost/Effectiveness Analyses and Evaluation of Risk Reduction Measures, 2-nd World Congress on safety Science Budapest, 1994.

[3] SOUKAS, Iuko: On the reliability and validity of safety analysis (Espoo, 1989). Innen: Kiss Sándor im. 20. p. A terminológiát Gál Csaba használja először, lásd ugyanitt

[4] McCLAY, R. E.: Using Task Analysis to Estimate the Risk of Human Error (2-nd WCOSS Budapest, 1994)

[5] http://bizsecurity.about.com/od/physicalsecurity/a/What_is_physical_security.htm

[6] TRUMP, Kenneth S. – a Nemzeti Iskolai Biztonság és Biztonsági Szolgáltatások, Cleveland-i, nemzeti konzultációs, iskolai biztonságra és vészhelyzetekre felkészítő tréningre és konzultációra specializálódott cég elnöke in: American school Board journal/February 2007, p. 26-29.

[7] http://www.counterterrorbusiness.com/features/93-event-security/481-bringing-home-the-gold-in-event-security

[8] JACOBS, Jerome, ©27-01-2009.
Forrás:
http://www.iacpo.org/index.php?option=com_k2&view=itemlist&layout=category&task=category&id=5&Itemid=130

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Répás József
jozsef_repas@hellokity.com

PIEZOELEKTROMOS ANYAGOK BIZTONSÁGTECHNIKAI ÉS KÖZLEKEDÉSBIZTONSÁGI ALKALMAZÁSAI

Absztrakt

A piezoelektromosság 1880-as felfedezésekor a gyakorlati alkalmazásokon még nem gondolkoztak, ám az első világháború utolsó évében megjelentek az első szabadalmak és egy évtized múlva a piezoelektromos kristályok a modern elektrotechnika nélkülözhetetlen eszközei lettek. Piezoelektromos anyagokat gyakran és sok területen használunk, többek között a biztonságtechnikában is. Jelen cikk célja összefoglaló képet adni a piezoelektromos anyagok felhasználási területeiről működésükről és bemutatni néhány új lehetőséget a jövőbeni alkalmazásukra.

In 1880, time of discovery of piezoelectric the practical applications has not yet been thought, but the in the last year of the First World War appeared the first patents and a decade later, the piezoelectric crystals have become an indispensable tool of modern electrical engineering. Piezoelectric materials are often used in many areas, including in the security market as well. This article is designed to give a general picture of the areas of their operation and use of piezoelectric materials to introduce some new possibilities for their application in the future.

Kulcsszavak: *piezo kristály, piezo film, ultrahang detektor, rezonátor ~ piezoelectric crystal, piezoelectric film, ultrasonic detector, resonator*

PIEZOELEKTROMOSSÁG

A piezoelektromos anyagok kutatása a 19. században kezdődött. A jelenséget 1880-ban fedezték fel a Curie fivérek turmalin kristályon. Rövidesen több kristályon tapasztaltak hasonló hatást. Gyakorlati alkalmazáson azonban egyáltalán nem gondolkodtak. A piezoelektromos anyagok széleskörű felhasználására az elektrotechnika, főként az alaktronika rohamos fejlődése adta meg a lehetőséget. Az első világháború utolsó évében jelentek meg az első szabadalmak, s egy évtized múlva a piezoelektromos kristályok a modern elektrotechnika nélkülözhetetlen eszközei lettek.[1]

Egyes kristályokban a különböző előjelű töltéscentrumok mechanikai deformáció hatására szétválnak, ezáltal a kristály szélei között elektromos feszültség alakul ki. A folyamat megfordítható: ha az ilyen, ún. piezoelektromos anyagokra elektromos feszültséget kapcsolunk, akkor hosszúságuk megváltozik. Ezzel a módszerrel a távolság finoman, akár atomi méretekben is szabályozható.[2]

Piezoelektromosak azok az anyagok, amelyekből megfelelően kivágott vagy kialakított lemezek nem csak kondenzátorként, hanem mechanikai elektromos átalakítóként is használhatóak. A „piezo" szó görög eredetű, nyomást jelent. A piezoelektromos anyagon felületén mechanikai igénybevételkor elektromos töltés kialakulása figyelhető meg. A keletkezett elektromos töltés és az alkalmazott húzó ill. nyomó erő között lineáris összefüggés figyelhető meg. Amikor Pierre és Jacque Curie a piezoelektromos hatást a turmalin után kvarckristályon is észlelték, sikerült a jelenség fordítottját is kimutatniuk.

Direkt és reciprok piezoelektromos hatás

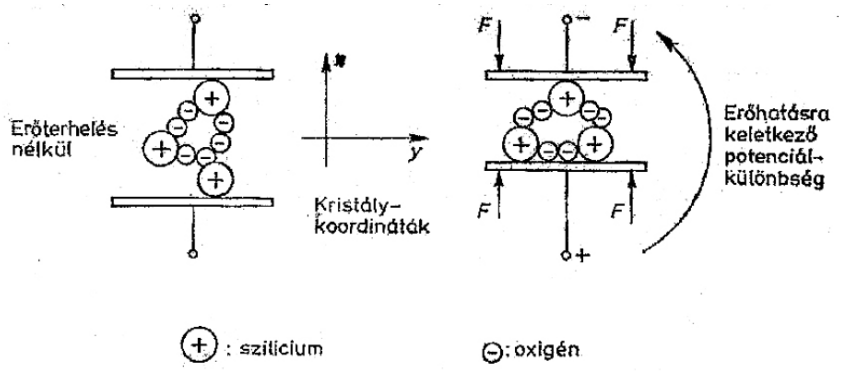
A piezoelektromos dielektrikumok ugyanis elektromos feszültség hatására mechanikai deformációt szenvednek. A mechanikai deformáció hatására keletkezett elektromos feszültség okát közvetlen (egyenes, direkt) piezoelektromos hatásnak nevezik. Az elektromos feszültség hatására keletkezett mechanikai deformáció oka a fordított (reciprok) piezoelektromos hatás.[3]

A keletkezett feszültség: $$U_f \cong \frac{1}{\mathbf{e_p}} \cdot \frac{l_p}{A_p} \cdot f_F$$

ep: kristályállandó — lp: a kristály hossza

Ap: a kristály felülete — ff: a felületre ható terhelés

A keletkező feszültség magyarázata (1. ábra), hogy a megfelelően kimetszett poláris kristálylapka felületein rácsdefiníció miatt szabad töltéshordozók jelennek meg. Elvileg ez az átalakító csak adott irányú erő, illetve elmozdulás érzékelésére alkalmas. Aktuátorként hasonlóan működik, ekkor a villamos feszültség hatására jön létre erő, illetve elmozdulás.[4]



1. ábra. Kristályban keletkező feszültség magyarázata [5]

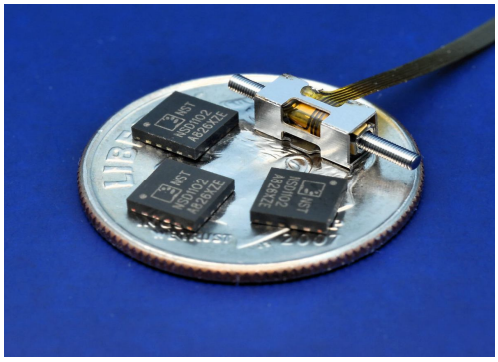
Piezo aktuátor és motor

Az aktuátor elektromos árammal, olajjal, vagy levegővel működtetett beavatkozó elem, amely képes valamilyen irányító jelnek megfelelő hatás kifejtésére.[6] A piezoelektromos mikroaktuátorokat nagy sikerrel lehet, és alkalmazzák is nanométeres feloldású pozícionálásokra. Jellemző rájuk a kb. 1 µm-es tartomány és az ezen belüli nagy, nm-es feloldás, a jó frekvenciakövetés és a viszonylag nagy kifejtett erő. Kedvező tulajdonságai:

- gyors működés
- nagy merevség
- alacsony energia disszipáció
- magas hatásfok

A piezokerámia hátrányos tulajdonsága, hogy feszültség hatására bekövetkező alakváltozása meglehetősen kicsi (0,1 %). A piezokerámia által kifejtett erő viszonylag nagy, ez lehetőséget ad arra, hogy mechanikai áttétekkel növeljük az elmozdulást.

Az optikai piezo aktuátorok a fény energiáját használják fel működésük közben. Ennek igen nagy előnye, hogy teljes mértékben megszüntethető az induktív zaj. Nincs szükség szigetelésre és érintés nélküli kapcsolat könnyen létrehozható. Az optikai piezoelem, bizonyítva a fotostrikció jelenségét, számos kutatás alanya. Felhasználásával mozgó mikrorobotot, illetve mikrorelét fejlesztettek ki.[7] A mikrorobotok esetében piezo motorokat alkalmaznak (2. ábra).

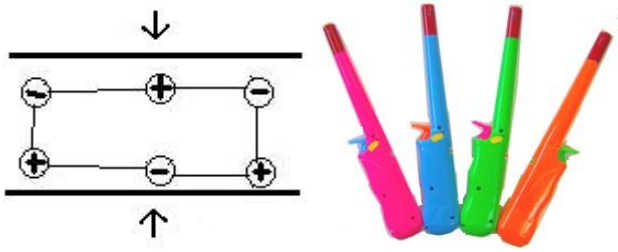


2. ábra. Piezo motor [8]

A piezoelektromos motor működése azon alapul, hogy elektromos mező hatására megváltozik a piezoelektromos kristály. A piezoelektromos motoroknál kihasználják a reciprok piezoelektromos hatást. Magas frekvencián vezérelve a kristályokat körülbelül 800 mm / s, vagyis majdnem 2,9 km / h sebességet érhetünk el.

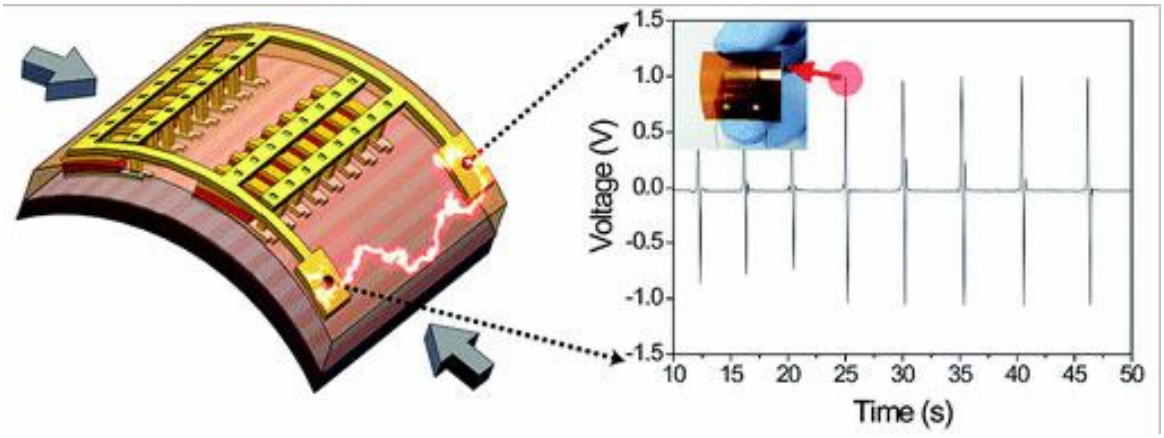
Gázgyújtó és nanogenerátor

Az egyik leggyakrabban alkalmazott kristály a kvarc, mely hatszöges rendszerben kristályosodik, ahol a rácspontokban pozitív és negatív ionok helyezkednek el felváltva. Egy ilyen kristályt két fémlap közé helyezve, majd összenyomva azt, a fémlemezek töltöttekké válnak, amivel elektromos szikrát lehet gerjeszteni (öngyújtó, gázgyújtó).[11]



3. ábra. Hatszöges rendszerű kvarc kristály és piezo gázgyújtó [9][10]

A piezoelektromos anyagoknak ezt a tulajdonságát kihasználva készítenek kisméretű ún. nanogenerátorokat. A nanogenerátor szintén a piezoelektromos hatás alapján üzemel. A kutatók hosszas kísérletezéssel fejlesztették ki azokat a nanotechnológiai módszereket, amelyekkel szinte atomról-atomra "szerelték össze" az első nanogenerátort. Először hatoldalú hasáb alakú, cink-oxid (ZnO) nanodrótokat növesztettek sűrűn egymás mellé egy szögletes alaplapra. Azért választották a generátor fő részeként a cink-oxidot, mert ennek az anyagnak megvan az a ritka képessége, hogy piezoelektromos tulajdonsága mellett egyben félvezető is. A felfelé meredező nanodrótok fölé egy másik szögletes lapot: platina-bevonatú, barázdált felületű szilícium-elektródát helyeztek el. Amint mozgás vagy erőhatás következtében a szerkezet oldalvást elmozdul, a nanodrótok meghajlanak az elektród alatt, és piezoelektromos tulajdonságuk következtében elektromos töltéseket produkálnak. A kutatók 2008-ban 6 négyzetmilliméter nagyságú nanogenerátorral 10 mV feszültégű és 800 nA erősségű áramot tudtak előállítani.

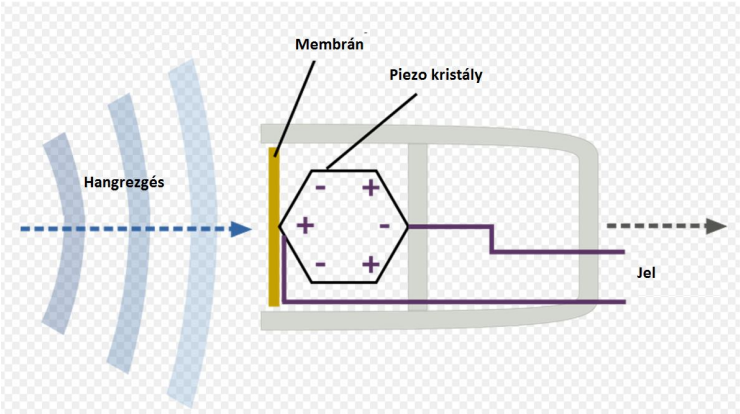


4. ábra. Nanogenerátor [13]

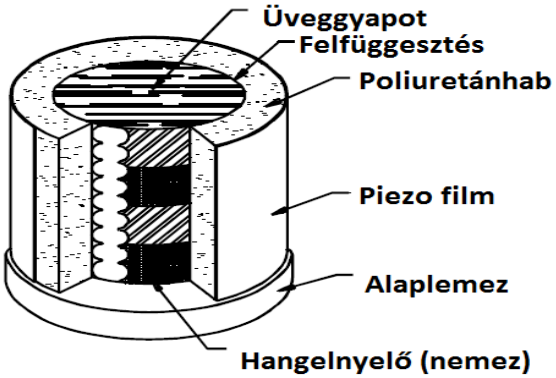
Mára a piezoelektromos nanocsöveket tartalmazó generátor elegendő energiát képes szolgáltatni a kisebb elektromos eszközök működéséhez.[14]

Piezo mikrofon és hangszóró

A piezoelektromos jelenség alapján működő mikrofonban legnagyobb feszültségváltozást a Seignette-só kristály ad. Két összeragasztott kristályt 3 ponton befogva a 4. pontra a membrán által közvetített hangfrekvenciás rezgést adva kapjuk a legegyszerűbb felépítésű kristálymikrofont (5. ábra). A mikrofon volt nagyságrendű feszültséget ad, impedanciája kapacitív. A kristály hőre és nedvességre érzékeny.



5. ábra. Piezoelektromos mikrofon Készítette: Répás József 2011

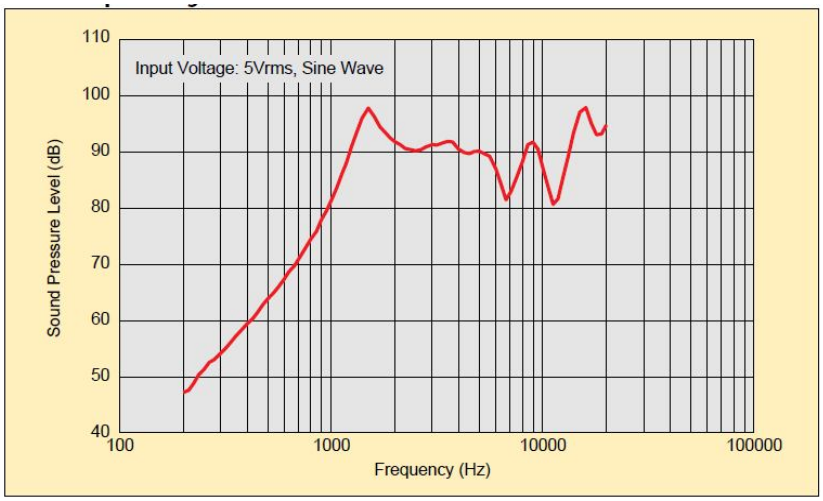


6. ábra. Pioneer Electronics piezo hagszórójának felépítése [15]

A Pioneer Electonics a piezoelektromos filmet fülhallgatókhoz alkalmazta (6. ábra), majd a Gallo Acoustics fejlesztett 52 µm vastagságú filmből kiváló hanghűségű hangsugárzót 2 kHz-es frekvencia fölé. A hangszórónak 330 °-os vízszintes szórása volt /ez 10 darab hagyományos hangszóróénak felel meg/, rendkívül széles dinamikatartománya, nagyon gyors impulzus-válasza, így a hűen reprodukálta a legmagasabb frekvenciákat is. Újszerű hangszórók fejlesztésekor a vékony kivitel, a kis súly és a konformitás játszott szerepet. Ilyenek voltak az ún. „felfújható hangszórók", például a lufi és egyéb felfújható, zenélő játékok és a hangos üdvözlőkártyák.

Napjainkban piezo hangszórókat használnak ébresztőórákban, egyéb elektronikus eszközökben és házimozi rendszerek magassugárzójaként. Az egyik legkisebb (19,5 mm * 14,1 mm * 0,9 mm) piezo hangszóró 92 dB ±3 dB hangnyomásszinttel és 0.9 µF ±30%-os kapacitással bír (7. ábra). Frekvenciaátvitele a 8. ábrán látható.

7. ábra. Ultra vékony és vízálló piezo hangszóró[16]



8. ábra. Ultravékony és vízálló piezo hangszóró frekvencia-átvitele [17]

Számos előnyük van a hagyományos hangszórókkal szemben, mivel ellenállnak a túlterhelésnek, nagyfrekvenciás teljesítményük növelhető így speciális körülmények között is alkalmazható. Például vízben sonárként, a szilárd kialakítás miatt ellenáll a tengervíznek. Piezoelektromos anyagokat már az 1940-es években alkalmaztak hidrofonokban és sonárokban. Új hidrofon technológia a búvárok által használt ultrahangos képalkotás.

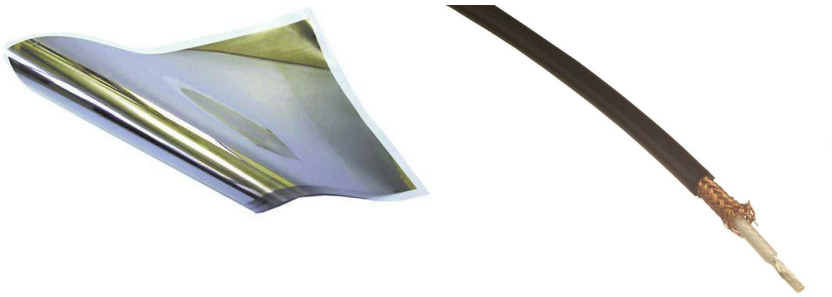
Piezoelektromos film

Piezoelektromos film (9. ábra) egy jelátalakító, ami a technológiában rejlő lehetőségek kiaknázását teszi lehetővé. Felépítése a 10. ábrán látható. Piezo film a nyomó vagy húzó mechanikai behatás hatására arányos feszültséget termel. Lehetővé teszi rendkívül megbízható és alacsony költségű rezgésérzékelők, gyorsulásmérők kialakítását. Alkalmazható 1 kHz és 100 MHz közötti frekvenciatartományban.

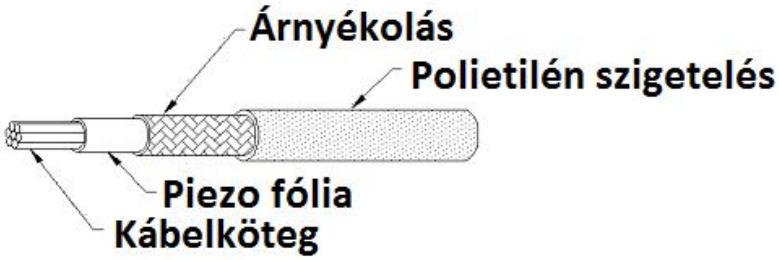
Különböző méretű és vastagságú egységekben kapható. Vékonyabb filmek leggyakrabban 28 és 52 mikron vastagságúak, jó mechanikai tulajdonságuknak köszönhetően. Vastagabb fóliát (110 mikron) akkor használnak, ha maximális stabilitás szükséges. Fémezése történhet porlasztott fémezéssel, vagy ezüst tintával. Előbbit mechanikai igénybevételkor alkalmazzák, utóbbit ha a jel/zaj viszonyok megkövetelik.

A piezo film mint érzékelő különböző kialakításban kapható és kerül felhasználásra:

- kábel
- bélyeg:
  - - ezüst tintás
  - - laminált
  - - rugalmas
  - - árnyékolt érzékelők
- fémezett fólia
- piezo kapcsolók és ultrahangos érzékelők



9. ábra. Piezo fémezett film fólia és piezo érzékelő koaxiális kábel [18]



10. ábra. Piezo kábel felépítése[19]

Piezo érzékelő kábelek biztonságtechnikai alkalmazása is jelentős lehet a későbbiekben. Külterületi védelem eszközeként hidraulikus lépésjelzők helyett alkalmazható lenne a piezo

érzékelő kábel is. Ezeknél az érzékelő elem szintén piezo kristály, de fagyálló folyadékkal feltöltött csövek helyett piezo kábellel is meg lehetne oldani az érzékelést. Védett sávon áthaladó személy által keltett talajnyomás-változást az érzékelő egység elektromos jellé alakítja át. Felderíthetetlen, mivel földfelszín felett semmi jele az eszköznek.

Piezo kristályt alkalmaznak még a gépjárműtechnikában, mint piezo működtetésű injektor. Optikai meghajtók pontos pozícionálása is piezokristályok segítségével történik, hasonlóképpen a modern fényképezőgépek autofocus beállításánál és giroszkópokban is. Nyomtatótechnikában is használatos, az Epson által kifejlesztett piezo technikánál, a tinta mechanikus nyomás hatására préselődik ki a fúvókából. Ezt egy kerámia piezo elem teszi lehetővé, ami nyomást gyakorol a tintacsatornára, kinyomva a tintát a fúvókából.

Piezo hangszedő többnyire az akusztikus gitárok hangjának erősítésére szolgáló hangszedő, mely a húrláb illetve az egész gitártest mechanikus rezgését alakítja elektromos feszültséggé. Hátránya a nagyon steril, éles hangzás, melyet sok esetben a gitárba beépített aktív hangszínszabályzóval szükséges szabályozni. Piezo hangszedő egyes típusai elektromos gitárba is beépíthetők, a meglévő húrláb lecserélhető méreteiben és működésében teljesen megegyező cserealkatrészre, így nincs szükség külön akusztikus gitárra, az elektromos gitárból is kicsalható az akusztikus hangzás, sőt a kétféle hangszedő (hagyományos és piezo) keverésével érdekes hangzásokat érhetünk el.[21] Londoni Surya diszkó pedig piezo generátorokat épített táncparkettjébe, hogy táplálják a villogó fényeket.

PIEZO KRISTÁLY A BIZTONSÁGTECHNIKÁBAN

Kerámia- piezo eszközök felhasználási területei igen szélesek. Mind az elektrotechnikában, mind a biztonságtechnikában. Biztonságtechnikai szempontból is széles körben alkalmazott. Mai építmények nagy részében alkalmazható, mint például metró állomások, bevásárlóközpontok, irodaépületek. Egy szóval mindenhol, ahol érthetően kell az információt eljuttatni a közönségnek, minden felesleges mellék zajtól mentesen, például egy esetleges katasztrófahelyzet esetén, de még egy átlagos kutyariasztóban is megtalálható.

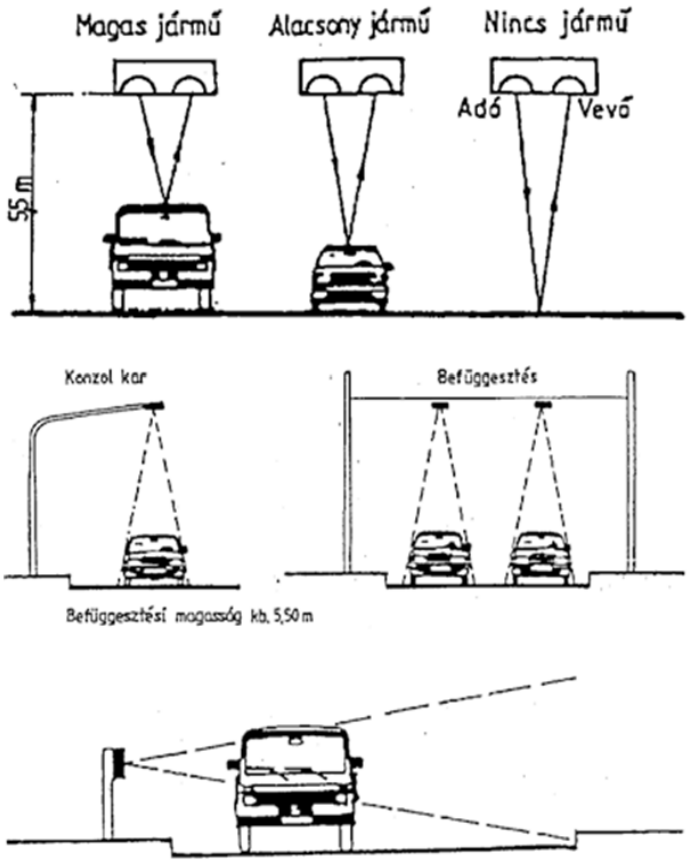
Kis teljesítményű piezo sugárzókat alkalmaznak például csipogókban, figyelemfelkeltő eszközökben. Nagy szerepe van a piezo anyagoknak riasztórendszerekben, ahol a fényjelzés mellett hangjelzéssel is jelzik az eseményeket. Gépjárművek biztonságának kialakításakor is nagy szerepe van a kis méretű, elrejthető, nagy teljesítményű hangforrásoknak, erre a feladatra is kiválóan alkalmas a kristály- piezo sugárzó (11. ábra). Piezo detektorokkal egyszerűen megoldható a bevásárlóközpontok alatti parkolókban várakozó gépjárművek biztonsága is, mert egyszerűen jelezhető, hogy melyik szint, melyik parkolóhelyén történik a gépjármű mozgatása. A közlekedésbiztonsági alkalmazáshoz hasonlóan a gépjármű felett elhelyezett adó-vevő segítségével.

11. ábra. Gépjárműben alkalmazható piezo sziréna[22]

PIEZO KRISTÁLY A KÖZLEKEDÉSBIZTONSÁGBAN

Víz alatti tájékozódás, különböző hanghullámok vétele, kibocsátása - akár az ellenség lokátorainak félrevezetéséhez - szintén piezo sugárzókkal történik, előnyös tulajdonságuk miatt, hogy ellenállnak a víznek. Víz alatti mikrofonok és hangsugárzók tökéletes alapanyaga.

Biztonság kialakításának egyik egyszerűbb formája lehet, ha például a postást látjuk el ultrahangos, piezo sugárzóval kialakított kutyariasztóval. Másik terület ahol piezo sugárzókat felhasználnak az úgynevezett ultrahangos detektorok, ahol mint rezonátor alkalmazzák.



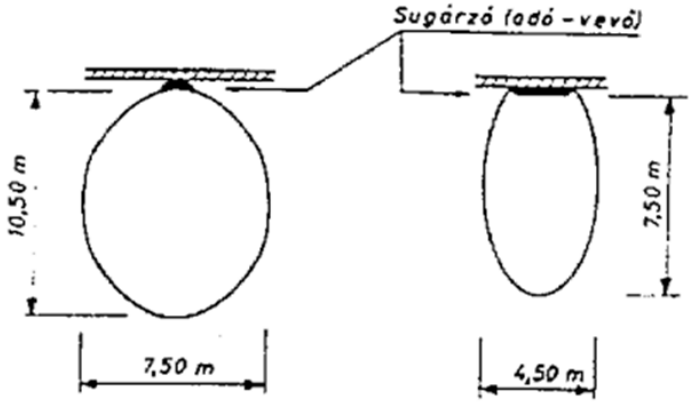
12. ábra. Adó-vevővel kialakított ultrahangos rendszer[23]

Ultrahang detektorok adó-vevő párból állnak, amelyek rendszerint egyetlen házban helyezkednek el. Működésük azon a jelenségen alapul, hogy az adó által kisugárzott ultrahangok a járművekről visszaverődnek, amelyeket azután a vevő érzékel, majd feldolgoz (12. ábra). Ultrahangos berendezések frekvenciája -amelyeket közutaknál használnak-, 18-40 KHz között vannak, ez ugyanis az emberi fül számára már nem hallható. Lehetséges mérési távolság 1-8 m között van. Visszaverődési időből a távolság közvetlenül számítható a következő kifejezés segítségével:

$$d = \frac{v * t}{2}$$

ahol: d = távolság
v = ultrahang terjedése a levegőben
t = idő.

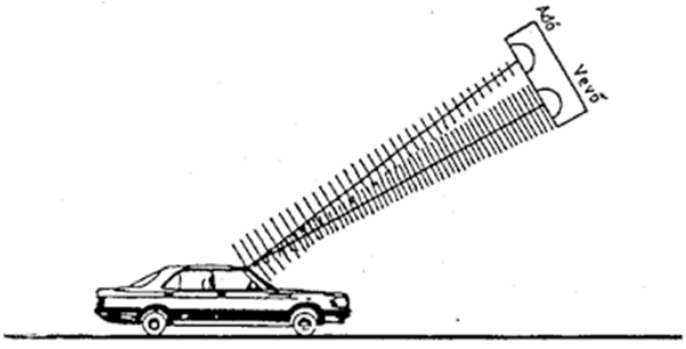
Számlálót azért kell osztani 2-vel, mert a jel útját oda-vissza kell számítani. Visszavert jelek tehát az érzékelőbe jutnak, amelynek sugárzási karakterisztikája a 13. ábrán látható, amely egyébként gyakran módosítható.



13. ábra. Ultrahangos adó vevő sugárzási karakterisztikája [24]

Ultrahangos érzékelőket kétféle módon használhatjuk fel attól függően, hogy a kisugárzott, illetve a visszavert jel mely paramétereit használjuk fel a vevőben. Ennek megfelelően:

- *Impulzus módszer:* Ekkor az adó periodikusan bocsát ki jeleket, impulzusokat. Vevő az impulzusok közötti időszakban figyeli a visszaverődött jeleket. Minél magasabb egy jármű, annál hamarabb érkeznek vissza a jelek. Ha a detektort a 12. ábra szerint az útpálya felett helyezzük el, akkor a jármű típusokat is meg tudjuk különböztetni. Oldalt elhelyezve a detektort, csak a kívánt forgalmi sávot ellenőrizzük. E rendszer egyébként alkalmas a parkolók foglaltságának ellenőrzésére is.
- *Doppler módszer:* Ellenőrzési elv a Doppler-hatáson alapul. Az ultrahangos mozgásérzékelő egyszerre ad és vesz visszaverődő ultrahanghullámokat. Ha a jelek utjában álló jármű van, akkor a visszaverődő hullámok frekvenciája ugyanakkora lesz, mint amit kisugárzott. Amennyiben mozgó tárgyak, vagy személyek kerülnek a jelsugár útjába, akkor az adó és vevő frekvenciája eltér egymástól, aszerint, hogy pl. a jármű távolodik vagy közeledik az ultrahang forrás felé. Ha távolodik, akkor a frekvencia csökken, ha közeledik, akkor nő. Ezen elv alapján mérhető a járművek sebessége. Ekkor a 14. ábra szerinti elrendezést kell alkalmazni. Látható, hogy az adó-vevő pár felül van elhelyezve, de a kibocsátott nyaláb ferde pályán halad. Erős szél, hó, esetleg más mellékzörejek esetében a pontosság jelentősen csökken.



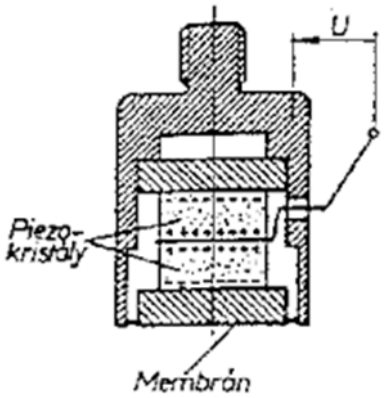
14. ábra. Doppler elven alapuló eljárás [25]

Rezgéskeltők feladata az ultrahang előállítása adás esetén, vétel esetében pedig a felfogott jelek-amelyek nyomóhatást fejtenek ki az érzékelőben-átalakítása villamos jellé.

- *Piezoelektromos rezonátorok:* A piezoelektromos hatás fordítottja rezgéskeltők készítésére használható.
- *Mágneses átalakítók:* Mágneses átalakítóknál azt a jelenséget használjuk fel, hogy a mágneses erőtér változásának hatására bizonyos anyagok a térbeli méreteiket

megváltoztatják. Méretváltozás a H mágneses térerősség növekedésével lehet növekvő, vagy csökkenő. A jelenséget magnetostriktív hatásnak nevezzük.

Piezo detektorok esetén is a piezoelektromos hatást használják fel. Egy ilyen, a nyomásváltozás hatására működő érzékelőt mutat a 15. ábra. A detektor közvetlenül a pályafelület alá, a haladási irányra merőlegesen, egyenes vonalakon fektetendő le. Az áthaladó kerekek nyomásának hatására keletkezik a feszültség, amelyet feldolgozunk. Mivel ez az érzékelő típus csak dinamikus hatásra dolgozik, ezért csak mozgó járművek megfigyelésére alkalmas. Felhasználható tengelyek számának meghatározására és tengelyterhelés mérésére.[26] A tengelyterhelés mérése közlekedésbiztonsági szempontból elsődleges feladat.



15. ábra. Piezoelektromos nyomásmérő [27]

A közlekedés biztonságának kialakításában egyéb módon is alkalmazható a piezo kristály. ABS rendszerek érzékelőjeként, keréknyomás ellenőrzőként használják. A piezo film felhasználására jelenleg is folynak kutatások. Kísérleteznek aktív rezgéscsillapítókkal, piezo polimereket próbálnak felvinni szilíciumra és az ún. Smart Skin kialakításánál is a piezo film alkalmazása lesz szükséges.

ÖSSZEGZÉS

Belátható, hogy a piezo kristály és a piezoelektromosság fontos szerepet játszik az elektrotechnikában, ám felhasználási területe túlmutat ezen. Mind a közlekedésbiztonság, mind a biztonságtechnika fontos alapeleme a piezo kristály és nem csak az ébresztő óránk csipogója, vagy egy dallamot játszó képeslap. A bemutatott felhasználási módokon túlmutatva elképzelhető, hogy a jövő nyitásérzékelőiben, vagy zárjaiban is találkozhatunk ezen alkatrésszel. A közlekedésbiztonsági alkalmazáshoz hasonlóan parkolóhelyek, mélygarázsok biztonságának növeléséhez is felhasználható az eszköz.

Felhasznált irodalom

[1][3] Gémesi József: *Piezoelektromos anyagok,* 3. oldal. BME Kézirat, Tankönyvkiadó 1964

[2] Botond Balázs: *Mi a piezoelektromosság?*
http://www.kfki.hu/chemonet/hun/teazo/miert/m01/218.html Letöltve: 2011-04-26 13:38

[4][5][7] Érzékelők és működtetők II. BME előadásvázlat 34-35. oldal.
http://www.fot.bme.hu/letoltes/ERZEKELOK%20ES%20MUKODTETOK/M%C5%B1k%C3%B6dtet%C5%91k.pdf Letöltve: 2011-04-26 15:44

[6] Aktuátor fogalma
http://www.idegen-szavak.hu/keres/aktuátor Letöltve 2011-04-26

[8] Piezo motor
Forrás: http://www.newscaletech.com/press_pics_hi-res/NSD-1102_3_motor_dime.jpg
Letöltve: 2011-04-26 14:38

[9] Kvarckristály
http://upload.wikimedia.org/wikipedia/hu/e/e5/SiO2Piezo.jpg Letöltve: 2011-04-26 14:17

[10] Piezo gázgyújtó
http://bolthely.hu/haztartasi/id/01646_Piezzo_toltheto_gaztuzhely-gyujto_szines_gazgyujto
Letöltve: 2011-04-26 14:16

[11] Piezoelektromosság http://hu.wikipedia.org/wiki/Piezoelektromosság
Letöltve: 2011-04-26 14:06

[12] Nanogenerátor
http://www.origo.hu/tudomany/20080218-nanotechnologia-energiatermeles-nanogenerator-es-energiaszal-segitsegevel.html Letöltve: 2011-04-26 14:23

[13][14] Nanogenerátor
http://www.mernokbazis.hu/cikkek/energiaellatas-nanogeneratorral
Letöltve: 2011-04-26 14:27

[15] Piezo film sensors Technikal manual 58. oldal
http://www.media.mit.edu/resenv/classes/MAS836/Readings/MSI-techman.pdf
Letöltve: 2011-04-26 19:19

[16] Ultra vékony és vízálló piezo hangszóró
Forrás: http://electronicdesign.com/Content/15000/02-Murata.jpg Letöltve: 2011-03-18 16:29

[17] Ultravékony és vízálló piezo hangszóró frekvencia-átvitele
Forrás: http://www.murata.com/products/catalog/pdf/p83e.pdf Letöltve: 2011-03-18 16:30

[18] Piezo fémezett film fólia és piezo érzékelő koaxiális kábel
Forrás: http://www.meas-spec.com/piezo-film-sensors.aspx Letöltve: 2011-04-26 20:30

[19] Piezo kábel felépítése
http://www.media.mit.edu/resenv/classes/MAS836/Readings/MSI-techman.pdf
Letöltve: 2011-04-26 20:50

[20] Piezo technika fogalma http://www.tintacentrum.hu/online/fogalomtar/piezo-technika
Letöltve: 2011-04-26 12:33

[21] Alan Ratcliffe: *Elektromos gitár kézikönyv* (ISBN 963-369-567-8) 2006 Alexandra kiadó

[22] Gépjárműben alkalmazható piezo sziréna
Forrás: http://www.techorium.com/images/products/Environmental-monitoring-system-mini-piezo-siren-enviromux-srn-m.jpg Letöltve: 2011-04-27 19:33

[23] Adó-vevővel kialakított ultrahangos rendszer
Forrás: http://eki.sze.hu/ejegyzet/ejegyzet/dr_olah/c2.htm Letöltve: 2011-04-27 20:32

[24] Ultrahangos adó vevő sugárzási karakterisztikája
Forrás: http://eki.sze.hu/ejegyzet/ejegyzet/dr_olah/c2.htm Letöltve: 2011-04-27 20:11

[25] Doppler elven alapuló eljárás
Forrás: http://eki.sze.hu/ejegyzet/ejegyzet/dr_olah/c2.htm Letöltve: 2011-04-27 9:48

[26] Dr. Oláh Ferenc: *Járműazonosító és helymeghatározó rendszerek* Egyetemi jegyzet
Forrás: http://eki.sze.hu/ejegyzet/ejegyzet/dr_olah/c2.htm Letöltve: 2011-04-30 20:10

[27] Piezoelektromos nyomásmérő
Forrás: http://eki.sze.hu/ejegyzet/ejegyzet/dr_olah/c2.htm Letöltve: 2011-04-27 9:56

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Földi László
foldi.laszlo@zmne.hu

IMPACTS OF CLIMATE CHANGE TO DISASTER MANAGEMENT TASKS WITH SPECIAL EMPHASIS ON CRITICAL INFRASTRUCTURES[1]

Absztrakt/Abstract

A globális klímaváltozás időjárás-módosító hatásai ma már a világon számos helyen, így Magyarországon is érzékelhetőek. A szélsőséges időjárási jelenségek mind gyakoribbakká válása komoly károkat okoz a gazdaságnak, a lakosságnak és megterhelő az emberek egészségére nézve is. Mivel a jelenségek és azok tendenciózus változásai ismertek, jó esély van arra, hogy alapos elemzéssel, megfelelő felkészüléssel, új eszközök és eljárások rendszerbe állításával az extrém időjárás olykor katasztrofális következményei megelőzhetőek vagy legalább enyhíthetőek legyenek. A cikk írója felvázolja és csoportosítja a klímaváltozás okozta fenyegetéseket, és igyekszik meghatározni azokat a válaszlépéseket, amelyekkel a katasztrófavédelem hatékonyan szállhat szembe ezekkel a kihívásokkal. A cikkben a védelmi feladatok bemutatása elsősorban a kritikus infrastruktúrák területére koncentrálódik.

The weather modification impacts of global climate change are already sensible in certain areas of the world and even in Hungary. More and more frequent occurrences of extreme weather phenomena cause serious losses to economy and population and also stresses human health. As the phenomena and their tendentious changes are well known, there is a good chance to evade or at least to ease the sometimes disastrous consequences of extreme weather with deep analysis, adequate preparedness and utilization of new equipment and methods. The author of this paper draws and configures the threats caused by climate change and attempts to determine answers and reactions that would useful for disaster management to efficiently face these challenges. In this paper the presentation of defence activities is focused on the area of critical infrastructures.

Kulcsszavak/Keywords: *globális klímaváltozás, katasztrófavédelem, kritikus infrastruktúrák ~ global climate change, disaster management, critical infrastructures*

[1] The paper has been supported by the Bolyai János Research Scholarship of the Hungarian Academy of Science

INTRODUCTION

Long range global climate forecast models dealing with climate change and irregular weather situations that occur more and more often are signing an imminent and growing danger to the critical infrastructure. This way, elaboration and evaluation of experiences from functional disorders of critical infrastructures emanating from extreme weather conditions are essential to shaping the actual reactions and future solutions of disaster management.

Forecasts concerning global climate change and climate models designate in general, that the load to critical infrastructure will rise heavily. In Hungary, the growing impact to critical infrastructure comes from the increasing amount and intensity of natural disasters that are consequences of the climate change process. Of course, extreme weather situations do not always mean disasters. The difference is easily separable from the definition of disasters. The circumscription makes the difference clear between extreme events and disasters of a natural origin.

EFFECTS AND INDICATORS OF CLIMATE CHANGE

Due to climate change, there are several negative consequences to the humans and/or the environment that can be grouped as primary and additional effects.

Primary effects are which directly come with climate change:

- Extreme low/high temperature;
- Extreme amount of precipitation (heavy rainfall, thunderstorm, drift, snowfall);
- Windstorm (gale, twister).

Secondary effects can be emanated from the primaries, occasionally as a combination of two or three of them:

- Flood, drainage;
- Mudflow, earthslide;
- Drought, desertification;
- Intensive fires, increase of explosion danger;
- Damage of critical infrastructure, disturbances in public utilities and other services, formation of shortages;
- Formation of negative consequences on sanitary and psychic human comfort;
- Social functional disturbances in financial, economic and/or administrative areas, e.t.c.

Primary effects and their consequences, the secondary effects together can cause disastrous events, which depend on their size, duration and the need of countrywide cooperation against them. Primary and secondary effects can be characterized with indicators, the so called primary and secondary climate indicators.

Primary climate indicators (meteorological indicators):

- Air temperature (average temperature, maximum and minimum values, their frequency and length);
- Ocean surface water temperature;
- Amount of precipitation (average amount, short time precipitation maximum, frequency of heavy rainfalls or snowfalls);
- Wind speed and direction (average wind speed values and maximums);

- Frequency and strength of storms.

Secondary climate indicators:

This group of indicators is further divided by environmental, ecological, health (sanitary), social-economical features.

Environmental indicators:

- Amount of ice in polar regions and in Greenland (size of territory covered by ice);
- Water levels in oceans, lakes and rivers;
- Date of frost-point temperate in calendar and duration of snow on lands;
- Level of ground water;
- Air and water quality;
- Humidity of soil;
- Forest and bush fires, e.t.c.

Ecological indicators:

- Date of leafing, flowering and defoliation of trees in calendar;
- Appearance and disappearance of butterfly species;
- Date of coming and leaving of birds of passage in calendar;
- Time of sittings of birds;
- Changes in populations of different species;
- Appearance of insects en masses;

Health (sanitary) indicators:

- Mortality due to extreme weather;
- Change in distribution of disease carriers, vectors;
- Appearance of new types of diseases, e.t.c.

Social-economical indicators:

- Financial losses due to bad weather (insurance costs);
- Water supply (shortages, restrictions to water consumption);
- Changes in agricultural production;
- Changes of human habits of life, e.t.c.

INCREASING RISKS FOR CHEMICAL INDUSTRY CAUSED BY THE CLIMATE CHANGE

Extreme weather can cause serious structural damages to human environment. Negative consequences can be deeper, if additional hazards exist in the effected area. In some cases, a serious natural event is only gives initiative of a disaster with the so called “domino-effect”. It means that a primary phenomenon can cause a series of incident with accumulated consequences. One of the critical areas is the chemical industry where dangerous goods can be stockpiled in great amount.

The adequate defence of industrial establishments producing dangerous substances is part of the common defence policy. In this field, a lot of national and international legislations exist that demand obligatory defence measures from the owners and operators of dangerous industrial installations.

In our country, the Act LXXIV of 1999 on the management and organization of the prevention of disasters and the prevention of major accidents involving dangerous substances defines the phrase "disaster" (or "catastrophe") as follows: "Disaster means a state or situation (with natural, biological, human or other origin)… which threatens human life, health, properties, support of population, natural environment or natural resources in such a way, that prevention, response, relief and elimination of damages exceeds the capabilities of regular forces and their normal co-operation forms and needs special counter-measures and synchronized co-operation of local authorities and governmental forces and sometimes international contribution."

During the use of hazardous materials certain events can happen, that can cause serious accidents such are:

- Large scale fires and/or explosions;
- Emission of toxic materials from enclosed technological systems.

In chemical industry, most of the accidents caused by emission problems from production or storage devices. In details, reasons for serious accidents could be the followings:

- Damage of a container or pipeline containing flammable material, emission of the dangerous substance to the environment, where the chemical mixed with air is producing a gas or vapour cloud that causes fire.
- Damage of a container or pipeline containing toxic material, emission of a toxic gas or vapour cloud that disperses in the vicinity causing risk for human life and health.
- Vapours from an explosive material container spill out to the environment forming explosive mixture with air.

In average circumstances, greatest risks to the human life, buildings and the environment are heat waves, overpressure and explosions where flying debris can cause mechanical wounds. These effects mean dangers in approximately some hundreds of meters from the centre of the accident. But sometimes, mainly in extreme weather situations, gas or vapour clouds can have lethal concentrations even in some kilometres of a distance.

In Hungary, main points of interest during the investigation of weather consequences can be:

- Floods caused by heavy rainfalls;
- Structural damages caused by extreme cold and icing;
- Extraordinary windstorms, supercells.

Focus of further investigations and researches can be the meteorological indicators. Main obstacle of these indicators' use in practice is the difficulty of their complicated quantification. For the use of these indicators in disaster management we need to know the primary and secondary effects of climate change more precisely. To get adequate numbers, deep analysis of event types initiated by them is also essential.

CONSEQUENCES OF CLIMATE CHANGE TO CRITICAL INFRASTRUCTURES

The National Climate Change Strategy for 2008-2025 includes effect of climate change to operability of critical infrastructures in many points. Situations and events emanated from nowadays weather anomalies are good starting points to build-up tasks of preparedness and reaction. In addition, to identify future production malfunctions, technology breakdowns and their possible consequences to other sectors of critical infrastructure it is imperative to reconsider some elements of operational safety that are not inspected or stated as non-relevant nowadays.

It is necessary to analyse the changes in climate that carry risks for critical infrastructures from many aspects. On one hand, it means the origin of resources bounded together to fulfil their functions, on the other hand, mean the allocation end-points. Other field of production malfunctions and technology breakdowns that can endanger security is the collapse of technological systems themselves and the damage in the environment as their consequence. Finally, the question that needs probably the deepest investigation is the problem and behaviour of risks arising from interdependencies.

So based on the above described the consequences and effects to the supply of population and to the distribution system must be revealed in the following situations:

- It is impossible to distribute the necessary raw material, product or service (resource in the followings) to the users on the essential infrastructure that is normally responsible for it due to obstacles emanating from modified weather circumstances.
- Although resources are accessible throw the essential infrastructure, but the functionally damaged system is unable to transport them to the users due to malfunctions caused by negative weather extremities.
- Existing weather circumstances are capable of damage the security system that stands against the environmental impacts of hazardous technology or resource used during production.
- There are disturbances in operation of a critical infrastructure that depends on other infrastructures exposed to extreme weather elements.

Growing impacts of climate change are new and arising aspects in defence tasks related to critical infrastructures, because they enhance their vulnerability. Probability of disturbances is expected to grow due to extreme weather phenomena especially in the following areas: road and railway transport, in electrical distribution system (damage of tower lines, span-wires), drinking water supply utilities (damage of water resources) and in connection with these in public services and info-communication.

Extreme weather events can cause a so called “domino-effect” in road and railway transportation networks. Consequences of a short-time current failure can grow up from local level to regional, national and even to international levels. Western European current failures in recent years can provide useful experiences for this. In 2003, about 30,000 passengers stalled on open railroad and needed help to reach the nearest railway station. As the impacts can appear directly or indirectly in many sectors at the same time, it makes the handling of these extraordinary situations even more difficult.

The above mentioned situations can take form because of extreme weather situations as weather components:

- can have direct impact to physical elements of critical infrastructures;
- can cause such environmental modifications, that neither preventive planning nor security systems for handling crisis situations can manage them.

Based on this, starting from the prognosed weather variations, in order to determine their threat to operational security of critical infrastructures, the followings are to be investigated

- extraordinary large amount of precipitation;
- heavy windstorms;
- unusual temperature fluctuation;
- radiations from extremely intensive natural sources (e.g. solar flares)

The fact, that these dangerous weather parameters can generate large modifications in environmental elements causing additional risks this way needs special attention. For example, an intensive precipitation zone can initiate spates going down the river endangering the stability of banks and bulwarks, in serious situations can cause floods. Earthslides caused by heavy local rainfalls can have similarly significant impact to critical infrastructures.

Constant heat waves are similarly dangerous for critical infrastructures that can go wrong due to structural damages. Water shortages caused by heat waves not only endanger technological water needs for critical infrastructural installations with large amount of water consumption (e.g. for cooling), but can degrease drinking water resources.

In Hungary, investigation of critical infrastructures with special attention to population support and settlement safety is a task of the National Directorate General for Disaster Management since 2001. As part of its annual plan it is an important task for the Directorate General to measure the states of essential services for the citizens as electrical, gas and drinking water (sewage-water) systems, certain types of transportation (road, railroad, inland water and air), telecommunication, information networks, power-supply (electricity, fuel, coal, natural gas and district-heating) and installations for flood control.

Climate change can amplify the above mentioned problems this way can increase the risk of damage to the critical infrastructures. Expected consequences of climate change in Hungary can be predicted as follows:

- Summers will be warmer and more arid;
- Winters will be milder with more precipitation;
- Weather extremities will be more frequent;
- More days with hotness and less with freezing can be expected;
- Risks of serious droughts and floods will simultaneously grow up;
- More serious and more frequent storms are expected;

So it is statable that climate change is such a phenomenon that increases the frequency of malfunctions in operation of critical infrastructures. However, its strength depends on many circumstances. Delay or cancellation of necessary maintenance works on safety installations against hectic variations of weather conditions and intensive harmful environmental events, reduction of budget on security structures can cause dramatic decrease of operational reliability of critical infrastructure elements. This way, some elements can not stand against the increased stress caused by repeated crisis situations and can not fulfil requirements on fail-safe operation. In our country most of the elements of critical infrastructures are operating near the maximum capacity, so the increased needs in case of critical situations caused by weather anomalies are hard to satisfy. In some cases, inadequate development of an area can slow down the advancement on other well funded fields of critical infrastructures through interdependency thus it can affect negatively the social development or operational readiness.

Cancelled measures towards risk reduction both on source and consumer sides there can be more and more difficulties with handling of crisis situations emanating from interruption of operational continuity.

KEY STEPS FOR EFFICIENT DEFENCE AGAINST THE ARISING THREATS

Most of the emerging problems can be handled as follows:

- Minimum requirements should be determined for factors influencing operational continuity and readiness capabilities of critical infrastructures.
- An adequate financing system should be established to form solid background to enhance the conditions to the appropriate operation of critical infrastructures.
- Elements of critical infrastructures should be identified that can be affected by harmful consequences of climate change.
- Periodic investigation of impacts of weather extremities should be a part of the operational continuity planning for the affected elements of critical infrastructures.
- Modifying effects due to climate change should be included to defence provisions and programs on critical infrastructures.
- Risk assessments should be carried out based on climate models to find optimal actions that guarantee the best and safest continual operation and availability of critical infrastructure elements.
- Common procedures should be formed in protection of with regional or global interdependencies tailored to the national defence structures.
- Necessary reserves and possibilities to apply alternative solutions should be improved during planning the protection of life and properties of population.
- Needs of significant amount of population, so called “climate refugees” should be taken into consideration during planning of adequate capabilities of certain critical infrastructures.
- Possible challenges of climate change should be included to institutional and technical development concepts of civil emergency management systems.
- Governmental, self-administrative, owner and operator tasks and responsibilities should be determined in the field of operation, maintenance and protection of critical infrastructures.
- Care should be taken on civilian preparedness in order to minimize damages and casualties in case of emergency situations.
- Procurement of new equipment should be necessary, as handling the consequences of more frequent and more intensive local and regional precipitations in some cases exceed the capabilities of regular engineering rescue tools. It needs additional extra founds to the annual budget.

It is essential to build up a system for protection of critical infrastructures against the harmful consequences of climate change that makes a common reaction possible from every related sector and installation in order to handle emergency situations effectively. International experiences in handling disastrous events are necessary to build in. Forming of integrated research teams is important to make risk assessments with scientific methods from as many points of view as possible. In addition, obtainment of a wide social support toward critical infrastructure protection is also needed, otherwise the efforts made in this field can be ineffective.

REFERENCES

[1] Nemzeti Éghajlatváltozási Stratégia (National Climate Change Strategy) 2008-2025, 75. o., http://www.kvvm.hu/cimg/documents/nes080214.pdf (2011. 08. 28.);

[2] Attila Horváth: Relationships of Sustainability, Climate Change and Security Policy. Review of the Air Force Academy. The Scientific Informative Review. Brasov, Romania. No 2/2007. pp. 65-68. ISSN 1842 - 9238 (peer reviewed)

[3] Dr. Halász László, Dr. Pellérdi Rezső, Dr. Földi László: Katasztrófavédelem I (Disaster management I.), ZMNE Elektronikus egyetemi jegyzet, 2009. https://olibx.zmne.hu/cgi-olib91/w207.bat?session=373703985&infile=&sobj=3725&cgimime=text/html

[4] Földi László, Halász László: Környezetbiztonság (Environmental security), Complex Kiadó (Kiskönyvtár a biztonságról, ISSN 2060-8047; 4.), 2009. Budapest, oldalszám: 419, ISBN: 978-963-295-020-4,

[5] Dr. Pálvölgyi Tamás: A klímaváltozás folyamata és társadalmi-gazdasági következményei (Course of climate change and its social-economical impact), http://www.eukn.org/Hungary/hu_hu/E_könyvtár (2011. 08. 11.);

[6] National Security and the Threat of Climate Change. The CNA Corporation final report. URL cím: http://securityandclimate.cna.org/report/SecurityandClimate_Final.pdf (2010. 09. 17.)

[7] Horváth Attila: Hogyan értessük meg a kritikus infrastruktúra komplex értelmezésének szükségességét és védelmének fontosságát? (How to explain the need of complex definition for critical infrastructure and the importance of its protection?) Hadmérnök on-line, Budapest, 2010. V. évfolyam 1. szám. pp. 377-386. ISSN 1788 1919. http://www.hadmernok.hu/2010_1_horvatha.pdf

[8] Nagy Rudolf, Földi László: A kritikus infrastruktúrák és védelmük nemzeti programja (Critical infrastructures and the national program for their protection), Polgári védelmi szemle, 2009./1. szám, 57-71. o. http://www.mpvsz.hu/letoltes/pvszemle/pv2009_1.pdf

[9] Horváth Attila: Az élelmiszerellátási lánc kritikus infrastruktúrái terrorfenyegetettségének jellemzői. (Characteristics of terrorist threat on the critical infrastructures of the food supply chain) Hadmérnök on-line, Budapest, 2009. IV. évfolyam 2. szám. pp.437-449. ISSN 1788 1919. http://www.hadmernok.hu/2009_2_horvatha.pdf

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. október

M. Mátyus - Gy. Kocsis - O. Boldis - A. Gachályi
matyum@freemail.hu - colonel1971@freemail.hu - ottoboldis@citromail.hu

DETERMINATION OF MORPHINE AND CODEINE IN SERUM AFTER POPPY SEED CONSUMPTION USING GAS CHROMATOGRAPHY – MASS SPECTROMETRY

Absztrakt

An analytical method is presented here for the assessment of morphine and codeine concentrations in human serum by employing mass spectrometry in the selective ion monitoring mode following its separation with gas chromatography. Deuterated (marked with heavy water) analogies of the analytes were used as surrogate internal standards. Samples were cleaned up using solid phase extraction. The target compounds were analyzed as pentafluoropropionic esters. The monitored ions were m/z=414, 577 and 361 [morphine], m/z=417, 580 and360 [D_3-morphine], m/z=282, 445 [codeine], m/z=274, 448, [D_3-codeine]. The recovery of the analytes from solid phase extraction was 70 to 80% (morphine) and 75 to 85% (codeine) at a concentration of 10 ng/mL. The limit of quantitation (confidence limit) was 0.87 ng/mL for morphine and 0.9 ng/mL for codeine. Calibration was accomplished employing blank human serum spiked with the analytes at various concentrations.

Egy analitikai eljárás került kidolgozásra a vérszérum morfin és kodein tartalmának meghatározására gázkromatográfiás-tömegspektrometriás technikával szelektív ionmonitorozás technikával. Az eljárással kísérő sztenderdként a vizsgált vegyületek deutériummal jelölt molekuláit alkalmaztuk. A minták tisztítása és kivonása szilárdfázisú extrakcióval történt. A vizsgált hatóanyagokat penta-fluoropropionsavanhidriddel származékoltuk. A mért inonok (n/z) morfin: 414, 577 és 361; morfin-D3: 417, 580 és 364; kodein: 282, 445; kodein-D3: 285 és 485 voltak. Az analitikai eljárás visszanyerési hatásfoka 10 ng/mL koncentrációknál morfinnál 70-80 % illetve kodeinnél 75-85 %. Az eljárás mennyiségi kimutatási határértékei morfinnál 0,87 ng/mL illetve kodeinnél 0,9 ng/mL. A kalibrációhoz humán szérumot használtunk úgy, hogy a vizsgált anyagnak a kalibrációhoz szükséges koncentrációjú elegyével jelöltük meg.

Keywords: *tiltott kábítószerek, anyagcsere, mák, GS-MS, morfin, ingyenes morfin, kodein ~ illicit drugs, metabolites, poppy seed, GS-MS, serum morphine, free morphine, codeine*

INTRODUCTION

Serum and urine samples are frequently tested to identify illicit drug consumption. The presence of illicit drugs or their metabolites in urine is proof of drug use, while their concentrations in blood are proportional to their effects upon the user. *[1-2]* The consumption of these drugs by the personnel of the Hungarian Defence Forces is strictly prohibited. In order to enforce this rule, urine samples are analyzed for the presence of compounds which would indicate heroin, morphine or codeine abuse. *[3-4]*

EXPERIMENT

Testing for illicit substances in biological samples is very difficult due to the fact that there are very small quantities involved, and the fact that these biological samples themselves contain many different substances, some of which could cause interference during the testing. It is therefore very important to perform some in vitro tests to determine how reliable the testing we do is. We need to test for these substances in normal human volunteers. Unfortunately, we run into a quandary here, because if we give illegal substances to human volunteers, it would be in fact unethical. In this situation, however, Hungary finds itself in a unique situation. Poppy seed (Papaver Somniferum), which contains morphine and related compounds in substantial amounts, is a staple item in the Hungarian cuisine, and it is routinely and regularly ingested by a large part of the Hungarian nation. No law restricts the amount of poppy seed contained in food and for example, up to 120 g is usually contained in a piece of poppy seed cake. Investigations performed in our laboratory show that adults excrete morphine and codeine in urine above the approved cut-off level for up to 3 days after eating one piece of this cake. *[5-6]* However, in Hungary there is a law *[7]* regulating the level of narcotics a Poppy-seed can contain that can be sold to the public *(Table: 1)*.

Drugs	Food group, type of food	Maximum Allowable Consumption
1. Morphine	poppy seed	30 mg/kg
2. Narcotin	poppy seed	20 mg/kg
3. Morphine & narcotin	poppy seed	40 mg/kg
4. Thebaine	poppy seed	20 mg/kg
5. Codeine	poppy seed	20 mg/kg

Table 1. The maximum allowable consumption of controlled material from natural origin allowed in food groups

Extracts of Poppy-seed were tested for the amount of Morphine is contained, at the level varied between 0-70 mg/kg. We decided to run tests on human volunteers after the ingestion of food articles containing poppy-seed in order to determine the abilities of our lab to detect small quantities of morphine and related substances. In this way, we can get adequate substation that gives real values. It also is ethical, but even then, to double check the ethics, we submitted our proposal to the Committee of Ethical Studies of the Institute of Health Protection, Hungarian Defense Forces, and it was dually approved prior to the beginning of the investigations.

EQUIPMENT

Analysis was performed on an Agilent 6890 gas chromatograph (GC) coupled with an Agilent 5973 single quadrupole mass spectrometer (MS; Agilent Technologies, Wilmington, DE). Samples were injected using an Agilent autosampler unit. The extraction of analytes was performed on a Bond Elute Certify cartridge (CP-Analitika Kft., Budapest, Hungary). Disposable equipment was used for sample preparation whenever possible, including pipette tips, vials, caps and solid phase extraction cartridges.

Gas chromatography conditions

1.0 µL splitless injections were made at 280 °C injector temperature. Carrier gas was Helium 6.0 grade (Messer Hungarogáz Kft., Budapest, Hungary) introduced at a flow rate of 1.0 mL/min. Separation was performed on a Varian FactorFour™ VF-5MS capillary column (length: 30 m, internal diameter: 0.25 mm, film thickness: 0.25 µm; CP-Analitika Kft., Budapest, Hungary). Oven temperature was kept at 100 °C for 1 min, followed by an increase of temperature of 20 °C/min to 220 °C, then 3 °C/min to 240 °C, then at 20 °C/min to 300 °C and was finally held constant for 5 min.

Mass selective detection

The transfer line temperature was 280 °C. Electron impact ionization was performed at 70 eV energy, 230 °C ion source temperature. Quadrupole temperature was 150 °C. The MS was operated in single ion monitoring (SIM) mode. Monitored ions are displayed in *Table 2*.

Name of compound	Purpose	Target ion (m/z)	Qualifier ion #1 (m/z)	Qualifier ion #2 (m/z)
Morphine pentafluoropropionic ester	analyte	414	577	361
Codeine pentafluoropropionic ester	analyte	282	445	
D_3-Morphine pentafluoropropionic ester	internal standard	417	580	364
D_3-Codeine pentafluoropropionic ester	internal standard	285	448	

Table 2. Monitored ions of analytes and internal standard compounds

Data acquisition and processing.

Data was acquired with the Agilent Chemstation Software (Kromát Kft., Budapest, Hungary). Peak areas were used for quantification.

Analytical results were produced using B.E.N. Software (a program designed to run on Windows Excel™ determining the analytical parameters of the GC-MS measurements) *[8]*.

MATERIALS AND METHODS

Chemicals

Morphine [100µg/mL in methanol], D_3-morphine [100µg/mL in methanol], codeine [100µg/mL in methanol] and D_3-codeine [100µg/mL in methanol] solutions were obtained from Cerilliant Company (Austin, TX).

Pentafluoropropionic anhydride (PFPA) and pentafluoropropanol were purchased from Sigma Aldrich Hungary Kft. (Budapest, Hungary).

Standard human serum was acquired from Promochem (Budapest, Hungary).

All other chemicals and solvents were obtained from Merck Kft. (Budapest, Hungary) and were analytical grade.

Solutions

Calibrations were done using the standard serum and were taken through the same preparation steps as the blood samples. Serum standards and blood samples were spiked with standard solutions A and B as well as the surrogate internal standard solution *(Table 3)*.

ID	matrix	volume	Volume of standard solution spikes (µL)			Morphine and codeine concentration (ng/mL)
			Standard solution B	Standard solution A	Surrogate internal standard solution	
Chemical standard	methanol	1 mL	0	5	1	50
Serum blank	blank serum	1 mL	0	0	0	0
Calibrator #1	blank serum	1 mL	1	0	1	1
Calibrator #2	blank serum	1 mL	2.5	0	1	2.5
Calibrator #3	blank serum	1 mL	5	0	1	5.0
Calibrator #4	blank serum	1 mL	10	0	1	10
Calibrator #5	blank serum	1 mL	0	2.5	1	25.0
Calibrator #6	blank serum	1mL	0	5.0	1	50
Calibrator #7	blank serum	1mL	0	10	1	100
Blood sample	serum	1 mL	0	0	1	

Table 3. Composition of calibrators, blanks and serum samples

pH=9 carbonate buffer solution. To 20 mL 0.2 mol/L sodium carbonate aqueous solution 230 mL 0.2 mol/L Sodium Hydrogencarbonate aqueos solution was added. The mixture was diluted with distilled water (LichroSolv® grade) to 1000 mL.

Morphine and codeine concentrations that were obtained during the analysis of the chemical standard were considered 100% in recovery experiments.

Standard solution A. 100 µL Cerilliant Morphine Solution and 100 µL Cerilliant Codeine Solution was diluted to 800 µL with methanol in a 2 mL silanized vial (CP-Analitika Kft., Budapest, Hungary). The solution was used for 1 week and stored at -20 °C.

Standard solution B. 100 µL Standard solution A was diluted 900 µL to with methanol in a 2 mL silanized vial (CP-Analitika Kft., Budapest, Hungary). The solution was used within 24 hours.

Surrogate internal standard solution. 100 µL Cerilliant D3-Morphine Solution and 100 µL Cerilliant D3-Codeine Solution was diluted to 800 µL with methanol in a 2 mL silanized vial (CP-Analitika Kft., Budapest, Hungary).

The solution was used for 1 week and stored at -20 °C.

Blood collection

Blood was collected in tubes with walls previously coated with sodium fluoride from healthy volunteers who had given their written informed consent in advance. The tubes were gently shaken for 30 seconds and then kept at 5 °C for 10 minutes. Centrifugation was done at 3000 rounds per minute for 10 minutes using an Eppendorf 584 Centrifuge (Eppendorf GmBH, Hamburg, Germany). 1 mL supernatant was then transferred to a 2 mL silanized vial for clean-up and derivation.

SAMPLE PREPARATION AND DERIVATION

Sample clean-up was performed by applying the supernatants to solid phase extraction cartridges containing a mixed special C_8 and strong cation exchanger sorbent *[9]*. Recovery of the analytes from solid phase extraction was assessed by processing three standard serum samples spiked with both compounds at a concentration of 10 ng/mL each. The column was pre-conditioned with 3 mL methanol and 3 mL pH=9 carbonate buffer solution. Serum samples previously spiked with the standard solutions were allowed to drip through at a rate of 1 mL/min.

After the sample passed through the sorbent the latter was washed with 3 mL distilled water and allowed to dry for 35 minutes *in vacuo* (-50 mm Hg). The analytes were eluted at a rate of 1 mL/min into a 2 mL silanized vial using 1 mL dichloromethane:propanol:ammonia 80:20:2 mixture. The elution process was repeated once. The eluted fractions were combined and desiccated at 36 °C under a gentle stream of nitrogen, using a Pierce Reacti-Therm™ Heating Module (Dr. Wéber Consulting Kft., Budapest, Hungary). The dry residue was reconstituted with 100 µL PFPA and 70 µL pentafluoropropanol, the vial was closed and kept at 60 °C for 30 minutes. After this period the solution was allowed to cool to room temperature and was then forwarded for analysis.

RESULTS AND DISCUSSION

The illicit consumption of drugs and psychotropics is a serious problem in modern societies. The specific and sensitive identification and quantification of these chemicals and their metabolites, as well as utilization of analytical data for the verification of the influence of illicit acute and chronic drug consumption on individuals involved in felonies therefore remains an important challenge.

A number of approaches have been established for the verification of illicit drug consumption. Urine is one of the most widely used sample for such investigations *[10-13]*. However, the collection of urine is not always feasible without invading the subject's privacy. In addition to this, urine analysis does not always provide evidence of a single intake since it takes time, usually a few hours, for urinary metabolite concentrations to reach the limit of detection *[10]*. Assessed concentrations are affected by fluid intake, nutritional regimen, age, consumption of pharmaceuticals and health status especially noting whether the person has circulatory or renal disorders, which raises the risk of obtaining false negative results.

The presented method was developed for the determination of morphine and codeine concentrations in serum. The linear dynamic range was found to range from 1 to 100 ng/mL for both compounds. For each curve, seven different concentrations were used, not including the standard matrix. The regression line *(Table 4)* was calculated by the German Industrial Standards(DIN) 32645 rules*[14]*.

Compound	Intra-assay Calibration curve	Correlation coefficient(r2)	Intra-assay Calibration curve	Correlation coefficient(r2)
Morphine	y=0,1085x-0,0399	0,99999	y=0,1059x-0,0019	0,99998
Codeine	y=0,1029x+0,0634	0,99999	y=0,102x+0,395	0,99999

Table 4. Results of the regression lines(n=5)

Statistical tests were performed with confidence level of 95%. The limit of quantification was 0.87 ng/mL for morphine and 0.9 ng/mL for codeine. Determination coefficients (r^2) of the calibration curves were higher than 0.9999 in all cases. Recovery of the analytes from solid phase extraction was estimated by processing three standard serum samples spiked with both compounds at a concentration of 10 ng/mL each. The recovery was found to be 70-80%

for morphine and 75-85% for codeine. The recovery of the internal standards did not differ significantly (p=0.05) from that of the analytes. Running a solvent standard *(see Table 2)* allows for the calculation of recoveries after processing each set of samples.

Several measures were taken to assure specificity during the analysis. Disposable equipment was used for sample preparation whenever possible, including pipette tips, vials, caps and solid phase extraction cartridges. The absence of interfering peaks was verified for each sequence of samples that were analyzed by running serum standards *(see Table 2)* concurrently.

The identity and purity of ion chromatogram peaks were checked by matching the retention time, peak shape and the ratio of target and qualifier ions *(Table 5)* with those of the standards *[14-16]*.

Name of compound	Retention time (min)	Qualifier #1 / Target ion	Qualifier #2 / Target ion
Morphine pentafluoropropionic ester	8.93	20±4 %	10±2 %
Codeine pentafluoropropionic ester	9.53	55±6 %	
D_6-Morphine pentafluoropropionic ester	8.89	28±4 %	12±2 %
D_3-Codeine pentafluoropropionic ester	9.50	60±6 %	

Table 5. The accepted ranges of the ratios of target and qualifier ions, provided as percentage

Peak symmetry was also a requirement. As a result of these efforts, the detection of the analytes and the internal standards was specific after chromatographic separation. The evaluation of the analytical data obtained from serum blank runs indicated that no interfering ion peaks were present in the matrix. In order to further reduce the chance of misidentification caused by interference occurring at the retention time of the analyte peaks, narrow time reference peak windows (±0.5%) were set *[18]*.

Spiking the deuterated analogs of the analytes to the samples as surrogate internal standards prior to sample preparation eliminated all difficulties arising from the diversity of matrix components and the loss of analyte during the extraction process. This approach renders the analytical method equivalent to reference methods as it can be categorized as a special kind of isotope dilution techniques with the labelled internal standards being analogous to the analytes. The minimal difference between the molar masses of the analyte molecules and the internal standard chemicals, along with the overwhelming similarities in physical and chemical properties, results in virtually identical retention of analyte and its deuterated analog on the chromatographic column. The probability of the appearance of interfering peaks is therefore reduced, just as any inaccuracies that would otherwise be inevitably introduced during sample preparation. Standardization was performed using standard serum specimens and were taken through the same sample preparation steps as the samples. This eliminated analytical errors arising from adverse chemical reactions between analytes and molecules normally present in human serum. Using surrogate internal standards also promoted a one-step calculation of analyte concentrations by placing the ratio of the target ion peaks of the analyte and the internal standard into the equation obtained during calibration.

The calculation of the limits of detection, identification and quantitation were based on average concentrations obtained during intraassay and interassay comparison studies *(Table 6)*.

	Intra-assay		Inter-assay	
	Morphine	Codeine	Morphine	Codeine
Limit of detection (ng/mL)	0.23	0.24	0.25	0.25
Limit of identification (ng/mL)	0.47	0.48	0.51	0.52
Limit of quantitation (ng/mL)	0.87	0.90	0.93	0.98

Table 6. Limits of detection, identification and quantitation of morphine and codeine (n=5)

These studies were conducted as defined by the German Industrial Standard DIN 32645 *[14]*. The aim of these studies was to estimate the accuracy of the analytical procedure. The analysis was performed on the lowest concentration level (1 ng/mL morphine and codeine; n=5) *(Table7.).*

Compound	Calculated concentration (ng/mL)	Relative standard deviation (%)	Relative error (%)
Morphine	1.004	7.6	0.4
Codeine	0.914	7.0	8.6

Table 7. Results of the intra-assay accuracy analysis (n=5)

Nominal concentration of both morphine and codeine was 1.0 ng/mL. Calculated concentrations are the means of concentrations obtained in 5 sequential runs. Relative error is the deviation of the calculated concentration from the nominal concentration *(Table8.).*

Compound	Calculated concentration (ng/mL)	Relative standard deviation (%)	Relative error (%)
Morphine	1.01	10.5	1
Codeine	0.92	11.5	8

Table 8. Results of the inter-assay accuracy analysis (n=5)

Nominal concentration of both morphine and codeine was 5 ng/mL. Calculated concentrations are the means of concentrations obtained in runs performed on 5 consecutive days. Relative error is the deviation of the calculated concentration form the nominal concentration. The bias was less than 10% in the case of the lowest concentration calibrator. .In studies of accuracy the differences between measured and expected concentrations were not higher than 10.5% in the case of morphine and not higher than 11.5% in the case of codeine *[15-16]*.

System applicability analysis indicated that the task presented herein could be accomplished using GC-MS, therefore this technique was selected *(1. Figure).*

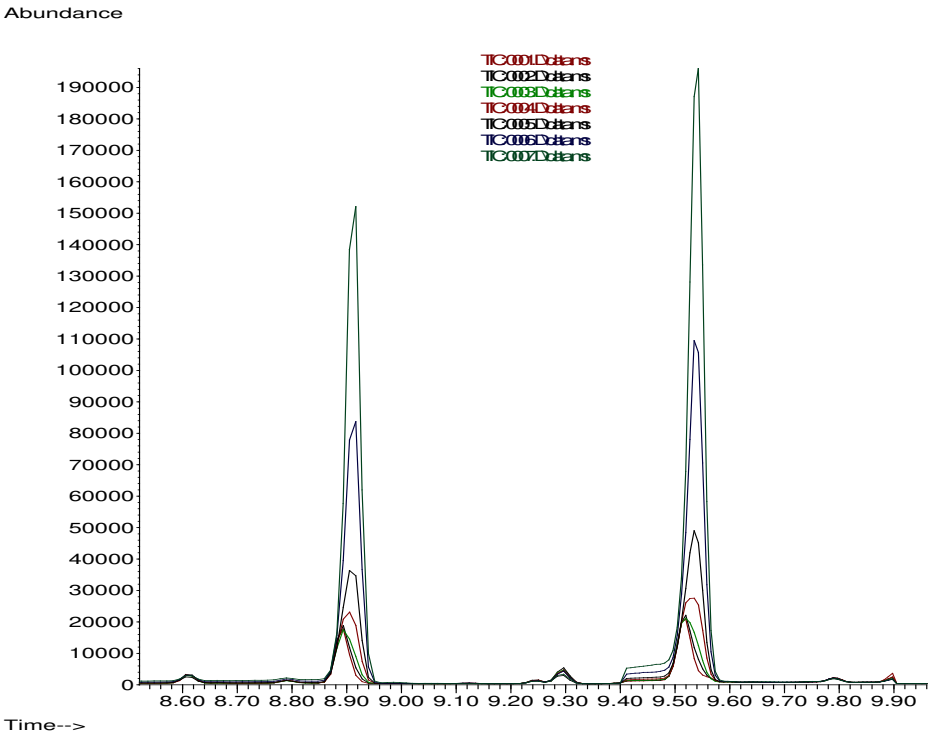


Figure 1. Overlay chromatograms of morphine and codeine belonging to the same series of calibration

Employing PFPA as a derivation agent provided several benefits. It is a very reactive chemical, allowing a simple, rapid and complete derivation of the analytes and the internal standards. The adducts are volatile and have a molecular mass considerably higher than that of the analytes. Electron ionization mass spectra of adducts were pure with an intensive molecular ion in the case of all monitored compounds. The adducts are highly fluorinated, so they can be detected with a high degree of sensitivity using negative chemical ionization.

Exploratory measurements were performed for the following reasons:

- The concentrations of the analytes in the samples were expected to be less than the low end of the therapeutic range (2 ng/mL),
- Blood is a complex matrix containing endogenous chemicals and macromolecules, which causes difficulties during separation,
- Retention parameters of both the target compound and the internal standard and the reproducibility of these parameters (<2% relative standard deviation) was evaluated,
- Tailing factors of the chromatographic peaks of the target analyte and the internal standard were determined and it was verified the value of these factors was below 5%.

System applicability analysis indicated that the task presented herein could be accomplished using GC-MS, therefore this technique was selected.

CONCLUSIONS

The presented method can be applied successfully for the fast and accurate determination of morphine and codeine concentrations in human serum. The method meets quality control requirements. With the use of calibrators prepared by spiking the analytes and the internal standards that were added to standard serum, and by employing deuterated analogs of the analytes as internal standards, the important analytical parameters (limits of detection, identification and quantification) can be inferred after running each sequence of samples.

Running serum extracts allow the most favourable signal-to-noise ratio among all the biological matrices. Therefore, serum is the matrix of choice in pharmacokinetic studies. The small volume required for analysis makes the method compliant with ethical requirements.

Deuterated analogs of the analytes were used as surrogate internal standards (isotope dilution technique). This allows for the elimination of many errors normally introduced during sample preparation and analysis. The other important factor that contributes to the elimination of errors is that calibration was performed using standard serum spiked with the analytes. The way that this was evaluated was the ratio of signal intensities.

Solid phase extraction was employed for cleaning up the samples. This is the most widely used sample preparation method as adsorbents are available with various polarities and selectivities. Solid phase extraction is a simple, easy-to-learn technique with high sample throughput. It also allows remarkable selectivity and reproducibility for analysis.

The analysis was performed using a fully computer-controlled GC-MS equipped with an auto-sampler unit. Samples could be analyzed with using both electron impact ionization and chemical ionization. The latter increased sensitivity three times.

This method developed by our team is suitable not only for therapeutic drug-level processing but also for investigating and confirmation of drug abuse.

This method was also applied to distinguish the consumption of foods containing poppy seed from abuse of different kinds of drugs produced from the poppy plant (opium, poppy straw, poppy tea etc.). The results of blood analysis of the participants taking part in the experiment are shown in the *Table 9*.

Partici-piants' ID No.	Morphine (free) (ng/mL)			Codeine (ng/mL)		
	in 1h	in 2h	in 4h	in 1h	in 2h	in 4h
I.	1.10	1.80	<1.00	<1.00	<1.00	-
II.	1.18	2.00	<1.00	<1.00	-	-
III.	1.20	2.10	<1.00	<1.00	<1.00	-
IV.	1.15	1.78	<1.00	<1.00	-	-
V.	1.00	1.80	<1.00	<1.00	-	-
VI.	1.15	1.50	<1.00	<1.00	<1.00	-
VII.	1.40	1.90	<1.00	<1.00	-	-
VIII.	1.10	1.40	<1.00	<1.00	-	-
IX.	<1.00	1.15	<1.00	<1.00	-	-
Blank	0.00	-	-	-	-	-

Table 9. The participants' blood analysis results for the morphine and its metabolites

References

[1] Fed. Regist. 1994, 59(110), 29922.

[2] J.H. Autry, III. Notice to all DHHS/NIDA Certified Laboratories, December 19, 1990. United States of America Department of Health and Human Services, Public Health Service, Alcohol, Drug Abuse and Mental Health Administration, Rockville, MD (1990).

[3] M. Thevis, G. Opfermann, W. Schaenzer. Urinary concentrations of morphine and codeine after consumption of poppy seeds. J.Anal. Toxicol., 27: 53-58 (2003).

[4] R. Meatherall. GC-MS quantitation of codeine, morphine,6-acetylmorphine,hydrocodone,hydromorphone,oxycodone,oxymorphone in blood. J. Anal. Toxicol., 29: 301-308 (2005).

[5] M.R. Moeller, K. Hammer, O. Engel. Poppy seed consumption and toxicological analysis of blood and urine samples. *Forensic Science International*: 181-187 (2004).

[6] F.P.Smith, ph.D. Morphine and Other Opiates in Body Fluids After Ingestion of Poppy Seeds. *Handbook of Forensic Drug Analysis*

[7] 17/1999. (VI. 16.) EüM rendelet az élelmiszerek vegyi szennyezettségének megengedhető mértékéről.

[8] M. Herbold and G. Schmitt. B.E.N. Program. Institut für Rechts und Verkehrsmedizin, Heidelberg, Germany, 1999.

[9] J.D. Ropero-Miller, M.K. Lambing and R.E. Winecker. Simultaneous quantitation of opiods in blood by GC-EI-MS analysis following deproteination, detautomerization of keto analytes,solid-phase extraction, and trimethylsilyl derivatization. J. Anal Toxicol., 26: 524-528 (2002).

[10] K. Róna, K. Ary, L. Vereczkey: Acta Pharm. Hung., 67: 51 (1997).

[11] J. Trafkowski B. Madea, F. Musshoff. The significance of putative urinary markers of illicit heroin use after consumption of poppy seed products. Ther Drug Monit. 28: 552-8 (2006).

[12] B.A. Rashid, G.W. Aherne, M.F.Katmeh, P. Kwasowski, D. Stevenson: Determination of morphine in urine by solid-phase immunoextraction and electrochemical detection. J. Chromatogr. A 797: 245-50 (1998).

[13] T. Hyötylainen, H. Keski-Hynnila, M-L. Riekkola. Determination of morphine and its analogues in urine by on-line coupled reversed-phase liquid chromatography-gas chromatography with on-line derivatization. J. Chromatogr. A 771: 360-65 (1997).

[14] Deutsches Institut für Normung 32645. Nachweis-, Erfassung- und Bestimmungsgrenze. Beuth Verlag, Berlin, Germany, 1994.

[15] Harmonized guidelines for singlelaboratory validation of methods of analysis, Pure Appl. Chem., Vol 74. No. pp. 835-855, 2002. IUPAC.

[16] Method validation and quality control procedures for pesticide residues analysis in food and feed, Document No. SANCO/2007/3131

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Tamási Béla
tamasi.bela@hm.gov.hu

Földi László
foldi.laszlo@zmne.hu

A TOKIÓI METRÓBAN VÉGREHAJTOTT SZARIN TÁMADÁS KATASZTRÓFAVÉDELMI ASPEKTUSAI

Absztrakt

A 1990-es évek elejére, az „AUM Shinri Kyo" néven ismert szélsőséges csoport a vegyi és biológiai fegyverek arzenálját halmozta fel és használta ártatlan civilek ellen Japánban. Ennek egyik példája a Matsumotoban 1994-ben, a másik 1995-ben a Tokiói Metróban alkalmazott szarin gáz használata. A két támadásnak összesen 19 halálos áldozata és több ezer sérültje volt. Az 1995. évi tokiói szarin támadás vizsgálati tanulmánya feltárja egy ilyen támadás előre jelezhetőségét a hatások csökkentése érdekében.. Az „AUM Shinri Kyo" esettanulmány egy jó tanulási eszköz a politikai döntéshozók és a katasztrófa-elhárítási szakemberek számára, abból a célból, hogy összefüggő rendszert képezzenek a hazai felkészülési stratégiájának.

In the early mid 90s an extremist group known as „AUM Shinri Kyo" amassed arsenal of chemical and biological weapons and used against innocent civilians in Japan. Two examples are the use of sarin gas in Matsumoto in 1994 and in Tokyo Metro in 1995. The attacks claimed a total of 19 lives and caused thousands of injuries. A review of the scenario of Tokyo Metro sarin attacks, reveals potential opportunities to preempt such an attack or to mitigate its effects. The „AUM Shinri Kyo" case study is a good learning tool for policymakers and disaster management professionals seeking to form a coherent domestic preparedness strategy.

Kulcsszavak: *szarin, AUM Shinri Kyo, vegyi és biológiai fegyverek, katasztrófa elhárítás ~ sarin, AUM Shinri Kyo, chemical and biological weapons, disaster management*

BEVEZETÉS

„Vess be pormérget a gályákon. Finomított arzén szulfidját, mésszel keverve, és porított rézrozsdát dobhatnak ellenséges hajók között kicsi hajítófák segítségével, és mindazok kik belélegezik a port, a tüdőik megfojtottá fognak válni.”[1]

A tanulmány aktualitását adja az a megállapítás, miszerint napjaink biztonsági kihívásai között első helyen szerepel a szélsőséges csoportok, terroristák által alkalmazható vegyi és biológiai anyagokkal végrehajtott támadások bekövetkezésének lehetősége. A Japánban szarin[2] alkalmazásával bekövetkezett két esemény tanulmányozása közül, különösen a Tokiói Metróban végrehajtott támadást követő, a felszámolás során elkövetett hibák feldolgozása tanulságos lehet a katasztrófavédelmi szakemberek számára. Egyrészről az elkövetett hibák újbóli megismétlődésének kiküszöbölése a tevékenységek összehangolása és begyakorlása céljából, másrészt a megfelelő együttműködési megállapodások megkötése, valamint az elégséges logisztikai háttér biztosítása érdekében. A nemzetközi együttműködés lehetősége szempontjából pedig a teljes eseménysorozat tanulmányozása, valamint a kormánynak és a katasztrófavédelembe bevont szerveknek az eseményekre adott válasz reakciója alapján a következtetések levonására adhat segítséget.

A tanulmányt az alábbi fejezetekkel és tartalommal építettem fel. A *bevezető részben* ismertetem az eset áttekintését, valamint ezt követően a támadást végrehajtó csoport az eseményekhez kapcsolódó tevékenységét, az események hátterét. A fejezetet a szarin gázzal végrehajtott támadás fontosabb kronológiai eseményei felsorolásával zárom. A *fő részben* ismertetem a szarin mérgező harcanyag jellemző tulajdonságait és az emberi szervezet szarin mérgezésre utaló tünetegyüttesét. Megfogalmazom –a katasztrófa helyzetértékelés lépéseinek figyelembe vételével – az eset kapcsán a katasztrófavédelembe bevont szervek a támadásra adott válaszreakciót, azok hatékonyságát, a hiányosságait és az azok kiküszöbölésére tett javaslatokat. A *befejező részben* a fő rész mondanivalójának összefoglalásán kívül az alábbiakban megfogalmazoott kérdésekre.is megadom a választ.

- Melyek voltak a krízisreagálási képesség hiányosságai?
- Milyen tényezők akadályozták a helyszíni ellátást és a sérültek kórházba szállítását?
- Rendelkezésre állt-e megfelelő mennyiségű ellenanyag?

AZ ESET TÖRTÉNETI ÁTTEKINTÉSE

1995. március 20-án a kora reggeli órákban az “AUM Shinri Kyo”[3], egy az apokalipszisben hívő terrorista csoport tagjai hajtottak végre szarin alkalmazásával támadást. A támadás célpontja a Tokiói Metró hálózat öt vonala volt. A támadás eredményeként tizenkilenc polgári személy meghalt és több mint 5,000 megsebesült. A támadás úgy híresült el, mint a béke történet legnagyobb ideggáz támadása. Attól a pillanattól kezdve a tömegpusztító fegyverek kiléptek a viszonylag jól szabályozott és ellenőrzött szuverén katonai felhasználás köréből és a világ számára egy új minőségű fenyegetés teremtődött meg. Ezáltal a terrorizmus arzenáljába illesztette a tömegpusztító eszközöket.[1]

A metróállomások ellen végrehajtott szarin támadás nem az első támadás volt, amit Japán átélt. A támadás céljának megértéséhez szükséges a támadást végrehajtó szekta kultuszának megismerése. 1984-ben Shoko Asahara nevű buddhista személy által egy közösségi ház került megalapításra, amely később szektává nőtte ki magát és nemzetközi tagokat vonzott soraiba.

[1] Leonardo da Vinci feljegyzése a vegyi hadviselésről.
[2] Gerhard Schrader az IG Farben vegyésze fedezte fel.
[3] Jelentése: Legfőbb Igazság.

A csoport fő célkitűzése a nemzeti fennhatóság megteremtése volt Japánban. A korai 90-es években a csoport vegyi- és biológiai fegyverek előállításával kezdett foglalkozni, amelynek komolyságát jelzi, hogy erre a célra több mint 30 millió dollárt költöttek. Korábban a szekta kilenc alkalommal próbálkozott antrax-támadással is. A csoport első szarin gáz alkalmazásával végrehajtott támadása 1994-ben történt. Egy a számunkra nem kedvező bírósági vitában eljáró bíró ellen alkalmaztak szarint, erősen higított állapotban. Az eljáró bíró a támadást túlélte, azonban hét ártatlan állampolgár életét vesztette és 144 sérülést szenvedett. A hatóságok azonban nem találtak semmiféle bizonyítékot a csoport tevékenysége és a támadás között.[2] Fél évvel később a Matsumoto-i támadást követően azonban az összekapcsolódást bizonyítani tudták és amennyiben a csoport ellen időben akcióba lépnek, a későbbi, metró elleni támadás nem történik meg. A csoport terve szerint a Kasumigasek-i állomás volt a merénylet kiinduló pontja, amely állomáson öt metróvonal találkozik. Az állomás közelében található a kormány számos épülete, valamint a tokiói rendőrség főhadiszállása is. A terv szerint a kiinduló metróvonalak egy-egy kocsijában elhelyezett szarin kapszula felrobbantásával a szellőző rendszeren való tovaterjedésével kívánták a kívánt mérgező hatást elérni. Mindegyik kapszula 30 %-os töménységű szarint, mintegy 20 uncia (622 gramm) mennyiséget tartalmazott. A rendőrségi felvételek elemzése alapján a támadás 1995. március 20-án 7.55 perckor következett be. Az első segélyhívás 8.09 perckor történt, míg az első mentőautó megérkezése a helyszínre 8.40 perckor következett be.[3]

A bekövetkezett esemény - a tanulmány szempontjából fontos- főbb időpontjai:

07.55	A terroristák elfoglalják helyüket a metrószerelvényeken.
08.00	A támadás végrehajtása.
08.09	Az első fogadott elsősegélyhívás ideje.
08.16	A tűzoltók értesítése.
08.25	Az első áldozat kórházba érkezése. (önerőből)
08.40	Az első mentőautó megérkezése a helyszínre.
10.00	A mérgező anyagot tévesen acetonitrilként azonosítják.
11.00	A rendőrség szarinként azonosítja az anyagot.
12.00	A kórház tudomására jut, hogy a mérgező anyag szarin.
12.45	Helyi elkülönítés és fertőtlenítés elrendelése.
06.00	Németország, Franciaország, és Anglia felajánlja segítségét.

A szarin jellemzői és az emberi szervezetre gyakorolt hatásai:

A szarin igen erősen toxikus hatású, az idegmérgek csoportjába tartozó, szerves fluro-foszfát típusú vegyület. Az ilyen jellegű anyagok erős mérgező-képességét már az 1930-as évek előtt is ismerték, de szándékosan idegméregként történő felhasználásuk 1935-40-től datálható. Dr. Gerhard Schrader, az IG Farben kutató mérnöke 1937-ben állította elő az első ilyen típusú anyagot, a tabunt, majd 1938-ban a szarint. A német vezérkar már abban az évben néhány kilogramm hatóanyaggal rendelkezett. Nagyüzemi gyártása 1944-ben indult meg, a háború végéig néhány ezer tonnányit gyártottak, de bevetésére nem került sor. A hidegháborús szembenállás korszakában mindkét fél óriási mennyiségű idegméreg típusú mérgező harcanyaggal rendelkezett, többek között szarinnal is. A szembenállás megszűnése és a vegyifegyvereket korlátozó nemzetközi egyezmény életbe lépése után a meglévő készletek megsemmisítése megkezdődött és még napjainkban is tart. Az 1990-es évektől kezdődően idegmérgek alkalmazásának veszélye főként az ún. „haramia-államok” és befolyásos terrorista csoportok részéről jelentkezik.

A szarin közönséges körülmények között víztiszta, átlátszó, enyhe gyümölcs illatú higroszkopikus folyadék, a vízzel minden arányban elegyedik. Melegítés hatására bomlik,

emellett illékony, gyorsan párolgó anyag, ezáltal szabadba kerülése esetén gyorsan terjed veszélyes koncentrációban.

Toxikus tulajdonságai: A szarin légzőszerveken keresztül illetve bőrön keresztül felszívódva mérgez. A bőrön keresztül való felszívódás csak nagyobb koncentrációknál következik be.

Könnyű lefolyású mérgezés 0,0002...0,002 mg/1 koncentrációk 2 perces belégzésekor alakul ki.

Súlyos mérgezés alakul ki 0,01...0,005 mg/1 koncentrációk 5 perces belégzésekor.

A szarin mérgezések jellemzője a halmozódás, azaz kis koncentrációk hatása összeadódik. A mérgezés szimptómái:

- Könnyű mérgezés (a halálos koncentráció egytizede). 10-15 perces lappangási idő után pupillaszűkület, fejfájás, majd mellkasi fájdalmak, étvágytalanság, álmatlanság jelentkezik 1-5 napig.
- Közepes mérgezés (a halálos koncentráció egyötöde). A szimptómák 5 perc után jelentkeznek, a tünetek 1-2 óra múlva a legerősebbek és 4-6 hétig megmaradnak. A tünetek hasonlóak a könnyű mérgezéséhez, de sokkal intenzívebbek. Jelentősek a légzési problémák, erős köhögés jelentkezik.
- Súlyos mérgezés (a halálos koncentráció 1/3-ától jelentkezhetnek). A szemekben nyomásérzés jelentkezik, rendkívül erős fejfájás lép fel, mellkasi fájdalmak, szabálytalan légzés és szívverés következik be, majd bénulásos halál állhat be. A lappangási periódus rendkívül rövid, a halál 6-12 órán belül bekövetkezhet.

Számos gyógyszerészeti cég forgalmaz szarin elleni készítményeket. Az ellenanyag gyors beadása számottevő mértékben csökkenti a mérgezés kialakult hatásait, továbbá csökkenti a kialakuló egészségügyi problémák bekövetkeztét.[4]

A helyzetértékelés lépéseinek megvalósulása

A terrorista támadás során alkalmazott mérgező harcanyag hatásának helyzetértékelése azonosnak tekinthető veszélyes anyag gyártása, tárolása, szállítása során bekövetkező balesetekéhez, katasztrófákéhoz. A helyzetértékelés ebben az esetben, az alábbi lépésekben valósul meg:

- Felderítés, információgyűjtés
- Hatások értékelése, veszélyforrás azonosítás
- Védelmi intézkedések megtétele
- Beavatkozás
- Rehabilitáció [5]

Ez a fejezet a szarin támadást követő, a helyzetértékelés egyes lépései végrehajtása során elkövetett hiányosságok ismertetését, valamint a hiányosságok felszámolására és újbóli bekövetkezésének elkerülésére tett javaslatokat foglalja magába.

Felderítés, információgyűjtés

A felderítés, információgyűjtés során mindenek előtt szükséges *a mérgező harcanyag beazonosítása*. Esetünkben a tokiói tűzoltóság tévesen acetonitrilnek[4] azonosította a vegyi anyagot, majd később, amikor a rendőrség felismerte a valós vegyi anyag kilétét (ami körülbelül 3 órával a támadás után történt) azonnal tájékoztatta a tűzoltóságot és a kórházakat, valamint a médiát. A vegyi támadás, esetünkben konkrétan a tokiói támadás során alkalmazott vegyi anyag azonosításának időszerűsége alapvető fontossággal bírt, hiszen a késlekedés,

[4] A legegyszerűbb szerves nitril-származék, amelyet oldószerként széles körben alkalmaz a vegyipar.

vagyis a késői azonosítás a sérülteknél halálos kimenetelű következményekkel járt. A mérgező harcanyag azonosítása azért is volt fontos, mert a klinikai megfigyelés és kezelés alapján az acetonitril és a szarin okozta sérülések közel azonos tüneteket mutatnak. Az azonosítást követően a kórházak tudomására jutott, hogy a tünetek és a sérülések nem acetonitriltől, hanem szarintól származnak. Ezáltal ismertté válhattak *a veszélyes vegyi anyag jellemző tulajdonságai*, egyúttal meghatározhatóvá vált, hogy az *milyen veszélyeket hordoz a polgári lakosság és a beavatkozók számára.* Elsődleges fontosságú volt, hogy a tűzoltóság felismerte a médiával történő kapcsolatfelvétel jelentőségét. Ennek következtében bevezethetőek és széles körben ismertté lettek a *prioritást igénylő intézkedések.*

Következtetések, ajánlások:

A katasztrófavédelem nem rendelkezett olyan, a szarin beazonosítására megfelelő érzékelő egységgel, amellyel a szarin jelenlétét egyértelműen azonosítani lehetett volna. A könnyebb érzékelés jelentősen csökkentette volna az exponálási időt, ezáltal az áldozatok számát. Érdekesség, hogy 9 évvel a támadás után a sérülteknél még mindig ki lehetett mutatni a szarin jelenlétét a vérből. A hamis azonosítás a halálesetek számának exponenciális növekedését jelentették. Ezért fontos, hogy a katasztrófavédelem el legyen látva vegyi anyagok kimutatására alkalmas érzékelőkkel. A biztos tudás hiányában sokszor irreleváns adatok tömegének közlésével nehezítik a felderítők a mentést. Amennyiben az érzékelők beszerzése nagy számban pénzügyileg nem kivitelezhető, azokat legalább a frekventált központi fekvésű helyeken kell biztosítani. Fontos az is, hogy az incidens megtörténtét követően a riasztásra kerülő, meglévő mobil érzékelő egységek mihamarább elérhetőek legyenek. Ezen egységeket könnyen elérhetővé kell tenni, amelynek a valós bekerülési és fenntartási költsége nem számottevő. Sok esetben nem lehet különbséget tenni a természeti katasztrófa és a terrorista támadás hatásai között, ezért a reagáló erők (tűzoltóság, rendőrség, mentők és kórházak) részére nem kell külön feladatokat meghatározni.[6]

Hatások értékelése, veszélyforrás azonosítás

A hírközlés hiányosságai

A személyek veszélyeztetettségét nagymértékben növelték a bekövetkezett eseményekre való reagálás alapvető hiányosságai, melyek alapvetően a katasztrófavédelmi hírközlés, ezen belül a tokiói mentőszolgálat egyes egységei közötti koordináció hiányában mutatkoztak meg. Az incidens bekövetkezését követő első órában a segélyhívások 15 különböző metróállomásról érkeztek be. A tokiói mentőszolgálathoz beérkező segélyhívásokat az amúgy intelligens számítógépek nem tudták a helyzetnek megfelelően lekezelni, ami tulajdonképpen felért egy vírustámadással a számítógép rendszer ellen. A rendszer nem volt képes kapcsolatot teremteni a különböző alhálózati állomások között, mindemellett hibázott a helyszínek beazonosításában is. Ennek következtében az áldozatok száma szükségtelenül megnőtt az eseményt követő első két órában.

Következtetések, ajánlások:

A hírközlés hibáit, mint a tanulmányban gyakran látjuk, létfontosságúnak kell tekinteni. Szükség van állandó kapcsolattartásra a különböző telefonos rendszerek között. A koordináció jóval nagyobb időt vett igénybe, mint a korábbi egyedi esetek során, ezért a rendszer képességét javítani kell. A rendszernek különbséget kell tennie a valós és vírus jellegű támadások között. Az automata rendszernek elsőbbséget kell adnia az olyan hívások irányába úgynevezett programindító szavak segítségével, mint például „metrómegálló”, „égő szem” vagy „mérgezés”. Ezek a szavak szinte minden segélyhívásban megtalálhatóak voltak.

Információ túlcsordulás

Az információk késleltetett feldolgozása az információk egy időben való sokaságának köszönhető. A rádió hálózat egyidejű túlterhelése a mentéshez szükséges frekvenciát nagymértékben lefogta, ezáltal a helyszínen lévő orvos csoport nem tudott kapcsolatot teremteni a mentőközponttal. Ennek következtében a helyi orvosi kezelésben részesültek viszonylag későn jutottak kórházba. Szintén a rossz menedzselésnek köszönhetően a bejövő alapvető információk feldolgozása, úgymint *a szennyeződés, a fertőződés és a terjedés veszélye* és támadás azonosítása között eltelt 2 óra időtartam vezetett a II. világháború utáni időszak legnagyobb vegyi katasztrófájának bekövetkezéséhez. Ez a durva késlekedés, *a döntés meghatározás* késlekedése és a rosszul menedzselt információ átadás óriási pánikot okozott Tokióban.

Következtetések, ajánlások:

Egységes, lehetőség szerint digitális rádió rendszer kialakítása vált szükségessé, melyet kizárólag a védekezésbe bevont szervek használhatnak. A kiépített híradás rendszere helyi, területi és országos együttműködést valósítana meg. Fontos, hogy a híradó eszköz könnyen kezelhető, mindenki számára elérhető legyen, és kapcsolódni tudjon a meglévő vezetékes, vagy mobil hálózathoz is. Elvárás az is, hogy az eszköz sebezhetősége kicsi legyen, vagyis ellenálljon a vírustámadásoknak.

Védelmi intézkedések megtétele

A lakosság és a mentésben résztvevők védelme

A támadásban érintett területen belül lévő lakosság védelmére meglehetősen kevés eszköz állt rendelkezésre. *A mérgező harcanyag veszélyessége és gyors terjedése indokolta az azonnali tájékoztatást és a terület gyors elhagyására történő felszólítás mellett meghatározta a helyszín elhagyás irányát, módját, eszközeit, a mentesítő helyet és kitelepítés magatartási szabályait. A lakosság védelmére* alkalmazott kimenekítés során a sérülteket a beavatkozó állománynak a lehető legrövidebb időn belül ki kell mentenie, végre kell hajtani a részleges mentesítését és a mentőknek át kell adni. A kimenekítés és a sérültek ellátása során természetesen kiemelt figyelmet kell fordítani *a beavatkozók védelmére*, elsősorban a légzés és bőrvédelem biztosítására. A szarin támadás bekövetkezése utáni mentesítés egyik legfontosabb feladata volt a helyi fertőtlenítés időbeni megkezdése. A szarin fertőzöttnek a fertőzést követően azonnali friss levegőre van szüksége.

Az sem elhanyagolható, hogy a szennyezett ruházat további mérgezéseket okozott a beteggel érintkezők körében. A szarin képes párologni és levegőn keresztül terjedni, ezért a támadásnak másod-, harmad- és negyedfokú fertőzöttjei is voltak. A fertőzöttek számára kihatással volt az a tény is, hogy az átlagos civil öltözet nem nyújtott védelmet a mérgező harcanyag ellen. Ennek következményeként csak a sérültek 10 százalékát tudták azonnal kórházba szállítani, miközben a mentő kapacitás körülbelül ugyancsak 10 százaléka volt kihasználva. Körülbelül 110 orvos foglalkozott a betegekkel, akik a mérgezést követően taxival vagy gyalog érkeztek a kórházakba. A mentésben résztvevő 1364 fő szakszemélyzet tagjai közül 135-öt ugyancsak kórházba kellett szállítani. A fertőtlenítés feltételeivel nem rendelkező kórházak azt eredményezték, hogy az áldozatok száma jelentősen megnövekedett és még olyanok is áldozatul estek, akik viszonylag enyhe mérgezést szenvedtek.

Következtetések, ajánlások:

A fertőtlenítés elsődleges fontosságú és a támadást követően azonnal meg kell kezdeni. A különböző vegyi támadások fertőtlenítési eljárásai nagyon hasonlóak. A beavatkozó személyzet részére biztosítani kell a megfelelő fertőtlenítéshez szükséges berendezéseket és védőfelszereléseket. A védekezés gyorsasága elsődleges fontosságú és a támadás erősségével

kell arányban lennie, mivel a gyors beavatkozás megelőzi a később kialakuló tüneteket és egyben lehetővé teszi a betegek további kezelését. Az azonnali fertőtlenítés tovább csökkenti a másod-, harmad- és negyedfokú hatások kialakulását. Meg kell határozni a helyszíni és a háttérellátás összhangját is. Megoldás lehet mobil csoportok létrehozása, ami azt jelenti, hogy egy erre a célra speciálisan felkészített mentőcsoport készenléti szolgálatot lát el és a támadást követően azonnal bevethető. Így csökkenteni lehet az expozíciós időt, mivel a fertőtlenítés azonnal megtörténik. Természetesen fontos kérdés, hogy ezek a készenléti erők a fertőzéstől milyen távolságra helyezkednek el. Egy másik lehetséges megoldás, ha a kórházak pótlólagos fertőtlenítési lehetőségekkel rendelkeznek, amelyeket kialakítani a kórházak bejáratánál vagy a parkolóházakban lenne ajánlatos.[7] Ezek az ideiglenes szolgáltatások segítenének nagyobb létszám egyidejű fertőtlenítésében, ami által a támadás utólagos hatásai nagymértékben csökkenthetőek lennének.

Beavatkozás

A helyszíni ellátás, elsősegélynyújtás

Az ideggázzal végrehajtott támadásoknak jellemzője, hogy ha a beteg minél előbb szakorvosi kezelést kap, annál kisebb a szervi károsodás bekövetkeztének esélye. A szarin mérgezett azonnali légcső intubációval[5] egybekötött ellátást igényel. Ezt követően az *elsődleges cél a szarin mérgezett áldozatok kórházba juttatása* a lehető legrövidebb időn belül. Az ellátás következő lépése a sérült atropin-szulfáttal[6]való kezelése. A fertőtlenítési eljárásoknál azt is figyelembe kell venni, hogy a mérgezés hatásaként előidézett hányás miatt a mesterséges lélegeztetés nehezen alkalmazható. Az atropin segíti a légzés helyreállítását, ellenben hasonló tüneteket okoz, mint a mérgezés, úgymint émelygés, hányás, hasi görcs, szívverés lassulása, izzadás. Az atropin alkalmazása bénulást is előidézhet. A pralidoxim-klorid[7] adagolása szintén a szarin hatásainak csökkentése céljából alkalmazott. A sérültek nem azonnali, a helyszínen történő ellátás hiányában a kórházba érkezésig a fertőzés és annak mellékhatásai fennálltak.[8] A hírközlés és koordináció hiányosságai és ebből adódóan az áldozatok késői helyi kezelésének megkezdése következtében a fertőzöttek közül néhányan a kórházba szállítás közben életüket vesztették. A tokiói mentőállomás 47 orvost és 23 ápolónőt hívott be és küldött ki 15 helyszínre, amely gyakorlatilag a körzet teljes bevethető mentő kapacitását lefogta.[9]

Következtetések, ajánlások:

A helyi kezelésben beállt zavar kiindulópontul szolgált a kórházba szállítás zavarának kialakulásához. A szállítás során nem adtak elsőbbséget a súlyosabb, válságos helyzetben lévő betegeknek, néhány esetben olyanok is beszállításra kerültek, akiknek a helyi kezelés is elegendő lett volna. Az említett hibáknak a kiküszöbölésére olyan módszert kell létrehozni, amely meghatározza az áldozatok szállításának prioritását és amely a kiérkező orvos csoport osztályozását figyelembe véve meghatározza, hogy a betegek milyen szintű ellátásban részesüljenek és melyik kórházba kerüljenek beszállításra.

A mentőautóval történő szállítás problémái

A mentőautóval történő szállítás számos problémát vetett fel a támadást követően. Ennek értelmében, mintegy 4000 embert kellett volna szállítaniuk, de valójában csak 688-at sikerült.

[5] Életmentő orvosi beavatkozás, amelynek során csövet vezetnek be a szájon keresztül a gégébe az átjárható légutak biztosítására.

[6] A szer az Atropa belladonna, tehát a nadragulya néven ismert burgonyaféle növény alkaloidja, a vegetatív (akarattól függetlenül működő) idegrendszer működését módosító gyógyszer (az úgynevezett paraszimpatikus hatásokat gátló vegyület).

[7] Kolinészteráz reaktivátor, szervesfoszfát mérgezés és a kábítószer-túladagolás kezelésére

A taxik több áldozatot vittek kórházba, mint a mentősök, aminek következményeként a mérgezés másod-, harmad- és negyedfokú hatásainak a száma megnőtt. Ennek az eredménytelenségnek egyik oka szintén a hírközlés hiányossága volt. A támadást követően a hírcsatornák túlterheltek lettek, nem volt kapcsolat a kórházak és a helyszínek között és az orvosok nem ismerték a kórházak szabad kapacitását. Ennek eredményeként a mentőautók kénytelek voltak egyik kórházból a másikba vinni a betegeket, nem egy esetben azokat távoli kórházba kellett szállítani. A rossz információ következtében a metróállomásokhoz közeli kórházak betegellátási kapacitásaiknak csak a töredékét használták fel. [10]

Következtetések, ajánlások:

A mentőknek ki kell dolgozni egy úgynevezett felvonulási útvonalat a lehetséges katasztrófa helyszínek megközelítésére. Nehézséget jelentett, hogy a támadás a reggeli csúcsforgalomban történt, ezáltal a mentő gépjárművek mozgása a forgalomtól függött. Szintén hátráltatta az ellátást, hogy a támadások olyan metrómegállókban történtek, ahol különösképpen nagy forgalmú középületek álltak. Az áldozatok a közeli ellátás reményében taxival vagy gyalog próbáltak segítséghez jutni. Ésszerűen meg kell határozni, hogy melyik katasztrófa körzet melyik ellátó intézményhez van társítva, valamint azt is, hogy nem minden kórházi kapacitást felhasználó katasztrófa bekövetkezése esetén mi az együttműködés rendje. Emellett ki kell dolgozni a civil járművek bevethetőségét a betegszállításba úgy, ahogy azt a taxisok is tették.

A kórházak közötti együttműködés

A kórházak közötti együttműködés hiánya okozta, hogy a kórházak nehezen valósították meg az egymás közti betegátvételt. Egyes kórházak túlterheltek voltak, másikak pedig kihasználatlanok.

Következtetések, ajánlások:

A kórházak közti átvételek az események alatt ésszerűtlenül történtek, így a kórházak nem tudták a megfelelő beteglétszámot felvenni. Hasznos lenne egy úgynevezett adattárban rögzíteni a kórházak befogadóképességét, egymástól való távolságukat és az orvos-beteg arányokat. Ahol nem áll rendelkezésre mentőautó a kórházak közti betegátvételhez, ott alternatív szállítási rendszert kell kiépíteni, Ezek lehetnek taxik, autóbuszok vagy katonai járművek, melyeknek a katasztrófavédelmi tervekben meg kell jelenniük, hogy reálisan csökkenthető legyen a betegátadás során fellépő emberi veszteség.

A beavatkozó szervek korlátai

A katasztrófavédelmi szervek alkalmazási korlátai is számos problémát vetettek fel. A betegek ellátása során nem tudták az áldozatokba az endotracheális[8] csövet bevezetni, ezáltal a légzést fenntartani. A japán törvények szerint ezt a beavatkozást kizárólag a páciens vagy hozzátartozója beleegyezésével lehet végrehajtani, ezért a katasztrófavédelmi szervek szakemberei és a helyszíneken dolgozó orvosok nem kaptak beleegyezést arra, hogy az életmentő eljárást végrehajthassák.

Következtetések, ajánlások:

A katasztrófavédelem szakembereinek meg kell tanulniuk a helyszíni ellátás alapismereteket, különösképpen az életmentő eljárásokat, valamint számukra lehetővé kell tenni, hogy szélsőséges esetekben engedélyezés nélkül hajthassák végre az életmentő beavatkozásokat.

[8] A légzést biztosító tubus bevezetése a szájon vagy orron át.

Rehabilitáció

Az ellenanyag ellátottság

A rehabilitációt alapvetően befolyásoló hiányossága a nem elégséges mennyiségű szarin ellenanyag rendelkezésre állása volt. A kórházak korlátolt képességekkel bírtak az intézményi ellenanyag tárolás és ellátás terén. Miután azonosították a vegyi anyagot sok kórház azonnali, soron kívüli megrendeléseket adott le. Bármennyire gyors volt a feldolgozás és az ellátás végrehajtása, mégis jelentős időbe telt az utórendelések kielégítése.[11]

Következtetések, ajánlások:

Szükséges a helyes készletfelhalmozás kidolgozása, valamint egy vegyi támadás következtében felhalmozott ellenanyag mennyiség meghatározása. Ez a mennyiség függ az ellátott lakosság számától, a felbecsült kockázat nagyságától, valamint egyéb gazdasági tényezőktől. Szintén fontos meghatározni az utórendelésen alapuló ellenanyag ellátást és a megfelelő tárolás rendjét. Létfontosságú, hogy a tároló helyek viszonylag közel legyenek a kórházakhoz, ezzel az ellátási időt jelentősen lehet csökkenteni, ami egyúttal a bekövetkezett támadásra adott válasz hatékonyságának növelését eredményezi.[12]

A katasztrófavédelmi tervezés hiányosságai

A tokiói szarin támadás felszámolásában a Japán Nemzeti Kormány közvetve elenyésző szerepet játszott. Ennek fő oka az egységes katasztrófa törvény hiánya volt. A japán törvények szerint a katasztrófa felszámolására tett intézkedések irányításáért az illetékesség szerinti helyi szervek a felelősek. Ezért a nemzeti kormány kezdetben nem avatkozott bele a szarin támadás következményeinek felszámolásába, azonban az áldozatok nagy száma miatt a későbbiekben kénytelenek voltak más területi és országos illetékességű szerveket bevonni.

Következtetések, ajánlások:

Modell alkalmazásával meg kell tervezni rendszer túlterhelése esetére is a vezetés rendjét. A túlterhelés esetére ki kell építeni a szükséges háttértámogatás és a segélyhívás rendszerét. A katasztrófa felszámolási tervben szükséges meghatározni az együttműködő szervezeteket (úgymint a taxisok, a nemzeti gárda, a hadsereg stb.) valamint a logisztikai háttérbiztosítás elemeit. Amennyiben egy adott helyszínről a háttértámogatás lehívásra kerül, meg kell teremteni a feltételeket a készletek újbóli feltöltését, ezáltal megteremtve a lehetőséget a további támadások kezelésére.

BEFEJEZŐ RÉSZ

A tanulmány rámutat arra, hogy a katasztrófák elleni védekezésre történő felkészülés még a fejlett gazdaságú társadalmakban sem lehet teljes mértékű és teljesen megnyugtató. A tanulmány bevezetőjében említettem, hogy a szarin gázzal végrehajtott támadás nem következett volna be, ha a hatóságok az erre figyelmeztető és utaló jeleket komolyan veszik. Márpedig komolyan kellett volna venni, hiszen a hatóságok megfejtettek – véletlenszerűen egy kódkönyv alapján – néhány, a terrortámadás megszervezésére irányuló üzenetváltást. Az események bekövetkezéséhez és annak hatásainak eszkalációjához azonban számos további elkerülhető hiányosság is hozzáárult.

A krízisreagálás képességeinek hiányosságai alapvetően meghatározták az elsődleges beavatkozás hatékonyságát. A *hírközlés hibái, az együttműködés hiánya* és az *információ túlcsordulás,* amelyek során bizonyítást nyert, hogy az automata rendszerek a sűrűn bejövő hívásokat vírustámadásnak érzékelik, nem képesek a rendszer újraindítására és hibás adatok, helyszínek megadásával megtévesztik a beavatkozókat. A biztosított híradó rendszerek egyidejű túlterhelése a helyszínekről érkező segélyhívások beazonosítását, a mentésben

résztvevő egységek nem szervezett bevetését, valamint azoknak az optimálistól messze elmaradó alkalmazását eredményezte.

A helyszíni ellátást és a sérültek kórházba szállítását befolyásolta mindenek előtt a sérültek *elkülönítése, osztályozása, elsődleges ellátása* során elkövetett hibák, melyhez legfőképpen a *mérgező anyag téves azonosítása* vezetett, de előkerült ismét a sikeres kommunikáció hiánya, az életmentő beavatkozás törvényi háttere, a megfelelő védőeszközök hiánya*, a mentőautók alacsony számú igénybevétele*, a *kórházak egymás közötti együttműködése*, de ide tartoztak *a katasztrófavédelem szervezeti korlátai* is.

Az *ellenanyag tárolás és ellátás* a logisztikai háttérbiztosítás alapvető eleme. valamint a *kormányzati támogatás*. A két összetevő egymáshoz szorosan kapcsolódik, mivel egyik a másik nélkül nem létezhet. Az *ellenanyag ellátás biztonság*, valamint az utánpótlás biztosítása mellett, mint tárgyi feltételek, a *humán erőforrások biztosítása* elengedhetetlen követelmény.

Ezen tanulmány is rávilágít arra a lehetőségre, hogy az irracionális terrorista akciók lehetősége a hidegháborút követően megjelent és a veszéllyel napjainkban és a közeljövőben továbbra is számolni kell. Tisztában kell lenni azzal a ténnyel is, hogy a kormányok tevékenysége és válaszreakciói korlátozottak. A lakosság ellen elkövetett terrorcselekmények során pánik kialakulására lehet számítani, amely negatív hatással lehet a katasztrófavédelembe bevont szervek tevékenységére. A katasztrófavédelem anyagi-technikai feltételeinek megteremtése, a rendelkezésre állás, az utánpótlás és a szakképzett humán erőforrás biztosítása elsődleges feladat. A kormányok szerepe elengedhetetlen, azok felelőssége áthárithatatlan. A terrorcselekmények hatásainak és elhárításának komplex kezelésére fel kell használni valamennyi létező médiát. Mindezek felett a szerencse is kívánatos. A Tokiói Metróban a nagyobb tragédiát végül is a terroristák képzetlensége miatt sikerült elkerülni, mivel a szarin gázos csomagokat rossz helyre tették, ahol a robbanás huzatot idézett elő, ami pedig csökkentette a vegyület koncentrációját.

Felhasznált irodalom

[1] Dr. Simon Ákos: A vegyi fegyver alkalmazási lehetőségei terroristák által. Bólyai Szemle 2004/2. 200.oldal, ZMNE Budapest, ISSN 1416-1443

[2] Okudera H., Unexpected Nerve Gas Exposure in the City of Matsumoto: Report of Rescue Activity in the First Sarin Gas Terrorism, pp 17-21, Am J Emerg Med, 1997, Philadelphia, Pennsylvania, ISSN 0265-0215

[3] Chemical Terrorism in Japan: The Matsumoto and Tokyo Incidents, http://www.opcw.org/resp/html/japan Letöltve: 2010. október 10.

[4] Prof. Dr Halász László, Nagy Károly: Mérgező anyagok kémiája, Egyetemi jegyzet, 31-34. oldal, ZMNE Budapest, 2001.

[5] Prof. Dr. Halász László: Katasztrófa előrejelzés és helyzetértékelés, Egyetemi jegyzet, 204-208 oldal, ZMNE Budapest, ISBN 978 963

[6] Okumura T., the Tokyo Subway Sarin Attack: Disaster Management, Part 1: Community Emergency Response, pp 613-617, Academic Emergency Medicine, 1998, Lansing, MI, ISSN 1065-6563

[7] Cox RD, Decontamination and Management of Hazardous Materials Exposure Victims in the Emergency Department, pp 25-33, Ann Emerg Med, 1994, Irving, TX, ISSN 0092-2102

[8] Okumura T., the Tokyo Subway Sarin Attack: Disaster Management, Part 2: Hospital Response, pp 618-624, Academic Emergency Medicine, 1998, Lansing, MI, ISSN 1069-6563

[9] Horváth Attila: A vasúti közlekedés terrorfenyegetettségének jellemzői a városokban. Hadmérnök on-line, 2009. IV. évfolyam 3. szám. pp. 180-189. ISSN 1788 1919. http://www.hadmernok.hu/2009_3_horvatha.pdf

[10] Attila Horváth: Terrorist Threats of the Urban Transportation Systems. Economics and Management - p.2. 2010 - Published by University of Defence in Brono. Czech Republic. pp. 62-69. ISSN 1802-3975 (peer reviewed).

[11] Ishimatsu S., Takasu N., The Tokyo Subway Sarin Attack: Medical Care at St. Luke's Intl Hospital, pp 618-624, Kyukyu-Igaku, 1995. ISSN 1534-7656

[12] Okumura T., the Tokyo Subway Sarin Attack: Disaster Management, Part 3: National and International Responses, pp 625-630, Academic Emergency Medicine, 1998, Lansing, MI, ISSN 1069-6563

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Lázár Gábor
gabor.lazar@gmail.com

Szatmári-Juhász Ditta
ditta.szatmari@gmail.com

A VESZÉLYES ANYAGOK KÖZÚTI SZÁLLÍTÁSÁNAK ÉS TÁROLÁSÁNAK KÖZBIZTONSÁGI ASPEKTUSAI

Absztrakt

Jelen tanulmány összegzi a veszélyes anyagok szállítására és tárolására vonatkozó legalapvetőbb közbiztonsági szabályokat és irányelveket, továbbá bemutatja az összegzett elvek gyakorlati megvalósítását lehetővé tevő eszközöket, alkalmazásokat. Kitér a veszélyes áruk szállításában résztvevő járművek, helyszínek, személyek biztonságára, kötelességeire és dokumentációira, illetve kockázatbecslési szempontból taglalja a veszély árukat és helyszíneket. A cikk a legtöbb esetben konkrét javaslatokat, tanácsokat nyújt az egyes árufélékkel, helyszínekkel kapcsolatos biztonsági intézkedésekre vonatkozóan. A szerzők a közlemény végén definiálják a témában használatos legalapvetőbb fogalmakat is.

This article summarizes the fundamental public safety rules of the transportation and storage of dangerous goods. In the main part of study are introduced the tools and methods that facilitate the practical realization of the summarized principles. The article provides detailed information on the security obligations and documentation of the vehicles, the sites, and the persons that participate in the transportation of dangerous goods and for risk assessment, provides details on the dangerous goods and their storage sites. In most cases the article provides useful recommendations and advices on the security measures relating to certain goods and sites. At the end of the article, the authors also define the basic concepts in this topic.

Kulcsszavak: *közbiztonsági követelmények, veszélyes áru, szállítás, kockázatbecslés, megelőzés ~ security requirements, dangerous goods, transportation, risk assessment, prevention*

BEVEZETÉS

Napjainkban a közúti teherfuvarozás mértéke globális mértékben is jelentős, világszerte óriási mennyiségű áru utazik rendeltetetési helyére nap mint nap. Ezen áruk bizonyos hányada veszélyes besorolású, amelyek esetében az ADR szabályok betartása kötelező. Az európai hatókörű ADR szabályzat 1.10 pontja foglakozik a közbiztonsággal. Az ilyen óvintézkedések alapvető céljaként határozza meg, hogy általa a lehető legkevesebbre csökkentsék a veszélyes áruk eltulajdonítását, ill. a velük való visszaéléseket, amelyek az embereket, az anyagi javakat vagy a környezetet veszélyeztethetik. [1]

Az fentebb említett direktíva általános alapelveket fogalmaz meg az érintett személyek kompetenciáinak részletezése és a lehetséges műszaki megoldások említése nélkül az általános feladatok, a képzés, valamint a közbiztonsági terv vonatkozásában.

Az általános feladatok között említi:

Az átmeneti tároló helyeken ill. terminálokon, jármű telephelyeken, kikötőkön és rendező pályaudvarokon belül a veszélyes áruk szállítása során átmeneti tárolásra használt területeket megfelelően biztosítani kell, jól meg kell világítani, és ha lehetséges és indokolt, az illetéktelenek elől el kell zárni.

Olyan készüléket, berendezést kell alkalmazni, illetve olyan intézkedéseket kell foganatosítani, amely megakadályozza, hogy a nagy közbiztonsági kockázattal járó veszélyes árut szállító járművet, ill. rakományát eltulajdonítsák, és biztosítani kell, hogy ezek az eszközök mindig jól működjenek.

A képzési feladatok között szerepel:

Az érintett személyek ADR-es kiképzésének és ismeretfelújító oktatásának a közbiztonsági szempontok tudatosítására is ki kell terjednie. A közbiztonsági szempontok tudatosítása során foglalkozni kell:

- a közbiztonsági kockázat jellegével,
- a közbiztonsági kockázat felismerésével,
- a kockázatkezelés és -csökkentés módszereivel és a közbiztonság megsértése esetén teendő intézkedésekkel.

Közbiztonsági Terv:

A nagy közbiztonsági kockázattal járó áruk (ld.: 4. fejezetben) szállításában részt vevő fuvarozóknak, szállítóknak, feladóknak és a többi résztvevőnek közbiztonsági tervet kell készíteniük, bevezetniük és annak megfelelően eljárniuk. A Közbiztonsági Terv tartalmi elemeként említi például:

- a szállítási információk fizikai védelmének biztosítására szolgáló intézkedéseket;
- fontos, hogy a közbiztonsági tervben szereplő szállítási információkhoz csak az érdekeltek juthassanak hozzá;
- a résztvevők felelősségével és feladatával arányban álló intézkedések egyértelmű meghatározását, amelyeket a közbiztonsági kockázat csökkentéséhez meg kell tenni, beleértve például: az üzemi eljárásokat, érzékeny infrastruktúra közelségét, a veszélyes árukhoz való hozzáférést az átmeneti tároló helyeken, útvonalak kiválasztását; a kockázat csökkentéséhez használandó eszközöket.

A fentiekben összefoglalt általános szabályozási elvekkel összhangban az alábbi közleményünkben a veszélyes áruk közúti szállítására és tárolására vonatkozó konkrét közbiztonsági ellensúlyozó intézkedéseket és alkalmazható műszaki megoldásokat elemezzük és adjunk közre, segítve ezzel a fuvarozást végző vállalkozásokat, valamint a hatóságok munkáját.

A VESZÉLYES ANYAGOT SZÁLLÍTÓ JÁRMŰVEKRE VONATKOZÓ KOCKÁZATCSÖKKENTŐ MEGOLDÁSOK

Az alábbi fejezetben a járművek azonosíthatósága szempontjából fontos adatokkal, a járművek fizikai védelmét szolgáló műszaki megoldásokkal foglalkozunk, valamint összefoglaljuk a személyzet adekvát képzési követelményeit.

A szállítójárművek biztonsága

A járművek biztonsága számos eszközzel/módszerrel növelhető, a vizsgált téma szempontjából az alábbiak tűnnek relevánsnak:

- Fontos a biztonsági berendezések kötelező jellegű és állandó használata;
- A biztonsági eszközöket a gyártóval rendszeresen ellenőriztetni kell;
- Minden járművet fel kell szerelni a feladatához szükséges szintű biztonsági eszközzel, és minden járművet el kell látni valamilyen típusú indításgátlóval;
- A járművek vásárlásakor célszerű a felszerelésbe biztonsági eszközt is belefoglalni, illetve a bővítési lehetőségekről érdeklődni;
- A biztonsági eszközökkel/módszerekkel kapcsolatban speciális biztonsági tanácsok részben a rendőrségtől és a biztosítótársaságoktól is beszerezhetőek;
- A teherautókat bármilyen rakománnyal/szállítmánnyal ellophatják. [2]

Lopásvédelem és lopás

Amikor lopásvédelemről/lopásról van szó, a gyártók és a tolvajok mindig új ötletekkel állnak elő és nem jelenthető ki, hogy az egyik vagy a másik oldal találékonyabb. Az emberi feledékenység miatt a mai lopásgátló eszközök általában önmagukat élesítik. Kikapcsolásukhoz általában kód, kódkulcs vagy kódkártya szükséges. A vásárlói igények miatt a járműgyártók manapság alapfelszereltségként kínálják a riasztórendszereket és az indításgátlókat. Ha azonban egy gyártó bevezet egy típust, azonnal hozzákezdhet az újabb kifejlesztéséhez, mert így az aktuálisat tálcán kínálja a tolvajoknak elemzésre. Célszerű a biztosítótársaságok által ajánlott berendezéseket beszerezni (ez egyúttal a biztosítási díjat is csökkentheti) és előírásszerűen alkalmazni.

Az indításgátlóknak az önálló és a riasztórendszerbe épített formái ismertek. Beépítésük előtt figyelembe kell venni a jármű típusát, a járműre és a rakományra leselkedő veszély nagyságát, illetve a be- és kirakodás folyamatát. Járműflotta esetén nem javasolt egyetlen rendszerrel felszerelni az egész flottát.

A kormányzárat, mint fizikai védőeszközt gyakorlatilag minden jármű gyárilag tartalmazza, de ez önmagában nem elegendő, mivel hatástalanítási módszere régóta ismert és akár kézi erővel is eltörhető.

Az adagolózárak benzinmotornál a motor beindítását akadályozzák meg (többféle lehetséges mód ismert), dízelmotoroknál az üzemanyag befecskendező rendszert bénítják meg. Megjegyzendő, hogy ha a tolvaj bejut a vezetőfülkébe és inaktiválja a kormányzárat, illetve kiengedi a kéziféket, a jármű elvontatható.

Az indítómotor-letiltó berendezésnek általában más riasztó/indításgátló rendszerbe integrált formái léteznek. Működését tekintve az indítómotor csatlakozó vezetékébe van bekötve.

A fékrendszer-letiltó berendezés a levegős fékrendszerek szelepeibe van beépítve – tekintve, hogy a kamion méretű szerelvények ilyen fékrendszerrel rendelkeznek. Általában más riasztó/indításgátló rendszerbe integrálva találjuk, ami a jármű rögzítőfékjének oldását akadályozza meg.

A kerékbilincsek rendszerint személygépkocsi és furgonméretű járműveknél használhatóak, nagyobbaknál már kevésbé praktikus a használatuk, jelentős súlyuk és méretük miatt. Megjegyzendő, hogy csak pontos felszerelés esetén védenek, és önmagukban nem elegendőek.

A pótkocsi biztosítására a legegyszerűbb módszer a vonószerkezet reteszelése egy acélsatuval vagy fedőlemezzel. Hátránya a jelentős súly és a kenőzsírok miatti erős szennyeződéssel járó felszerelés. Más megoldásként szóba jöhet a vontatmány támaszlábainak (gólyalábainak) reteszelése. Mindkettőt a sofőr működteti, így csak akkor védenek, ha a sofőr aktiválja őket. Bekamerázott járműveknél a kamerák rendszerint a jármű/pótkocsi hátsó részén találhatóak, és a védelem mellett a manőverezésben is segítenek.

Riasztórendszereken belül az immobilizálás nem akadályozza meg a jármű rongálását vagy kirakodását. A riasztórendszerek erős figyelmeztetőhangot bocsátanak ki, mely elrettentésre is szolgál, továbbá aktiválhatja az indításgátlót. Beszerezhetőek kézi (a sofőr által aktivált) és automata (önmagát aktiváló) riasztók is. Érdemes meghatározni, hogy a riasztó a jármű akkumulátoráról vagy egyéb áramforrásról működjön. A személygépkocsiknál és a furgonoknál az akkumulátorok elzárt helyen találhatóak, de a nagy teherautóknál viszonylag szabadon hozzáférhetők, könnyen szabotálhatóak, így esetükben célszerű külön áramforrásról működő riasztót választani. Célszerű olyan riasztóberendezést alkalmazni, melynek kulcsa/kártyája véletlenszerűen változtatja a deaktiválási kódot.

Lopás után segítik a jármű légi azonosítását, megtalálását a jármű tetején lévő jelölések. A nyomkövető rendszerek általában az eltulajdonítástól a megtalálásig eltelt időfaktort csökkentik. Manapság egyre nagyobb számban alkalmazzák őket, néha a beépítő cég vállalja az akár 24 órás megfigyelést is. A berendezések képesek lehetnek a jármű távolról történő immobilizálására, az ajtónyitások monitorozására, a riasztórendszer(ek) beindítására, illetve előre kijelölt terület elhagyásakor vagy abba történő belépéskor figyelmeztetni is.

A nagy fontosságú és kockázatú árukat szállító járművek védelme

A vontatmányok és áruk dokumentációinak mindig könnyen hozzáférhető állapotban és helyen kell lenniük, mert ez segíti a rendőrség munkáját. A minimálisan szükséges azonosítók a következők:

- jármű/pótkocsi rendszáma,
- gyártmány,
- típus,
- felépítmény típusa (pl. billenős, platós, ponyvás, dobozos, tartányos),
- alvázszám,
- motorszám,
- sebességváltó gyártási száma,
- egyéb azonosítószámok, jelölések és egyen-festési részletek,
- tengelyek száma,
- különleges berendezések (gyártási számokkal),
- biztonsági berendezések,
- futásteljesítmény.

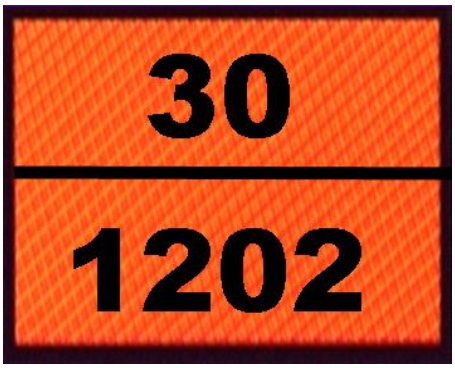
A járművet és a telephely eszközeit minden oldalról le kell fotózni, amely a lopás után a rendőrségnek nyújt segítséget a körözés kiadásában és az azonosításban. Elengedhetetlen a menetlevél pontos vezetése, melynek célszerű tartalmaznia a jármű, a sofőr, a szállítmány és az ezekkel kapcsolatba kerülő személyek (pl. a rakodók) adatait.

A járművek fizikai védelme tartalmazhat egyszerű eszközöket, például további megerősített zárakat vagy rácsokat. Riasztórendszerekből többféle is felszerelhető. Egyszerű, de hatékony védelem a jármű izolálása/elzárása a környezettől. Jelenleg széles körben alkalmazzák a csapódó-zárakat, melyek a rakomány védelmét szolgálják (az ajtó becsukása után a zár automatikusan reteszelt helyzetbe kerül). Ehhez annyit kell hozzáfűzni, hogy a csapódó-zárak leggyengébb pontja a környező karosszéria, mert könnyen kivágható. A járművek manapság egyöntetűen válaszfallal (homlokfallal) vannak felszerelve a sofőr és a rakomány között, így a rakományhoz csak a raktérajtó nyitása útján lehet eljutni. A tömör, masszív válaszfalak előnyösebbek, mert ezeken nem lehet átlátni, így a tolvaj sem látja, mi van a raktérben.

További védelmet jelent az e körbe tartozó rakomány esetén, ha külön riasztórendszert szerelnek a vontatóra, a vontatmányra, a tartányra és ezek zárjaira is. Megfontolandó a külön áramforrás más járműelemen való elhelyezése is.

Külön ki kell emelni a robbanó anyagok biztosítását. Bizonyos mennyiségen felüli robbanó anyag szállításakor a gépkocsivezető mellett árukísérőnek is kell lennie, és a szállítás a lehető legrövidebb időtartamú kell legyen. Ilyen típusú szállítás csak az adott anyagok tárolására alkalmas, biztonságos helyszínei között végezhető. Az illetéktelen hozzáférést mindenképpen meg kell akadályozni, akár a rendőrség igénybevételével. A szállítmány ellenőrzésének számát a lehető legkisebbre kell korlátozni (az illetéktelen hozzáférés elkerülése érdekében).

A szilárd ammónium-nitrátot tartalmazó műtrágya egy speciális veszélyes anyagnak számít, így erre az anyagra is a robbanóanyagoknál leírt elveket kellene vonatkoztatni. A veszélyes árut szállító tartányos, illetve ömlesztett módon szállító járműveket minden esetben el kell látni az ún. számozott sárga táblával, melynek számkódjai a szállított veszélyes áru fajtájáról, illetve a vele kapcsolatos veszélyekről tájékoztatnak. [3] Az 1. ábrán egy ilyen ADR-tábla látható.



1. ábra. ADR-tábla. (ADR 2009 alapján)

Ismeretes, hogy a veszélyes árut szállító személyek részére az ADR-ben rögzített témákban rendszeres oktatásokat kell tartani. A gépjárművezetőket az áru veszélyeztető tulajdonságainak ismertetésén túl fel kellene készíteni arra, hogy mi a teendő járműeltérítés vagy támadás esetén; pl. önmaguk biztonságát sohasem veszélyeztethetik a szállított áru biztonsága érdekében. [2] Szükség esetén a tudnivalók kis könyvecske formájában elhelyezhetőek a szállítójárműben. A járművezetőknek természetesen részletesen ismerniük kell a jármű és a tároló telep biztonsági felszereléseit, illetve ezek optimális alkalmazását a közbiztonsági problémák megelőzésére.

Ugyanakkor a fent említett alapképzésen túl, a veszélyes és/vagy nagyértékű árukat szállító személyeknek külön, részletesebb oktatás szervezése és tartása is indokolt lenne. Ugyancsak indokolt lenne képzést tartani a kockázatfelmérésben vagy a közbiztonsági kivitelező folyamatban szerepet játszók számára is. Jelenleg hazánkban csak az ADR-es gépkocsivezetők fentebb említett oktatásához kiadott tanterv tartalmaz ilyen irányú kötelezettségeket. [4]

A „közbiztonsági” oktatásoknak tehát, foglalkozniuk kell a biztonsági kockázatok természetével, felismerésével, lehető legkisebbre csökkentésükkel, illetve az események kezelése során szükséges teendőkkel. A képzésnek olyan konkrét információkat kell közvetíteni, amely alkalmazható az érintett dolgozók mindennapi munkájában. Tisztázni kell azt is, hogy adott esetben kinek mi a teendője, ki miért felel. Természetesen itt is követelmény a foglalkozások megfelelő dokumentálása, szükség esetén vizsga is tartható.

A VESZÉLYES ANYAGOK TÁROLÁSÁRA SZOLGÁLÓ HELYSZÍNEKKEL KAPCSOLATOS MEGFONTOLÁSOK

A veszélyes anyag rakományú járművek tárolására, fogadására szolgáló helyszíneken - a helyszín sajátosságait nem számítva - a legfőbb probléma a járművek ismert vagy kiszámítható mozgása. Külön problémát jelentenek az üzemanyag szállító járművek, hiszen a célállomáson végzett áttöltéskor a helyszínre vonatkozó irányelvek nem alkalmazhatóak, legfeljebb a helyszín helyi kialakítása különítheti el a járművet a közforgalomtól és az illetéktelen hozzáféréstől.

Alapvetően négyféle helyszíntípust különböztetünk meg az áru mennyisége, előfordulása/használata és fontossága alapján [2]:

1. szint: kis mennyiségben vagy ritkán használt, alacsony fontosságú áruk;
2. szint: nagy mennyiségben vagy gyakrabban használt, alacsony fontosságú áruk;
3. szint: kis mennyiségben használt, nagy fontosságú áruk;
4. szint: nagy mennyiségben használt, nagy fontosságú áruk (a kórokozók is).

Az *1. szintű* helyszínnek csak azt a részét kell biztosítani, ahol a veszélyes áruk tárolása történik. Elég lehet egy széf is, de használható zárható ajtóval ellátott, hegesztett hálós ketrec is. A belépés szükség szerint korlátozható és ellenőrizhető.

A *2. szintűnél* lehetséges, hogy az egész helyszínt biztosítani kell. Szabad ég alatti tárolásnál használható egy 2 m magas hegesztett hálós kerítés (szögesdróttal a tetején). A belépés szintén korlátozható, akár azonosítás céljára szolgáló fényképezés is alkalmazható. Járművekben történő tárolás esetén a kerítés lehet láncalapú, ha a jármű biztosítása önmagában elegendő a védelemhez (a járművek fokozottan őrzöttek, a pótkocsik önmagukban nem mozgathatóak, vagy a jármű mozgását cövekek akadályozzák). Kerítés helyett alkalmazható a jármű mozgását lehetetlenné tevő árok is (híddal).

A *3. szintű* helyszín teendői megegyeznek az 1. szinten lévőkkel, de az óvintézkedések megkettőzhetőek (pl. körbekerített széf).

A *4. szintű* helyszínen legalább 2 m magas hegesztett hálós, szögesdróttal ellátott kerítés szükséges, fényképes beléptető rendszerrel. A kerítést riasztórendszerrel kell ellátni, melynek a biztonsági erőknél kell jeleznie (pl. a rendőrségen).

Operatív tevékenységet tekintve az 1., 2., 3., szinten elegendő a rendőrségen tett azonnali feljelentés, ha behatolás/lopás jele észlelhető a napi helyszínellenőrzés során. Nagyobb fontosságú áruk esetén naponta szükséges lehet biztonsági jelentés készítése, leadása.

A tárolási helyszín kiválasztásakor érdemes kikérni a rendőrség és a biztosítótársaságok véleményét, továbbá építész tanácsát a helyszín ismeretében, és kockázatbecslést kell végezni. (A szállítás baleseti kockázat becslésével a 3. fejezet foglalkozik). Ebben az esetben a kockázat egy törvénytelen cselekedet sikeres véghezvitelének megvalósítási valószínűsége. Felméréséhez elengedhetetlen a cél sérülékenységének és a veszély mértékének ismerete, melyet indokolt írásba foglalni. Első lépés az információgyűjtés, majd a kockázatelemzés és a kockázatértékelés alapján meghatározzuk az ellensúlyozó intézkedéseket, amibe beletartozik a szükséges eszközök, műszaki megoldások számba vétele is.

A helyszín védelmére, az illetéktelenek távol tartására az alábbiakban kifejtett intézkedések jöhetnek szóba.

Belépési korlátok, szabályozók

A látogatókat előre be kell jelenteni, be kell léptetni és csak kísérővel mozoghatnak. Az elektronikus eszközeiket az őrségnél kell hagyniuk. Nagy fontosságú veszélyes áruk esetén az alkalmazottak mozgását, kritikus tárgyakhoz vagy területekhez való hozzáférését ellenőrizni kell, továbbá:

- Fizikailag meg kell akadályozni az áramforrásokhoz, a nagy fontosságú áruhoz, számítógépes rendszerekhez vagy nagy értékű berendezésekhez való hozzáférést.
- Az üzleti szempontból érzékeny információkhoz való hozzáférést hardveresen és szoftveresen is védeni kell.
- A személyzetnek állandóan fényképes azonosítót kell viselnie.
- A szerződéses munkatársak mozgását, belépését és személyes tárgyainak bevitelét szintén ellenőrizni kell.

A beléptető rendszernek a már meghatározott jogosultságok alapján történő mozgások szabályozása mellett biztosítania kell néhány munkavédelmi feltételt is. Ezek közé tartozik, hogy bizonyos terekbe csak kettesével biztosítson belépést, amennyiben a helyiségben más személy nem tartózkodik. A baleseti veszélyforrásokat is jelentő zárt veszélyes árutárolók esetében a kétkártyás zárvezérlés jelenthet megoldást. Ilyenkor a helyiségek zárjának nyitása csak akkor engedélyezett, ha két feljogosított kártyát egymás után olvasnak le. A bennlévők listázása pedig lehetővé teszi a rendszer által felügyelt terekben tartózkodók számának és személyének nyomon követését. [6]

A szállítójárművek tárolása, felügyelete

A belépési pontok megtervezésekor ügyelni kell a vészkijáratok elhelyezésére és a mozgáskorlátozottak számára fenntartott belépési helyszínre. Ki kell zárni annak a lehetőségét, hogy egyszerre több személy vagy jármű jöjjön át egy adott kapun, vagy megkerüljék az illető kaput. A nem várt járműveket azonosítani kell a bebocsátás előtt.

Kutatás és motozás alkalmazása beléptetés előtt nagy fontosságú áruknál különösen a kórokozókkal foglalkozó helyszíneken javasolt, melyet csak képzett személyzet végezhet, megfigyelővel. A kutatás és motozás végezhető véletlenszerűen is.

A járművek tárolása zárt épületekben különösen éjszaka, legfeljebb furgonméretű járműveknél megoldható (tűzveszély is fennáll). A nagyméretű szállítójárművek tárolása rendszerint a szabadban történik. Nem célszerű a kerítés mellé parkolás, mert így könnyű hozzájuk férni. Legegyszerűbb a járművek szorosan egymás mellé történő parkoltatása úgy, hogy a megrakott járművek középen helyezkedjenek el.

Nagy fontosságú áruk esetén a szállítójárműben történő tárolás nem javasolt sem éjszaka, sem nappal. Ha mégis szükséges az áru járműben történő tárolása, akkor biztos helyszín, lezárt jármű, bekapcsolt riasztó és/vagy indításgátló szükséges, megfelelő helyre elzárt járműkulcsokkal.

A védett vagy „biztos” tárolási helyszín első fizikai határvonala a kerítés. Figyelembe kell azonban venni, hogy minden kerítés átvágható vagy kikerülhető. Általában a szabványok láncelemekből, hegesztett hálóból állót vagy biztonsági mintázatút tartalmaznak. Ezekre riasztórendszer is felszerelhető, ami azonban riaszthat túl gyakran, ha a kerítés forgalmas út vagy járda mellett van. A legpraktikusabb a dupla vagy tripla kerítés, ahol a belső(k) riasztóval és kamerarendszerrel van(nak) ellátva. Célszerű a legbelsőt a legnehezebben áthatolhatóvá tenni. Alkalmazhatóak elektromos kerítések is. A természetes akadályok (folyó- vagy állóvíz, illetve mezők) nem megbízhatóak. A kerítések felszerelhetőek szögesdróttal is,

amely kiváló elrettentő eszköz, de nem lehet a járókelők által elérhető helyen. A kerítéseket időközönként karban kell tartani. Lehetséges szögesdrót kerítéstípust szemléltet a 2. ábra.

2. ábra. Szögesdróttal felszerelt kerítés
Forrás: www.bildarchiv-hamburg.de

A dombok és árkok csak megfelelő elhelyezés esetén védenek, de általában csak a járművek ellopása ellen.

A kapuk erősségének arányosnak kell lenni a veszély nagyságával, a kapuknak pedig legalább olyan erősnek kell lenniük, mint a kerítésnek. A legjobbak a sínen csúszó elektromos kapuk, mert ezek jobban tartanak, mint a zsanérosak, de jók a zárral/zárakkal ellátott fémkapuk is.

Ajtók esetében mindenképpen a nehéz, nagy, a falhoz megfelelően rögzített konstrukciójú ajtók javasoltak. A szellőzővel ellátott ajtókon a szellőzőnyílásnak stabilan rögzítve kell lennie. Ahol csak lehet, dupla ajtókat, továbbá rácsokat, rolókat kell használni. A földszinti ablakoknak törhetetlennek és megfelelően rögzítettnek kell lenniük, továbbá boríthatóak ráccsal, rolóval vagy fóliával.

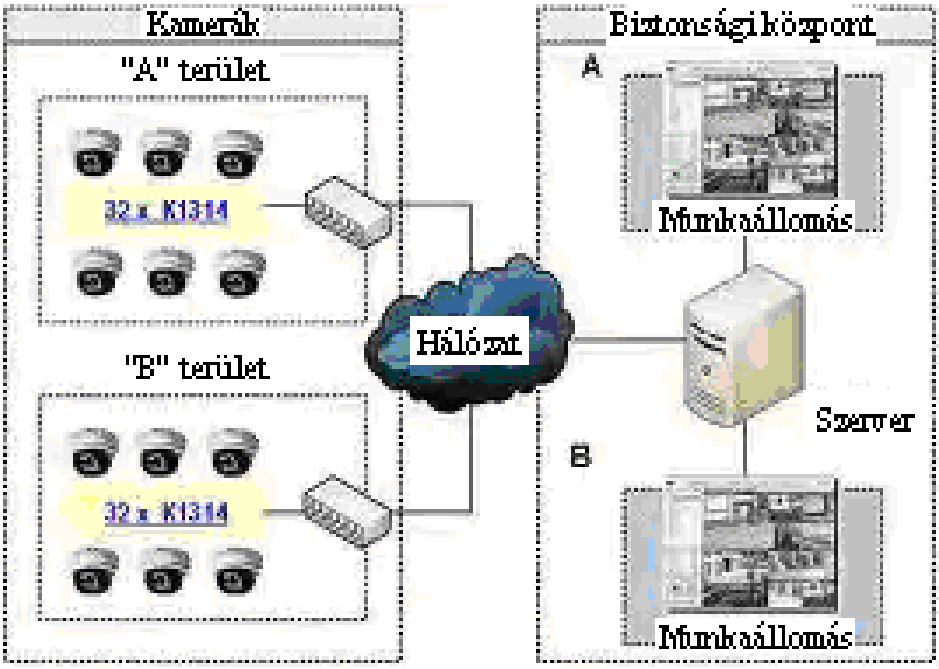
Előnyös, ha a falak, mennyezetek és a padlók fémet vagy erősített betont tartalmaznak. A falaknak kisebb ütközéseket is ki kell bírniuk, illetve az érintkező széleknek is ugyanilyen erősségűnek kell lenniük.

A tároló létesítmények riasztórendszerei főleg a kapuknál, de mozgásérzékelővel kiegészítve bárhol, például a kerítéseknél is használhatóak. Fontos az érzékenységi szint beállítása, hogy ne riasszanak mindenre. Figyelembe kell venni, hogy a rendőrség esetleg a korábban sok téves riasztást leadó helyszínre csak lassan vagy egyáltalán nem reagál. A riasztórendszereket célszerű képalkotásra is képes berendezésekkel kiegészíteni.

Az adott terület megfigyelése feltételezi a jó beláthatóságot és megvilágítást. A megfelelő megvilágíthatóság pedig magában foglalja a zavaró növényzet, tárgyak, objektumok eltávolítását. A jó világítás:

- elrettent a belépéstől,
- elrejti az őröket,
- segíti az őrök és a zártláncú TV vizuális megfigyelését,
- megvilágítja a belépési pontokat,
- segíti a járművek átkutatását.

Video megfigyelés céljából a nagyfelbontású, nagyításra is képes, lehetőleg színes kamerákat/zártláncú TV-t (3. ábra) célszerű 24 órában üzemeltetni, továbbá a felvételeket rendszeres időközönként ellenőrizni is kell. Fontos, hogy az őr állandóan lássa a monitort, de a látogatók ne láthassák azokat. A zártláncú TV-nek minden fontos pontot le kell fednie, akár rendszeres időközönként végzett kameramozgatással (4. ábra).



3. ábra. Megfigyelő rendszer felépítési sémája
Forrás: www.dvbtinform.hu

4. ábra. Video megfigyelő
Forrás: www.multisecurity.hu

A rendszer legalapvetőbb hibái a következők:

- a készülék bekapcsolásának elmulasztása,
- nincs elegendő szalag/memória,
- a szalagok/memóriák/készülékek elhasználódása.

Még nagyobb lefedettséget biztosít a (sötétített) gömbkamerák használata (ld.: 4. ábrán középen), mert a behatoló nem tudja megmondani, hogy melyik kamera látja. A külső falakra előnyösebb és olcsóbb rögzített kamerákat telepíteni. Egyszerre természetesen több kameratípus is felszerelhető. Felállíthatóak külön kameratartó oszlopok is, hogy a kamerák ne

legyenek az épületek geometriájából fakadó korlátoknak kitéve (ld.: 4. ábrán). Alkalmazhatóak mozgásdetektorok által aktivált fényképezőgépek is. Itt is fontos a rendszeres karbantartás és a lencsevédők rendszeres cseréje (eltorzíthatja a látott képet). Előnyös, ha több kamera is néz ugyanarra a helyre. Képrögzítő eszközök használatakor ügyelni kell a személyiségi jogokra.

Az őrző-védő szolgálat személyi állományával szemben - a nagyfontosságú veszélyes áruk őrzéséből kifolyólag - elengedhetetlen a megbízhatóság. Ők képviselik a legdrágább őrzési módszert, mert a 24 órás időtartam lefedéséhez több váltásra van szükség. A biztonságra nézve kompromittáló lehet az őrök „ismeretsége" az alkalmazottakkal. Fontos az őrök oktatása a vállalat tevékenységével, értékeivel kapcsolatban. A járőrözésnél figyelembe kell venni, hogy egy adott helyre ne ugyanabban az időpontban érkezzenek. Vészhelyzetben a biztonsági cégnek/őröknek tudniuk kell, hogyan vegyék fel a kapcsolatot hatékonyan az értesítendő személlyel.

A tároló telep, illetve az ott leparkolt és lezárt járművek kulcsait egy zárható szekrényben kell tartani. Ebbe a helyiségbe csak az illetékes személyek léphetnek be. Rögzíteni kell, hogy melyik kulcs mikor és kinek lett kiadva. Nyitvatartási idővel rendelkező telephelynél fontos annak ismerete, hogy kinél vannak a belépéshez szükséges kulcsok (e személyek számának minimálisnak kell lennie). A kulcs elvesztése esetén zárat vagy járművet kell cserélni, illetve megfontolandó a kulcsszekrény más helyiségbe/épületbe való áthelyezése is.

További, a tárolás biztonságos működési feltételeit rontó körülmények meglétét is figyelemmel kell kísérni. Így például hibának számít kerítés mellé helyezni a raklapokat, mert ezek természetes lépcsőként szolgálhatnak. Nem célszerű felügyelet nélkül hagyni a nehéz munkagépeket sem, mert velük a kerítések és a kapuk könnyen károsíthatóak. A pótkocsikat le kell akasztani a vontatókról és mozgás- vagy csatlakozás-gátlóval kell őket ellátni. A ponyvákat az üres vontatmányokon célszerű felhajtani, mert az üres vontatmány látványa nem vonzza a tolvajokat. Sohasem szabad elfeledkezni a járművek és a személyek átkutatásáról.

A KÖZÚTI VESZÉLYESÁRU-SZÁLLÍTÁS BALESETI KOCKÁZATA, ANNAK ÉRTÉKELÉSE ÉS KEZELÉSE [5]

Az előző fejezetekben tárgyalt, szándékosan előidézett közbiztonsági veszélyhelyzetek (lopások, terrorcselekmények) megelőzési lehetőségeinek ismerete napjainkban egyre nagyobb jelentőségű. A mindennapi gyakorlatban ugyanakkor az emberi gondatlanságból illetve műszaki meghibásodásból fakadó balesetek kezelése nagyfokú publicitásuk okán is, jelentősen befolyásolja a lakosság közbiztonságról alkotott véleményét. Ennélfogva, továbbá a biztonságos szállítási útvonal megtervezése érdekében röviden érdemes áttekinteni a kockázat fogalmát, illetve a közúti veszélyesáru-szállítás baleseti kockázatát befolyásoló tényezőket.

A nemzetközi szakirodalmában általánosan elfogadott, hogy a veszély bekövetkeztének mértékét a kockázattal fejezik ki. A kockázat mértékének - mely a bekövetkezés valószínűségéből és a következmények súlyosságából együttesen adódik - megítélését követően a legfontosabb cél a kockázattal arányos védelem megkeresése.

Bármilyen veszélytől csak úgy lehet megvédeni valakit, ha információval rendelkezik arról, hogy:

- Hol fenyegeti veszély?
- Milyen veszély fenyegeti?
- Milyen lehetősége van a veszély elleni védekezésre?
- Hogyan értesül a veszélyről?
- Mi a tennivalója veszély esetén?

A kockázat értékelésének, kezelésének folyamata tervezést igényel. Ehhez azonosítani kell a potenciális veszélyforrásokat, aminek a legfontosabb célja esetünkben az adott településen/térségen belül előforduló veszélyes áruk (anyagok) típusainak meghatározása, amelyek szállítása közúton történik. Ez az alábbi lépésekben írható le:

- Hol következhetnek be súlyos balesetek (meg kell határozni a veszélyes anyagok fuvarozására igénybe vett főbb útvonalakat)?
- Milyen veszélyeztető hatást jelent egy lehetséges baleset?
- Milyen típusú balesetek valószínűsíthetőek?
- Kit és mit fenyegethet, veszélyeztethet?
- Következtetések, értékelés: a lehetséges kár becslése, a lehetséges kárszínhelyek.
- Kockázati tényezők, amelyek egy fuvarozási baleset bekövetkezését növelik, vagy következményét súlyosbíthatják.
- Az eredmények dokumentálása.

A veszélyhelyzeti (veszélyelhárítási) terv mellékleteként szereplő ún. folyamattanulmány készítését segíthetik az ipari és fuvarozó/szállítmányozó cégektől és a Közlekedési Felügyelettől begyűjthető adatok, illetve a veszélyes anyagokat szállító gépjárművezetők kikérdezése. Azonosítani kell a magas esemény-, illetve baleseti mutatójú útvonalakat, át kell tekinteni az egyéb közlekedési balesetek adatait, illetve elemezni kell a ki- és berakodás, fuvarközi tárolás közben történt eseményeket, baleseteket.

A következő lépés a közúti veszélyes áruk szállításából eredő kockázatok megbecsülése. A következményi károkat az is befolyásolja, hogy az érintett területnek milyen a beépítettsége, vagy az adott településnek milyen a lakósűrűsége, a település-szerkezete és a közmű-kiépítettsége. [7]

Általánosan azt mondhatjuk, hogy a csoportmunka, közös értékelés a legcélravezetőbb. Nem elég csupán a baleset bekövetkezése utáni intézkedésekre koncentrálni, lehetőség szerint a megelőzést szolgáló helyi megoldásokat is nevesíteni kell, a végrehajtási ütemezéssel együtt. A vészhelyzet során bevetendő elhárító erőket az adott terület sajátosságainak megfelelő feladatorientált kiképzésben kell részesíteni a terv alapján.

KÖZBIZTONSÁGI ALAPELVEK, FOGALMAK

Az alábbi fejezetben a közleményben előforduló fogalmak meghatározását, pontosítását, valamint bizonyos közbiztonsági alapelvek kifejtését láttuk indokoltnak.

Fizikai biztonság: az ésszerűség határain belül a lehető legnehezebbé kell tenni egy termék ellopását, beleértve a saját alkalmazottak általi lopást is, mely helyszínenként és árutípusonként eltérő lehet. Ebben segít a nemzetközi szakirodalomban meghonosodott úgynevezett *3D elv,* amiben a sorrend fontos:

- *elrettentés (deter)*– minden ilyen célt szolgáló fizikai és elektronikai eszközzel.
- *felismerés/felfedezés (detect)*– riasztórendszerek alkalmazása, lehetőleg zártláncú televízióval (CCTV).
- *késleltetés (delay)*– olyan fizikai eszközökkel, amelyek visszatartják a tolvajt a rendvédelmi erők kiérkezéséig.

A 3D elv természetesen nem alkalmazható közterületre (parkoló, éjszakai pihenő, szerviz, üzemanyagtöltő állomás), de óvintézkedések ilyenkor is tehetőek. [2]

Dokumentálás: az oktatásra vonatkozó iratokat a munkáltatónak és a munkavállalónak is meg kell őriznie, és új munkakör betöltése esetén ellenőrizni kell.

Dokumentálás az illetékes hatóság által: a járművezetők érvényes oktatási bizonyítványairól naprakész nyilvántartást kell vezetni.

Értesítési kötelezettség: közbiztonságra veszélyes helyzet esetén a résztvevőknek azonnal értesíteniük kell a rendőrséget és rendelkezésre kell bocsátaniuk az intézkedéshez szükséges információkat.

Járműszemélyzet tagja: a járművezető és minden olyan személy, aki biztonsági, közbiztonsági, oktatási vagy üzemi okból kíséri a járművezetőt.

Jármű: battériás jármű, fedett jármű, nyitott jármű, ponyvás jármű és tartány jármű.

Közbiztonsági terv: a nagy kockázattal járó veszélyes áru szállításában résztvevők által készített és alkalmazott, meghatározott tartalmi elemekből álló dokumentum.

Nagy kockázattal járó veszélyes áru: amellyel terrorista cselekmények során vissza lehet élni, ami súlyos következményekkel járhat, pl. tömeges balesetet vagy tömegpusztítást idézhet elő. A nagy közbiztonsági kockázattal járó veszélyes árukat 1. számú táblázat tartalmazza.

Osztály	Alosztály	Anyag vagy tárgy	Mennyiség		
			Tartányban (l)[c)]	Ömlesztve (kg)[d)]	Küldemény -darabban (kg)
1	1.1	Robbanóanyagok és -tárgyak	a)	a)	0
	1.2	Robbanóanyagok és -tárgyak	a)	a)	0
	1.3	C összeférhetőségi csoportba tartozó robbanóanyagok és -tárgyak	a)	a)	0
	1.4	UN 0104, 0237, 0255, 0267, 0289, 0361, 0365, 0366, 0440, 0441, 0455, 0456 és 0500 alá tartozó robbanóanyagok és -tárgyak	a)	a)	0
	1.5	Robbanóanyagok	0	a)	0
2		Gyúlékony gázok (a csak F betűt tartalmazó osztályozási kódok)	3000	a)	b)
		Mérgező gázok (T, TF, TC, TO, TFC vagy TOC betű(ke)t tartalmazó osztályozási kódok), az aeroszolok kivételével	0	a)	0
3		I és II csomagolási csoportba tartozó gyúlékony folyékony anyagok	3000	a)	b)
		Érzéketlenített robbanóanyagok	0	a)	0
4.1		Érzéketlenített robbanóanyagok	a)	a)	0
4.2		I csomagolási csoportba tartozó anyagok	3000	a)	b)
4.3		I csomagolási csoportba tartozó anyagok	3000	a)	b)
5.1		I csomagolási csoportba tartozó, gyújtó hatású, folyékony anyagok	3000	a)	b)
		Perklorátok, ammónium-nitrát, ammónium-nitrát műtrágyák és ammónium-nitrát emulziók, szuszpenziók vagy gélek	3000	3000	b)
6.1		I csomagolási csoportba tartozó mérgező anyagok	0	a)	0
6.2		„A” kategóriába tartozó fertõző anyagok (UN2814 és 2900)	a)	0	0
7		Radioaktív anyagok	3000*A1* (különleges formájú), ill. 3000*A2* aktivitás *B(U)*, *B(M)* vagy *C* típusú küldeménydarabban		
8		I csomagolási csoportba tartozó maró anyagok	3000	a)	b)

1. táblázat. A nagy közbiztonsági kockázattal járó veszélyes áruk felsorolása (ADR 2009 alapján)

Megjegyzés a táblázathoz:

a) Tárgytalan.

b) Az ADR-szabályzat 1.10.3 szakaszának előírásait nem kell alkalmazni, akármennyi is a szállított mennyiség.

c) Az ebben az oszlopban megadott értéket csak akkor kell alkalmazni, ha az ADR-szabályzat 3.2 fejezet „A" táblázat 10 vagy 12 oszlopa szerint a tartányban való szállítás megengedett. Azokra az anyagokra vonatkozóan, amelyek tartányos szállítása nem megengedett, ezen oszlop utasítása tárgytalan.

d) Az ebben az oszlopban megadott értéket csak akkor kell alkalmazni, ha az az ADR-szabályzat 3.2 fejezet „A" táblázat 10 vagy 17 oszlopa szerint az ömlesztett szállítás megengedett. Azokra az anyagokra vonatkozóan, amelyek ömlesztett szállítása nem megengedett, ezen oszlop utasítása tárgytalan.

Szállítás: fogalma kiterjed a veszélyes áruk átmeneti tárolására is azzal a feltétellel, hogy az áru átvételének és kiszolgálásának helyét feltüntető fuvarokmányt kérésre bemutatják, illetve a küldeménydarabokat vagy a tartányokat nem nyitják fel kivéve, ha az illetékes hatóságok ellenőrzik.

Tartány v. tartányos jármű: folyadékok, gáz halmazállapotú, pontszerű vagy szemcsés anyagok szállítására használt, egy vagy több rögzített tartánnyal felszerelt jármű.

Tartány: maga a tartányköpeny, beleértve annak üzemi és szerkezeti szerelvényeit is. A tartányköpeny az anyagot tartalmazó burkolat.

KÖVETKEZTETÉSEK

A cikkben bemutatottak alapján megállapítható, hogy a veszélyes áruk közbiztonsági szempontból megfelelő szállításának és tárolásának legalapvetőbb feltétele a megelőzés, vagyis az eltulajdonítás megakadályozása az arra alkalmas eszközök, módszerek segítségével. A megfelelő biztonsági környezet előzetes, tervszerű kialakításával a közbiztonsági kockázat jelentősen csökkenthető. A prevenció mellett természetesen meghatározó szerepe lehet egy nemkívánatos esemény bekövetkezésekor a gyors, hatékony beavatkozásnak is, gondoljunk esetleg egy folyamatban lévő rablási kísérlet szakszerű meghiúsítására vagy egy eltulajdonított jármű sikeres lokalizálására, az értékek biztonságos visszaszerzésére.

Az is nyilvánvaló, hogy a gondosan megtervezett biztonsági rendszerek és előírások mellett is nagyon sok múlik a gépjárművezetők felkészültségén és viselkedésén. A legnagyobb sikert nem az a járművezető jelenti, aki akár az élete árán is megvédi a rakományát a rablóktól, hanem inkább az, aki megfelelő óvatossággal tudja kezelni az érzékeny helyzeteket és el tudja kerülni a kockázatos szituációk kialakulását.

A nagy fontosságú, értékes áruk esetében ugyanakkor nem megvetendő eszköz az áru mibenlétével, nevével, szállítási kiindulópontjával/célállomásával kapcsolatos dezinformációk alkalmazása sem. Természetesen kiemelten fontos megjegyezni, hogy az érvényben lévő szabályozókkal a dezinformációs erőfeszítéseink semmilyen formában nem kerülhetnek összeütközésbe, tehát például a hivatalos fuvarokmányok nem tartalmazhatnak hibás vagy félreértelmezhető adatokat.

Felhasznált irodalom

[1] ADR 2009. pp.72-75.

[2] Guidance for the security of dangerous goods by road, DOT, 2005. pp.1-18.

[3] Dr. Lázár G.: Veszélyes anyagok szállítása, egyetemi jegyzet, ZMNE 2010.p. 106.

[4] Tanterv és útmutató ADR képesítő szaktanfolyamok számára; KFF; 2005. p. 18.

[5] Lázár Gábor: A hazai ADR balesetek jellemzői és elhárításuk stratégiai, taktikai elemzése. PhD-értekezés. 2006. pp. 57-74.

[6] Dr. Berek Tamás: ABV (CBRN) analitikai laboratórium beléptető-rendszere a biztonságos üzemeltetés szolgálatában, Hadmérnök VI. Évfolyam 2. szám, 2011. június http://www.hadmernok.hu/2011_2_berek.pdf pp. 29-30.

[7] Dr. Hornyacsek Júlia: A repülőterek környezetében lévő települések katasztrófavédelmi feladatai, Repüléstudományi Konferencia Szolnok, 2011. VII. Katonai műszaki szekció Repüléstudományi Közlemények On-line Tudományos Folyóirat, ZMNE, 2011/2 különszám, http://www.szrfk.hu/rtk/index.html

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Csépainé Széll Pálma
palma.szell@gmail.com

A HELYI ÖNKORMÁNYZATI FELADAT- ÉS HATÁSKÖRÖK ELOSZTÁSÁNAK LEHETSÉGES IRÁNYAI AZ ÚJ ÖNKORMÁNYZATI TÖRVÉNYBEN

Absztrakt

A helyi önkormányzatok legfontosabb megkülönböztető jellemzője, hogy kiterjedt önállósággal intézik a hatáskörükbe tartozó ügyeket. Ugyanakkor az elmúlt két évtized talán legfontosabb tanulsága az lehetne, hogy milyen szoros kapcsolatban áll egymással az ún. nagypolitika és a helyi politika, hogy a lokális döntések gyakorlatilag az egész állami döntéshozatali rendszert áthatják, meghatározva ezzel a központi döntések jellegét és irányait. Ezért a feladat- és hatáskörök újraelosztását egyszerre, a központi-területi és helyi szinten, egymással szerves egységben kell megvalósítani, egyik szféra reformlépései nem helyettesíthetőek a másik bármekkora reformugrásaival.

The local government main distinguishing characteristic is the extensive independence within their execution of duties that belong to their competence. However, over the past two decade, perhaps the most important conclusion could be that there is a close link between the local and the governmental politics, meaning that the local decisions that are made affect the state's decision making's nature and direction. This is why competencies and duties redistribution are made in unity locally, regionally, and centrally. Each sector's reforms can not be substituted with another sector's reforms.

***Kulcsszavak**: települési önkormányzat, helyi közszolgáltatás, alkotmány, reform ~ local government, local public servise, constitucion*

A SZABÁLYOZÁSI RENDSZER FELÜLVIZSGÁLATÁNAK ELVEI

A komplex törvényelőkészítő munka egyik alapvető része a helyi önkormányzatok szerepének általános és szintenkénti (településtípusra is tekintettel) meghatározása. Nem új keletű kérdés, hogy milyen munkamegosztás legyen a helyi önkormányzatok és az állam között a közfeladatok ellátása tekintetében; milyen irányba történhet elmozdulás, az önkormányzatok önállóságának kiterjesztése, vagy az állam szerepének erősítése kerül előtérbe? Jelenleg ellentmondásos helyzettel állunk szembe, ugyanis a helyi önkormányzatok (érdekképviseleteik) általános célként fogalmazzák meg, hogy az önkormányzati autonómiát erősíteni szükséges a lakossági igények, közösségi érdekek megvalósítása előfeltételeként. Érvényt kell szerezni a szubszidiaritás európai elvének. Ebből következik, hogy olyan feladatok kerüljenek a szükséges helyi ismerettel rendelkező önkormányzatokhoz, amelyek folytán a lakossághoz közeli ügyintézés lehetővé váljon, tehát az ehhez szükséges feltételek zavartalanok legyenek és folyamatosan rendelkezésre álljanak.[1]

Az ésszerűség, a hatékonyság és finanszírozhatóság szempontjait együtt kell érvényesíteni a célszerűség, az életszerűség elvével. Kétségtelen, hogy mindezeket nagymértékben befolyásolja a jelenlegi gazdasági kiszolgáltatottság, a nagymértékű financiális függés, amely minden korban a centralizációs visszarendeződések legfontosabb éltető eleme, ezért a jelenleg folyó monetáris, restrikciós gazdaságpolitika éppen az említett irányba hat. Mindezek ellenére nem szabad szem elől veszíteni, hogy a helyi önkormányzatok működésének nem csupán elégséges, hanem szükséges feltétele a gazdasági önállóság, a pénzügyi függetlenség megtartása.

Kétségtelen, hogy a helyi közügyek körében az államnak (központi szerveknek) továbbra sem szabad szerepet vállalni, továbbra is a helyi önkormányzatiság alapelveként kell meghatározni az alábbiakat:

- a helyi közösség (az önkormányzat) jogát az önálló tulajdonhoz és ehhez kapcsolódó önálló gazdálkodási, vállalkozási jogot;
- az önálló szabályozási (rendeletalkotási) jogot;
- a helyi közügyek köréhez kapcsolódó igazgatási jogot;
- a helyi adóztatás (a helyi célok megvalósításához szükséges közkiadások forrásának megteremtése) jogát;
- az általános (állami) közfeladatok ellátásához szükséges, a feladatokkal arányban álló állami támogatáshoz való jogot;
- az önálló szervezetalakítási jogot;
- a társuláshoz (érdekvédelemhez), nemzetközi együttműködéshez kapcsolódó jogokat;
- az alkotmánybírósági és bírósági jogvédelemhez való jogot.

Az önkormányzatok abban érdekeltek, hogy a társadalomirányítás rendszerében a decentralizáció erősödjön és a centralizáció (az állami szerepvállalás) ne haladja meg az európai uniós kereteket. Mindezekről nemcsak az Ötv. szabályozása, hanem az ágazati törvények és a kapcsolódó finanszírozási rendszer összhangját is biztosítani szükséges.

A kormányzati politika mai megnyilvánulásai, eseti döntései és megfogalmazott céljai ettől eltérő tendenciát mutatnak.

[1] ld. bővebben: Waldemar Hummer – Sebastian Bohr: A régiók szerepe a jövő Európájában Szubszidiaritás-föderalizmus-regionalizmus, Pécs, 1994, pp. 9-56.

Az állami közfeladatok értelemszerűen állami (központi) felelősséget jelentenek akkor is, ha azokat az állam átadja a helyi önkormányzatoknak. Ezért érzékelhetően mind erősebb az a nézet, amely ezt a felelősséget szinkronba kívánja hozni a feladatellátás szintjével és képességével.

Mind erőteljesebb az a koncepció, amely felül kívánja vizsgálni az állami és a helyi önkormányzati feladat- és hatáskörmegosztást és számos alapvető szolgáltatási területet visszaterelne az állami szférába. Ennek leggyakoribb érvei: a helyi önkormányzatok szakmai és anyagi hátterének gyengeségei, valamint az ország egész területén kívánatos egységes ellátási színvonal biztosítása.

Az önkormányzati megközelítés elfogadja az egész szabályozási rendszer felülvizsgálatának indokoltságát (ideértve a feladat- és hatásköröket is) az alábbi szemlélet érvényesítésével:

- az átalakításnál továbbiakban is a településnek kell az önkormányzati rendszer középpontjában állnia;
- vizsgálni kell, hogy a települések mennyiben képesek megfelelni a rájuk bízott feladatoknak;
- elő kell segíteni a községek (kisközségek) társulását az ésszerű munkamegosztás alapján, kivételesen a kötelező társulás intézményét is alkalmazni kell (erre utal az új Alaptörvény szabályozási elve is);
- meg kell határozni az önkormányzati „minimum" feladat- és hatásköröket és ehhez kiegészítésül meghatározható a különböző típusú (jogállású) települések un. többlet jogköre;
- tisztázandó az is, hogy a feladat ellátása települési vagy területi önkormányzathoz kerüljön;
- egyes mai állami közfeladat, igazgatási szerepkör önkormányzati szférába történő átadása is a felülvizsgálat tárgyköre lehet.
- A helyi önkormányzatok feladat- és hatásköre tekintetében a két évtized működési tapasztalatai tekintetében nemcsak azt érdemes vizsgálni, hogy milyen elvárást fogalmazott meg az Ötv. a helyi önkormányzatokkal szemben, hanem a társadalmi szükségletek kielégítésének lehetőségére is tekintettel kell lenni. Az e téren tapasztalható elmaradás, a lakossági és az önkormányzati teljesítés közötti konfliktus már önmagában is indokolttá teszi a helyi önkormányzati feladat- és hatásköri szabályozás általános felülvizsgálatát, az állami és a helyi önkormányzati teendők pontos szétválasztását és ezt követő szükségszerű koordináció kereteinek újragondolását. Egyértelműbbé kell tenni, hogy az egyes közösségi célok, közügyek megvalósításáért mit kell tennie az államnak és az önkormányzatoknak, illetve milyen eszközök állnak rendelkezésre az egyes felelősségi szinteken.

Nem elhanyagolható a felülvizsgálat során, hogy az un. külső tényezők, nevezetesen az európai uniós tagságunkból, illetve a Kartából milyen kötelezettségek következnek. Az uniós elvárások, irányelvek gazdag tartalmából figyelemre méltó a Program, amely nagy figyelmet szentel a jó kormányzásnak és ezzel összefüggésben a helyi közérdeket megtestesítő önkormányzatoknak. Másik megkerülhetetlen támpont a Karta tartalma, amelynek érvényesítését a magyar állam vállalta (ld. az Ötv. preambuluma, illetve a törvény általános indokolása).

A kilátásba helyezett önkormányzati reform legmarkánsabb része várhatóan az Ötv., feladatokat és hatásköröket elrendező sarkalatos elemei körül kristályosodik ki, de érinteni

fogja, az un. hatásköri törvényt is.[2] A feladatok és hatáskörök szabályozásának mai rendszerén akkor érdemes (egyben szükségszerű) változtatni, ha a helyi önkormányzatokra vonatkozó törvényi szabályozás több törvényben testesülne meg, azaz külön törvény lenne a fővárosra, a megyékre és településekre (mint az 1870-es években) vonatkozóan.

A szintenkénti szabályozás nagyobb lehetőséget adna a feladatok és hatáskörök tételesebb kimunkálására, de a mai alap intézmények köre (a feladat- és hatáskörök egymásmellettisége, azok megállapításának törvényi szintje, a hatáskör-telepítés elvei és az azt befolyásoló körülmények; a kötelező és szabadon vállalható feladat- és hatáskörök; a hatáskör gyakorlása és átruházása, az átruházási tilalmak) lényegesen nem alakulna át.

Az önkormányzati feladatellátás egyik alapvető feltétele az önkormányzati gazdálkodás klasszikus európai mintáihoz igazítása. Az elmúlt két évtized alatt e területen történt a legkisebb előrelépés. Nem alakult ki az alapvető pénzügyi, gazdasági biztosítékok és feltételek a jelen és jövő önkormányzati feladatainak ellátásához; az állami források gyakori változása (kormányzatonként) kiszámíthatatlanná és tervezhetetlenné teszi az önkormányzatok gazdálkodását, különösen a helyi stratégiák kialakítását.

Olyan szabályozó rendszer kialakítása állana a helyi önkormányzatok érdekében, amelyben a feladatellátás és annak forrásrendszere között egyértelmű összefüggés van.

A kötelező feladatok tekintetében az állami források egy időben és arányosan jelennek meg az önkormányzatok költségvetésében.

Az állami normatív támogatás több évre előre történő megállapítása és az önkormányzati bevételek tervezése adhat alapot az önkormányzati gazdálkodási stratégia kialakításához, úgy az intézmények működtetése, mint a település- és területfejlesztés tekintetében. Számolni kell azzal is, hogy az önkormányzatok saját bevételei – a központi adópolitikára figyelemmel – nem növelhetőek jelentős mértékben, a lakosság teherbíró képessége tovább nem terhelhető (belátható időtávon), az önkormányzati vagyon és vállalkozási lehetőségek differenciáltan és korlátozottan állnak rendelkezésre, az önkormányzatok hitelképessége jelentősen lecsökkent, sőt az adósságállományuk veszélyesen megemelkedett.

A kormányzati gazdaságpolitika a közelmúltban jelezte, hogy a központi és a helyi adók vonatkozásában jelentős változtatásokat tervez (pl.: iparűzési és idegenforgalmi adó elvonása). Az önkormányzatok abban érdekeltek, hogy a központi és a helyi adópolitika egymásra tekintettel, azokkal összhangban legyen átalakítva. A helyi közfeladatok ellátásának pénzügyi forrásai továbbra is kétirányúak: önkormányzati saját bevétel és a központi állami támogatás csatornái; az előbbi az önkormányzati elhatározású feladatok pénzügyi fedezetét, az utóbbi az állami felelősségű feladatellátás pénzügyi forrását jelenti. Nem új keletű az önkormányzati igény, amennyiben az állam, mint megrendelő többet és jobb minőséget vár el, akkor ennek ellentételezését is garantálnia kell.

A helyi önkormányzatok igazgatási szervei a magyar közigazgatás alapvető pilléreként definiálhatóak, az állami közigazgatással együtt képesek eredményes, a kormányzás és a helyi lakosság által igényelt igazgatási szerepüket ellátni.[3]

A FELADATTELEPÍTÉS IRÁNYAI

Jelen helyzetben két reformirány látható, az egyik: az állami igazgatási feladatok állami szervekhez telepítése az önkormányzati igazgatás köréből, ami lehet hatósági igazgatás és intézményi ellátási közszolgáltatás; a másik az önkormányzati igazgatás körének stabilizálása, de egyes szinteken és szakterületeken szervezeti, hatásköri változtatásokkal.

[2] 1991.évi XX. tv. a helyi önkormányzatok és szerveik,a köztársasági megbízottak,valamint egyes centrális alárendeltségű szervek feladat-és hatásköréről

[3] Legtöbb forrásmunka ezt a sikeres kormányzás egyik előfeltételének tekinti.

Az első esetben az állami dekoncentrált szervek köre és az általuk ellátott feladatok mennyisége tovább növekszik, az államigazgatás mindinkább meghatározó lesz. A kormányzati felelősség közvetlenné válik olyan feladatokért is, ami jelenleg az önkormányzatokat terheli. Ugyanakkor az önkormányzati igazgatás szerepköre szűkül, a közszolgáltatást nyújtó intézmények átkerülésével a lakossági ellátást kevésbé tudják befolyásolni. Ennek egyenes következménye, hogy a helyi politika tartalma sem maradhat változatlan (pl.: oktatáspolitika, egészségügyi ellátás stb.), de az igazgatási szervezeti struktúra is átalakításra kerül, a személyi állomány jelentősen csökken.

Az igazgatási feladatellátás nemcsak az állami és önkormányzati szervezeti rendszer közötti átcsoportosítással módosulhat, hanem azzal is, hogy új színtere is képződhet az igazgatási (főleg hatósági) feladatoknak.

Egyre nyilvánvalóbb, hogy a települési önkormányzatok egy része, azaz a kisközségek, az önkormányzáshoz való joguk megtartása mellett az igazgatási szervezetükről kénytelenek lesznek lemondani. A törvény által előírt kényszertársulás lényegében a mai társulási lehetőség ismert szervezeti formáit realizálhatja a racionalitás elvére és a gazdaságosságra tekintettel.

Az utóbbi időben ez a megoldás több szakmai és érdekképviseleti fórumon, állásfoglalásban felmerült, érzékelhetően a közbeszéd tárgykörévé vált; végső soron nagy meglepetést és működési zavarokat az átalakítás nem okozna.

Nem mondható el ugyanez az újabban felmerült közpolitikai javaslatok egyikére, azaz az új közigazgatási területi egységekként kialakítandó járásokról és az itt összpontosuló igazgatási feladatokat ellátó hivatali szervezetre, akkor sem, ha csak az állami igazgatási-hatósági ügyekről van szó. Ez alapvetően átalakítaná a mai társulási formákat (egy részük célját vesztené), másrészt jelentősen lecsökkenne a községi szinten ellátandó ügyköröket, ami megkérdőjelezné a községi önkormányzati igazgatási szervezet szükségességét.

A helyi szinten megmaradó önkormányzati vonatkozású igazgatási feladatkörök és a testületi tevékenységgel összefüggő teendők egészen más jellegű (méretű, szerkezetű, létszámú és felkészültségű) hivatali szervezetet igényelnének, melynek már kevés kapcsolatai lennének az állam szerveivel.

Ezek a feladatváltozások természetesen kihatnának a helyi önkormányzati szervezetekre is, csak az arányok és a hatások lehetnek más értékűek. Viszonylag kevesebb következményekkel lehet számolni a városi és főleg a nagyvárosi szinteken, mert itt az önkormányzati jellegű igazgatás és intézményhálózat kevesebb veszteségeket szenvedne el, akkor is, ha az állami feladatok (pl.: építésügy stb.) és az állami felelősségi körű közösségi szolgáltatási feladatok (intézmények) állami ellátási felelősségi körbe kerülnek.

Kétségessé válhat viszont a megyei igazgatási szint helyzete, ha az egészségügyi és közoktatási feladatok átkerülnek az állami szférába, illetve, ha egyes területi fejlesztési vagy koordinációs szerepkörök kormányzati szervhez kerülnek (pl.: árvízvédelem, természetvédelem, stb.).

Mindezekre tekintettel az önkormányzatiság alapjainak újbóli meghatározása nemcsak társadalompolitikai, alkotmányossági következményekkel jár, hanem jelentős kihatásai lesznek az igazgatási szervezetekre is.

A HELYI ÖNKORMÁNYZATOK TESTÜLETEI ÉS MŰKÖDÉSÜK

Az önkormányzati testületek működési alapnormáinak kialakítása nagymértékben függ a vonatkozó alaptörvényi rendelkezésektől és törvényi szabályozástól. A jelenlegi ismereteink viszonylag kevés támpontot adnak a várható változások megítélésére.

Meghatározó lesz, hogy mely területi szinteken lesz önkormányzati testület (pl.: járás), hogyan alakul a választási rendszer (pl.: főváros), a testületek létszámát mi határozza meg

(keretszám, helyi elhatározás, lakosságszám, települési funkció stb.). A működés másik determinánsa a helyi önkormányzati feladatok típusa, mennyisége.

E két alapvető feltételhez alakíthatók a szervezeti feltételek (pl.: létszám) és a testületen belüli szint (pl.: nagyobb létszámú lakosság által választott testület és az ebből kialakítandó kis létszámú elöljáróság).

A működési szabályozás tehát értelemszerűen következmény, amelyet a törvény – a jelenlegi elvhez hasonlóan – csak bizonyos garanciák tekintetében fog meghatározni. Továbbra is nagy szerepe lesz a testület által elfogadott szervezeti és működési szabályoknak, különös tekintettel az önkormányzati Kartában vállalt követelményekre.

A működés törvényességét kormányzati és bírósági eszközrendszerrel továbbra is vizsgálni kell, a jogvédelem komplex rendszerét kell fenntartani.

A testületi működéssel összefüggésben kialakult és bizonyos értelemben közmegegyezést kiváltó tapasztalatok sokirányúak. Ezek részletei azonban csak annyiban tekinthetők relevánsnak, amennyiben a mai normák megmaradnak. Az új, átrendezett szervezeti struktúrák, változó feladat- és hatáskörök esetében ezeket a tapasztalatokat kevésbé lehet irányadónak tekinteni.

A HELYI ÖNKORMÁNYZATOK ÉS KORMÁNYZATI SZERVEK KAPCSOLATA

Ez a témakör is szoros összefüggésben van az elfogadott új alaptörvénnyel, illetve az ott szabályozásra kerülő alaprendelkezésekkel. A láthatóan szűk körű szabályozás nagyobb mozgásteret kíván adni a vonatkozó sarkalatos törvénynek (törvényeknek?). Így azokra hárul az önkormányzatiság két évtizedes tapasztalatainak felhasználása, illetve a Karta tartalmának érvényesítése.

Néhány ponton már ma is érzékelhető, hogy van kormányzati szándék bizonyos kérdések újszerű megközelítésére, erre csak néhány témát említek:

- a helyi önkormányzatok feletti törvényességi ellenőrzést hatásosabb eszközzel is fel lehetne váltani, azaz a felügyelet eszköze beépíthető lenne (a Karta erre lehetőséget ad);
- a helyi önkormányzatok feletti törvényességi felügyelet eszközrendszere konkrét jogosítványai az általános közérdek, a társadalmi-kormányzati célokhoz is formálhatóak, a helyi és a központi érdekkonfliktusok kezeléséhez racionálisabb kereteket adhatnak;
- a szervezeti és működési normák tekintetében szintenként eltérő törvényi szabályozás lehetősége indokolttá válhat /egy törvényben szintenkénti bontásban, vagy külön-külön törvényekben (pl.: községi törvényben)/, de vonatkozik ez a feladat-hatáskör meghatározására is;
- átrendezésre kerülhet az alkotmánybírósági és a bírósági jogosítványok köre is, különösen, ha a közigazgatási bíróság létrejön (pl.: a helyi rendeletek bírósági felülvizsgálata);
- az önkormányzati gazdálkodás, pénzügyi területen hatékonyabb ellenőrzési megoldások kialakítása az önkormányzaton belüli és külső ellenőrzés tekintetében, az Állami Számvevőszék erősebb jogkörének meghatározása.

A helyi önkormányzatiság eszmerendszere az ország politikai és igazgatási alapnormái között fejlődhet tovább, építve azokra a tapasztalatokra, amelyeket az európai államok gyakorlata az évszázadok során szerzett.

Nemcsak a jó kormányzás, hanem a jó helyi önkormányzás előfeltételének is tekinthető egy életképes és erős polgári társadalom. Ezért a helyi önkormányzatoknak is meg kell

találniuk a polgári társadalom intézményeivel való együttműködés eszközeit, amelyek befolyásolják és alakítják a helyi közéletet, egyben megfogalmazzák a közösségi igényeket.

A polgári társadalom és a helyi önkormányzatok nélkülözhetetlen elemei a demokrácia működésének, erősítik a demokrácia pluralista dimenzióit.

A helyi önkormányzatok közéleti szerepcsökkenése a fenti gondolattal ellentétes folyamatokat indítana el, ártana az országos (általános) és helyi közérdek eredményes képviseletének és megvalósulásának. Ezért az önkormányzati reform csak széleskörű társadalmi támogatással, több dimenzióban megvalósuló érdekegyeztetés mellett lehet a közjót szolgáló, eredményes kormányzati stratégia.

Az Alaptörvény megalkotását követően, azzal összhangban feltétlenül át kell gondolni az Ötv szabályait, de elkerülhetetlen az önkormányzás szervezeti és működési kérdéseivel szorosabb kapcsolatot mutató más (elsősorban a helyi képviselők és polgármesterek megválasztásáról szóló és az un. polgármesteri külön stb.) törvények áttekintése is.

Alapkérdésnek tekintjük tehát azt, hogy egyértelműen tisztázni kell az önkormányzat, az önkormányzás alanyát (alanyait), tárgyát és tartalmát, valamint a helyi közügyek fogalmának – időnként homályos és mobil – körét. Továbbá sokkal átgondoltabban és differenciáltabban kell megközelíteni az egyes önkormányzati típusok szervezetét és működését érintő szabályokat is. A községek esetében (az 5 ezer főnél kevesebb lakosú településeket értve) – külön, önálló községi törvényben foglalt – a valóságos, a hazai községi viszonyokhoz (felfogáshoz) jobban igazodó – szabályok kimunkálása napjainkban egyre sürgetőbb feladatnak tűnik. Azonban az elmúlt évtizedek tanulságai okán, ma már az is felvetődik, hogy a helyi önállóság kiteljesedése még nem vonja maga után az önkormányzat szinte automatikus kiépülését (ahol – de jure – van község, ott lakosságszámra tekintett nélkül – de facto – működik önkormányzat).

ÖSSZEFOGLALVA

A szükségszerű központosítás mellett a szervezeti és működési kérdések kialakításában a jövőben sokkal szélesebb mozgásteret kell biztosítani a helyi jogalkotó számára, mert e nélkül – a jelenlegi törvényi szabályozás minőségét tekintve – esély sincs a jogszerű és nem utolsósorban a helyi érdekeket is maradéktalanul szolgáló autonóm helyi szabályok kialakítására.

Felhasznált irodalom

[1] Kaltenbach Jenő (1996): Közigazgatás és/vagy önkormányzat, in. : A magyar közigazgatás korszerűsítésének elvi és gyakorlati kérdései, szerk.: Fogarasi József, Unió Kiadó, Oktatási anyag, Budapest, pp. 63-68

[2] Kiss László (1996): Társulások-kényszertársulások – szervezeti konzekvenciák, In. : A magyar közigazgatás korszerűsítésének elvi és gyakorlati kérdései, szerk.: Fogarasi József, UNIÓ Kiadó, Oktatási anyag, Budapest, pp. 199-201

[3] Szente Zoltán (1994):A helyi területi önkormányzatok alkotmányos szabályozásának elvei de lege ferenda, Magyar Közigazgatás,44.évf. 6-7. sz. pp. 364-387. HU ISSN 0865-736 X

[4] Waldemar Hummer – Sebastian Bohr: A régiók szerepe a jövő Európájában, Szubszidiaritás-föderalizmus - regionalizmus, Pécs, 1994, pp. 9-56

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Fleiner Rita
fleiner.rita@nik.uni-obuda.hu

Munk Sándor
munk.sandor@zmne.hu

INFORMATIKAI BIZTONSÁGI ÚTMUTATÓK, KONTROLLOK ÉS SZEREPÜK AZ ADATBÁZIS-BIZTONSÁG MEGVALÓSÍTÁSÁBAN

Absztrakt

Az információk és az azokat kezelő informatikai rendszerek, eszközök a szervezetek fontos erőforrásai, biztonságuk valamennyi szervezet számára alapvető fontosságú. Ennek megfelelően jelentősen megnőtt az informatikai biztonság megvalósítására irányuló tevékenységek, eszközök szerepe is. Ez utóbbiak közé tartoznak a biztonsági útmutatók és kontrollok, amelyek a biztonság megvalósításának, szabályozásának és értékelésének fontos eszközei. Jelen publikáció bemutatja a biztonsági útmutatók fogalmát, rendeltetését, típusait; bemutatja a biztonsági kontrollok fogalmát, értelmezését, elemzi csoportosításuk lehetőségeit; végül elemzi az informatikai biztonsági útmutatók, kontrollok helyét, szerepét az informatikai biztonság irányításában, szabályozásában.

Information and the supporting IT systems, devices are important organizational assets, their security is fundamental for all organizations. As a consequence the role of security activities and means has significantly increased. Security guidelines and controls are important means of implementation, regulation, and evaluation of security. Recent publication presents the concept, purpose, and types of security guidelines; presents the concept, and interpretation of security controls, analyses their classifications; finally analyses the role of security guidelines, controls in management and regulation of information (IT) security.

***Kulcsszavak**: informatikai biztonság, adatbázis-biztonság, informatikai biztonsági útmutató, informatikai biztonsági kontroll ~ information (IT) security, database security, information security guideline, information security control*

BEVEZETÉS

Az információk és az azokat kezelő folyamatok, rendszerek, eszközök napjainkra megkérdőjelezhetetlenül valamennyi szervezet-típus alapvető szervezeti erőforrásává váltak. Ma már közhely, hogy az információk és a kezelésükben szerepet játszó erőforrások biztonsága szinte egyaránt fontos a gazdálkodó szervezetek, a kormányzati szféra, a védelmi szféra és gyakorlatilag minden szervezet számára. Ennek megfelelően jelentősen megnőtt az informatikai biztonság megteremtésére és fenntartására irányuló tevékenységek és az ezek során felhasznált eszközök, módszerek és eljárások szerepe, jelentősége is.

Az információk és az informatikai rendszerek, eszközök biztonságát sebezhetőségeiken keresztül számos fenyegetés veszélyezteti. A fenyegetések ellen különböző módokon és eszközökkel lehet védekezni, azonban tökéletes védelem elvileg nem létezik és nem minden védelmi megoldás "éri meg" a ráfordítást. Az egyes fenyegetések bekövetkezésük valószínűsége és várható következményeik alapján eltérő kockázatokat jelentenek a védendő objektumok biztonságára. A kockázatok azonosítása, elemzése és értékelése alapján lehet kiválasztani a megfelelő védelmi rendszabályokat, intézkedéseket (biztonsági kontrollokat).

Az informatikai és ezen belül az adatbázis-biztonság megkívánt állapota tehát megfelelő biztonsági kontrollok (folyamatok, eljárások, szervezeti megoldások, szoftver és hardver funkciók) segítségével érhető el és tartható fent. Ezeket a kontrollokat meg kell határozni, meg kell valósítani, folyamatosan figyelemmel kísérni és szükség esetén továbbfejleszteni, hogy a kitűzött biztonsági és ennek következtében szervezeti célkitűzések megvalósuljanak. Egy adott szervezet számára az alkalmazandó biztonsági kontrollok meghatározását, kiválasztását elméleti vizsgálatok és bevált gyakorlati tapasztalatok alapján nemzetközi és nemzeti szakmai szervezetek, informatikai gyártók által összeállított kontroll-gyűjtemények, biztonsági útmutatók segítik.

A biztonsági útmutatók – bár sok közülük nemzetközi, nemzeti és szervezeti szintű szabványokban is megjelenik – nevükből következően[1], alapvetően nem kötelező erejű dokumentumok. Ennek ellenére felhasználhatóak az informatikai biztonság, vagy valamely részterülete szabályozására is, meghatározva például, hogy bizonyos szervezetek, tevékenységek, rendszerek, rendszerelemek esetében az adott útmutató mely kontrolljait kell kötelezően megvalósítani. Ez általában nem egyedileg kerül meghatározásra, hanem a biztonság alanyai egyéb szempontok alapján biztonsági kategóriákba (osztályokba) kerülnek besorolásra és a minimálisan megvalósítandó kontrollok ezekhez a kategóriákhoz vannak rendelve. Végül a segítségnyújtás és a szabályozás mellett az útmutatók, illetve az azokban foglalt kontrollok kiterjedten felhasználásra kerülnek a biztonsági megfelelőség-vizsgálatok, igazolások, auditok során is.

A fentiek alapján jelen publikáció alapvető célja, hogy rendszerezze, bemutassa az informatikai biztonsági útmutatók, kontrollok alapvető információit és meghatározza szerepüket az informatikai biztonság megvalósításában. Ennek érdekében:

- - bemutatja a biztonsági útmutatók fogalmát, rendeltetését, típusait, valamint a főbb útmutatókat;
- - bemutatja a biztonsági kontrollok fogalmát, értelmezését, elemzi csoportosításuk lehetőségeit, helyüket és szerepüket az informatikai biztonság megvalósításában;
- - elemzi az informatikai biztonsági útmutatók, kontrollok helyét, szerepét az informatikai biztonság irányításában, szabályozásában, meghatározza a kapcsolódó feladatokat.

[1] Guideline = iránymutatás, irányelv.

BIZTONSÁGI ÚTMUTATÓK ALAPJAI

Az informatikai biztonsági útmutatók és a kapcsolódó dokumentumok (ellenőrző listák) az informatikai biztonság kialakítását és fenntartását (az informatikai biztonsági célkitűzések megvalósulását) szolgáló védelmi megoldások, rendszabályok és tevékenységek kialakításának, illetve ellenőrzésének alapvető eszközei. A következőkben a biztonsági útmutatókkal kapcsolatos alapvető kérdéseket összegezzük és rendszerezzük, ezen belül:

- bemutatjuk a biztonsági útmutatók és ellenőrző listák fogalmát, rendeltetését;
- rendszerezzük az útmutatók, ellenőrző listák felhasználásának lehetőségeit;
- megvizsgáljuk az útmutatók csoportosításának lehetőségeit, főbb típusaikat;
- ismertetjük a jelentősebb informatikai biztonsági útmutatókat;
- végül ismertetjük a jelentősebb adatbázis-biztonsági útmutatókat.

Az első három kérdésben a megállapításokat általános biztonsági megközelítésben fogalmazzuk meg, de példáinkat az informatikai biztonság területéről vesszük.

A *biztonsági útmutatók és ellenőrző listák* kérdéseinek vizsgálatához először meg kell határoznunk fogalmukat, rendeltetésüket. Az *útmutató* (guide, guideline[s]) az általános értelmezés szerint egy nem kötelező érvényű ajánlás arra, hogy meghatározott célkitűzések elérése érdekében mit és hogyan kell megtenni. [1, 2] Más megfogalmazásban az útmutató egy adott cél eléréséhez megkívánt, javasolt, jónak tartott, bevált eljárások, tevékenységek leírása. Az útmutatók általában a törvényekben, szabványokban, szabályozókban előírtak megvalósításának javasolt, célszerű módját tartalmazzák.

Útmutatók az élet sok területén felhasználásra kerülnek: felhasználói útmutatók (kézikönyvek) ismertetik, magyarázzák készülékek használatát; technikai útmutatók segítik rendszerek, eszközök telepítését, üzemeltetését, karbantartását, javítását; orvosi szakmai protokollok írják le egy betegség, vagy állapot kezelésének tevékenységeit.[2] Több szabványügyi szervezet (pld. ISO, IEC, ITU, NIST[3], stb.) bocsát ki dokumentumokat 'útmutató' megnevezéssel. Míg a szabványok megismételhető, mérhető és tesztelhető, normatív technikai referenciaként használható specifikációk, addig az útmutatók általában szabadabb értelmezéseket is lehetővé tévő iránymutatások.

A *biztonsági útmutatók* (security guideline) az útmutatók egyik csoportját alkotják, amelyek rendeltetése biztonsági célkitűzések megvalósítását szolgáló megoldások, eljárások, tevékenységek meghatározása: "hogyan lehet elérni a biztonságot". A biztonság alatt a továbbiakban olyan állapotot értünk, amelyben valaki/valami a lehetséges fenyegető hatások ellen a megkívánt mértékben védett. A biztonság kialakításához és fenntartásához meg kell határozni a biztonsági célkitűzéseket, azonosítani és értékelni kell a biztonságot veszélyeztető kockázatokat, majd ezek alapján meg kell határozni és valósítani a védelmi intézkedéseket.

Szervezetek esetében a biztonsági szabályozórendszer három szintre osztható (az informatikai biztonság esetében pld. lásd a KIB 25/1. ajánlást [3, 46. o.]). Felső szinten a biztonsági politika és stratégia található, amelyek megfogalmazzák az alapvető biztonsági elveket, célkitűzéseket és felelősségi köröket, illetve meghatározzák a biztonság fejlesztésének közép (hosszú) távú tervét. Középső szinten átfogó és részterületi szabályzatok, szabályozók, míg alsó szinten a konkrét feladat- és szerepkörökre vonatkozó részletes biztonsági eljárások, feladatok (eljárásrend) találhatóak.

---

[2] User's guide (manual), technical guide (manual), medical guide (protocol).

[3] International Organization for Standardization, International Electrotechnical Commission, International Telecommunication Union, National Institute of Standards and Technology [USA].

A biztonsági útmutatók a szervezetekben a középszintű szabályozóknak és az alsó szintű biztonsági feladatoknak az átfogó biztonsági politika és biztonsági célkitűzések alapján történő kialakítását támogatják, segítik. Ennek megfelelően a biztonsági útmutatók általában több szervezet számára felhasználható módon, azokon kívül kerülnek kidolgozásra. Emellett összetett szervezetrendszerekben (közigazgatás, haderő, stb.) is szükség lehet biztonsági útmutatók kidolgozására az egyes szervezetek biztonsági eljárásai, feladatai meghatározásának támogatásához.

Az *ellenőrző lista* (checklist) általános értelemben egy összetett feladat elemi tevékenységeinek, lépéseinek teljes körét tartalmazó lista, amelynek rendeltetése emlékeztetés, végigvezetés a végrehajtandó részfeladatokon. Az egyes lépések között lehetnek függőségek, egy lépés választásától, vagy eredményétől függhet, hogy egy másikat (másikakat) végre kell-e hajtani. Egy ellenőrző lista sok esetben ténylegesen egy fennálló állapot értékelésének, ellenőrzésének lépéseit tartalmazza.

A *biztonsági ellenőrző listák* (security checklist) a biztonsági útmutatókban foglalt konkrét megoldások, tevékenységek megvalósulásának – más megközelítésben az útmutatóban foglaltaknak történő megfelelés – ellenőrzésére szolgáló dokumentumok. Az informatikai biztonsági területen jelentős szerepet játszanak a biztonsági konfigurációs ellenőrző listák (security configuration checklist), amelyek adott informatikai termékek javasolt, biztonságos beállításait, valamint az alkalmazott adminisztrációs megoldásokat, eljárásokat ellenőrzik. [4, 2-1. o.] Az ellenőrző listák a megfelelőség-vizsgálat mellett természetesen felhasználhatóak a beállítások végrehajtása során is és a hagyományos dokumentum-formátum mellett megvalósíthatóak automatizált ellenőrzést lehetővé tévő elektronikus (pld. szkript) formában is.

A *biztonsági útmutatók, ellenőrző listák felhasználásának lehetőségei* három nagy területbe sorolhatóak. Ezek közé tartozik felhasználásuk:

- biztonsági intézkedések kiválasztása, kialakítása során;
- biztonsági szabályozások hivatkozási alapjaként;
- és biztonsági követelményeknek történő megfelelés ellenőrzése során.

A *biztonsági intézkedések kiválasztása, kialakítása során történő felhasználás* tekinthető az alapvető felhasználási módnak. Ebből a szempontból a biztonsági útmutatók elméletileg megalapozott és a bevált gyakorlatra épülő általános célkitűzés- és megoldás-gyűjtemények. Az útmutatók alapvető összetevőit a védelmi megoldások, intézkedések (biztonsági kontrollok, amelyekkel részletesebben a következő pontban foglalkozunk) képezik. Az egyes összetevők esetében a meghatározás mellett szerepelhet a megvalósítás javasolt módja is.

Az útmutatókban a rendszerezettség és a könnyebb kezelhetőség érdekében az egyes összetevők (kontrollok) jellemzően különböző szempontok alapján – esetleg több szinten is – csoportokba vannak sorolva. Az egyes csoportok esetében megfogalmazásra kerül a bennük foglalt összetevők általános célja, illetve e biztonsági célkitűzés részletesebb indoklása, elvei.

A *szabályozás során történő felhasználás* az önálló döntés alapján történő felhasználással szemben a külső előírásokhoz kapcsolódik. Ennek során egy szabályozás hatálya alá tartozó szervezetek számára meghatározásra kerül, hogy mely védelmi megoldásokat, intézkedéseket kell kötelező érvénnyel, vagy bizonyos feltételek fennállásának függvényében megvalósítaniuk. A szabályozás történhet nemzeti, vagy szervezeti szinten (utóbbi esetben olyan összetett szervezetrendszerek esetében, ahol az egyes szervezetek önálló biztonsági irányítási rendszert működtetnek), de lehetséges uniós, vagy szövetségi keretek között is. A felhasználásnak ez a módja tulajdonképpen egy többszintű biztonsági irányítási rendszert jelent, amelyben a magasabb szint célkitűzéseket és ezek megvalósítására egy minimum védelmi intézkedési "csomagot" határoz meg, amelyet az alacsonyabb szint saját hatáskörében bővíthet, finomíthat.

Az *ellenőrzés céljára történő felhasználás* a biztonság irányításának másik alapvető részterületéhez, egy szervezeten belül a biztonság állapotának ellenőrzéséhez, felülvizsgálatához, illetve a meghatározott követelményeknek történő megfelelés értékeléséhez kapcsolódik. Az ellenőrzés, értékelés lehet szervezeten belüli és azon kívüli (magasabb szintű irányító, vagy független minősítő szervezet részéről). A biztonsági útmutatókban foglaltak az ellenőrzés, értékelés során etalonként használhatóak fel annak megítéléséhez, hogy a meghatározott biztonsági célkitűzésekhez és kockázatokhoz megfelelőek-e a megvalósított védelmi intézkedések és megfelelő módon kerültek-e megvalósításra. A korábban említett konfigurációs ellenőrző listák alapvető rendeltetése (már nevük alapján is) a biztonság állapotának ellenőrzése.

A *biztonsági útmutatók, ellenőrző listák osztályozása* különböző szempontok szerint lehetséges. Ezek közül a következőkben röviden kettőt mutatunk be:

- az alkalmazási terület szerinti osztályozás;
- és a kidolgozók szerinti osztályozás.

A *biztonsági útmutatók, ellenőrző listák alkalmazási terület szerint* egy terület egészére, vagy egyes részterületeire vonatkozó típusokra osztályozhatóak. Ehhez az osztályozáshoz természetesen meg kell határozni az alapul vett szakterületet, ami lehet például informatikai biztonság, termékbiztonság, munkabiztonság, stb. Szűkebb vizsgálati témánk szempontjából a továbbiakban alapterületnek az átfogó informatikai biztonságot tekintjük.

Az informatikai biztonság részterületei többféleképpen kijelölhetőek és ennek megfelelően többféle részterületi útmutatóval is találkozhatunk. Ilyenek például a következőek:

- az informatikai rendszerek főbb összetevői szerint: alkalmazás-, operációs rendszer, adatbázis-, hálózat- és hardverbiztonsági útmutatók;
- a biztonság összetevői szerint: fizikai, személyi és dokumentum biztonsági útmutatók;
- a védelmi megoldások szerint: fejlesztés-, hozzáférés-, jelszó-, vagy kriptográfiai biztonsági útmutatók;
- valamint az informatikai biztonság adott alkalmazási területre kidolgozott – az átfogó biztonsági útmutatókat specializáló, kiegészítő – útmutatók[4] is.

A *biztonsági útmutatók, ellenőrző listák kidolgozók szerint* több csoportra oszthatóak, ami egyben rendeltetésüket, célközönségüket is meghatározza. Az első csoportot a nemzetközi szabványosítási és szakmai szervezetek által kidolgozott dokumentumok képezik. Ezek a legátfogóbb módon összegzik a biztonság kialakításához és fenntartásához szükséges, jónak tartott megoldásokat és az adott szervezetben kialakított rendnek megfelelően időszakonként újra kiadásra, átdolgozásra kerülnek. Ma már tulajdonképpen ezek képezik minden biztonsági útmutató alapját. A második csoportba a nemzeti szintű dokumentumok (köztük szabványok) tartoznak, amelyek egy adott – nagyobb, fejlettebb – ország biztonsági célkitűzései, szabályozásai megvalósítását támogatják. A harmadik csoportba az informatikai ipar szervezetei, a gyártók által kibocsátott dokumentumok sorolhatóak, amelyek egy-egy termék (esetleg termékcsoport) biztonságos alkalmazásához kapcsolódóan nyújtanak útmutatást. Végül a negyedik csoportot a szervezeti szintű dokumentumok alkotják, amelyek általában összetettebb szervezetrendszerekben, az összetevő szervezetek által történő felhasználásra kerülnek kidolgozásra.

A *legfontosabb informatikai biztonsági útmutatók* közé az ISO/IEC 27000 szabványsorozat egyik eleme, az Informatikai Biztonsági Fórum biztonsági ajánlásgyűjteménye és az Egyesült

[4] Az ISO 27000 szabványcsaládban például külön csoportot képeznek az úgynevezett alkalmazási terület-specifikus útmutatók (jelenleg az egészségügyi ISO 27799 és a távközlési ISO 27011). [1, 12. o.]

Államok Nemzeti Szabványügyi és Technológiai Intézete 800-as kiadványsorozatának egyes összetevői tartoznak.

Az ISO/IEC 27000 szabványsorozat az informatikai biztonság menedzsmentjének "legjobb gyakorlatait" fogja össze, melyet a Nemzetközi Szabványügyi Szervezet (ISO) és a Nemzetközi Elektrotechnikai Bizottság (IEC) közösen adott ki. A szabványcsalád egyik eleme az *ISO/IEC 27002:2005 Az informatikai biztonság irányítási gyakorlatának kézikönyve*[5] [2], amely a szervezet teljes körű informatikai biztonságának megteremtéséhez nyújt útmutatást biztonsági intézkedések, kontrollok felsorolásával.

A szabvány fejezetekből (sections) áll, ezek elején megtaláljuk az aktuális megvalósítandó biztonsági célokat (objectives); a célok megvalósításához szükséges biztonsági intézkedéseket, kontrollokat; a biztonsági kontrollok megvalósítási útmutatóját (implementation guidance) és egyéb szükséges információkat. A biztonsági kontrollok megfogalmazása általános szintű, a gyakorlati megvalósítás részleteit a szervezetnek saját magának kell kidolgoznia.

A szabvány felépítése alapján a védelem megvalósításának területei a következők: kockázatelemzés, szabályzati rendszer, biztonsági szervezet, vagyontárgyak kezelése, személyi biztonság, fizikai és környezeti biztonság, kommunikáció és üzemeltetés biztonsága, hozzáférés-ellenőrzés, informatikai rendszerek beszerzése, fejlesztése és karbantartása, incidenskezelés, üzletmenet-folytonosság, jogszabályi megfelelőség.

A szabványt bármely szervezet felhasználhatja a szervezeten belüli informatikai biztonság kialakításához, menedzseléséhez és javításához. A szabvány biztonsági kontrollok gyűjteményének tekinthető. A szervezetnek először kockázatelemzést kell végeznie, azonosítania kell a számára szükséges biztonsági előírásokat, követelményeket, majd ezek alapján fel kell építenie a saját biztonsági programját. Ezt a szabvány segítségével meg tudja tenni, a szabványban felsorolt biztonsági kontrollok kiválasztása és alkalmazása által.

Az Informatikai Biztonsági Fórum[6] (ISF) nevű nonprofit informatikai biztonsági szervezet kétévente frissíti az ingyenesen elérhető informatikai biztonsági ajánlásgyűjteményét, az *Informatikai biztonság legjobb gyakorlatainak szabványát*[7] [21]. Az ISO/IEC 27002-höz hasonlóan ennek a dokumentumnak is a célja a szervezeten belüli informatikai biztonság megvalósítása és támogatása gyakorlati és mérhető biztonsági intézkedések felsorolásán keresztül. A szabványt kutatások, nemzetközi szervezetek tapasztalatai és más jelentős szabványok alapján állítják össze elsősorban nagy nemzeti és nemzetközi szervezetek számára, de deklarálják, hogy a szabvány tetszőleges méretű szervezet számára alkalmas az informatikai biztonság megteremtéséhez és fenntartásához. Az ISF ajánlásgyűjteménye célul tűzi ki, hogy lefedje más hasonló célú szabványok (például ISO/IEC 27002 és COBIT) kontroll gyűjteményét.

A szabvány 6 fő fejezetre (aspects), alfejezetekre (areas) és szekciókra (sections) oszlik fel. Minden szekció egy speciális informatikai biztonsági területet fed le, tartalmazza az adott biztonsági elvet (principle), annak célját (objective) és a cél eléréséhez szükséges biztonsági intézkedéseket, kontrollokat, gyakorlati lépéseket (statements).

A szabvány a biztonsági intézkedéseket a következő hat csoportba sorolja be: számítógép telepítés, hálózatok, kritikus üzleti alkalmazások, felhasználói környezet, rendszerfejlesztés és biztonságkezelés.

Az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete (NIST) IT laboratóriuma által kiadott *informatikai biztonsági 800-as sorozat*[8] [5] különböző területek kérdéseivel foglalkozó dokumentumokból, útmutatókból áll. Az útmutatók felépítése

[5] Code of practice for Information Security Management.
[6] Information Security Forum.
[7] The Standard of Good Practice for Information Security.
[8] NIST Special Publications 800 Series.

ismertető-leíró jellegű, ebben eltérnek az előzőleg ismertetett két szabványtól, amelyek inkább pontokba szedett, biztonsági kontrollok gyűjteményeként jelennek meg.

Az Egyesült Államok hadseregében az informatikai rendszerek különböző összetevőire vonatkozó informatikai biztonsági ellenőrzési célokat, az alkalmazandó védelmi rendszabályokat, eljárásokat biztonsági beállítási (konfigurációs) útmutatók rögzítik, melyeket a Védelmi Informatikai Rendszerek Ügynöksége (DISA), valamint a Nemzetbiztonsági Ügynökség készít el és bocsát ki.

A DISA által kidolgozott Biztonsági Technikai Megvalósítási Útmutatók (Security Technical Implementation Guide, STIG) segédeszközök a DoD informatikai rendszerek védelme minőségének növeléséhez. Az egyes útmutatók az adott informatikai rendszer összetevő ismert biztonsági komponenseit, sérülékenységeit és a DoD informatikai védelmi politika által tárgyalt, ezekhez kapcsolódó kérdéseket tartalmazzák.

A DISA útmutatókhoz, az azokban foglaltak ellenőrzéséhez rendelkezésre állnak biztonsági ellenőrző listák és a biztonsági készenlétet ellenőrző szkriptek. Mindkettő lényegében azt ellenőrzi, hogy a vizsgált rendszer (rendszer-összetevő) megfelel-e az útmutatóban előírt követelményeknek (ellenőrzési céloknak), vagyis megfelelően van-e telepítve és konfigurálva, illetve megfelelően van-e felügyelve, kezelve. Az útmutatók és az ellenőrző listák bárki által ingyenesen letölthetők a szkriptek viszont belső használatra készültek [6, 7].

Az *adatbázis-biztonsági útmutatók* az adatbázis rendszerek telepítésére, konfigurálására, üzemeltetésére, illetve az adatbázis-kezelő rendszer működésére kiható, az informatikai rendszer egyéb összetevőire (operációs rendszer, hálózat, adatbázist elérő alkalmazások) vonatkozó biztonsági követelményeket és biztonsági kontrollokat tartalmazzák.

Adatbázis-biztonsági útmutatók készítői között megtaláljuk az adatbázis-kezelő rendszerek gyártóit, fejlesztőit, különböző informatikai biztonsághoz kötődő szervezeteket illetve állami szerveket. Példaként említhetjük az Egyesült Államok Védelmi Minisztériumát, az Adatbázis-biztonsági Konzorciumot, az Internet Biztonság Központját, a SANS intézetet[9], illetve az adatbázis-kezelő rendszerek fejlesztőit, például az Oracle-t.

A dokumentumokat két fő csoportra oszthatjuk a bennük található biztonsági kontrollok általános-részletes jellege alapján. Az egyik csoportot az általános adatbázis-biztonsági útmutatók alkotják (például [8, 9]), melyek az adatbázis-kezelő rendszer típusától függetlenül fogalmaznak meg biztonsági követelményeket. A másik csoportot az adatbázis-kezelő rendszer típusához (esetleg még verziójához is) készült útmutatók alkotják, melyek általában adatbázis ellenőrző lista (database checklist) elnevezést viselik (például [10, 11, 12]). Természetesen minél szorosabban kötődik az útmutató egy konkrét termékhez (azaz a gyártó és a verziószám is adott), annál precízebb és konkrétabb ellenőrzési és megvalósítási módszereket, biztonsági kontrollokat tartalmaz. Az általánosabban megfogalmazott útmutatók előnye, hogy szélesebb kör számára hasznosíthatók, azonban alkalmazás esetén a felhasználótól nagyobb szakmai tudást várnak el a követelmények konkrét megvalósításának meghatározása folyamán.

Az adatbázis ellenőrző listák fejezetekre osztva, táblázatos formában tartalmazzák a biztonsági kontrollok listáját. A táblázat egy sora egy biztonsági kontrollt tartalmaz, ami egy konkrét biztonsági követelményt, illetve annak megvalósítási és ellenőrzési módját írja le. A követelmény mellett gyakran találunk annak biztonsági szintjét leíró osztályozást is, ami azt mutatja meg, hogy a követelmény be nem tartása milyen mértékű biztonsági sérülést rejt magában. Bizonyos szervezetek (pl. DoD, CIS) az ellenőrzési lista mellé automatikus eszközöket, szkripteket is kifejlesztettek az ellenőrzések gyorsabb elvégezhetősége

[9] Database Security Consortium, Center for Internet Security; SysAdmin, Audit, Networking, and Security Institute.

érdekében. A listákban találhatunk utalást az ellenőrzési pontoknál arra vonatkozólag, hogy az adott követelmény ellenőrzését az automatikus eszköz elvégi-e.

BIZTONSÁGI KONTROLLOK ALAPJAI

A megfelelő biztonsági kontrollok az informatikai biztonság kialakításának és fenntartásának, a biztonság megkívánt (megkövetelt) szintje értékelésének alapvető eszközei, alapját képezik az informatikai biztonsági irányítás (security management) különböző módszertanainak, keretrendszereinek (pld. COBIT[10], ISO 27000 család). A következőkben a biztonsági kontrollokkal kapcsolatos alapvető kérdéseket összegezzük és rendszerezzük, ezen belül:

- bemutatjuk a biztonsági kontrollok fogalmát, rendeltetését;
- rendszerezzük a kontrollok csoportosításait, főbb típusait;
- elemezzük az informatikai biztonsági kontrollok fogalmát, értelmezését;
- megvizsgáljuk a kontrollok helyét, szerepét az informatikai biztonság megvalósításában;
- végül ismertetjük az adatbázis-biztonsági kontrollok fogalmát, csoportosítási lehetőségeit.

A biztonsági kontrollok fogalmának, rendeltetésének vizsgálatához először a kontroll fogalom tartalmát, értelmezését kell rögzítenünk. A *kontroll* (control) kifejezés angolul egyaránt jelent irányítást, illetve felügyeletet, ellenőrzést, többes számban pedig vezérlő-, irányító-, szabályozó szerkezetet, berendezést. Témánk szempontjából a kontroll kifejezés a (belső) ellenőrzés területéhez kapcsolódóan értelmezendő, amelynek széles körben, más szabályozók, módszertanok által is felhasznált alapdokumentuma a COSO[11] Integrált Belső Kontroll Keretrendszere. [13]

A dokumentumban két alapfogalom szerepel: a belső kontroll és a kontroll-tevékenység. A *belső ellenőrzés / belső kontroll* (internal control): a szervezet vezetői és munkatársai által megvalósított összetett folyamat, amelyet a szervezeti célkitűzésekkel kapcsolatos kockázatok meghatározására és ésszerű biztosítékok kialakítására hoztak létre. [14, 65. o.] A *kontroll tevékenység* (control activity) pedig a kockázatok meghatározása és a szervezet céljainak elérése érdekében kialakított elv (előírás) és eljárás, amelyet egy tevékenység kimenetele bizonytalanságának korlátok között tartására irányul. [14, 59. o.]

A COSO dokumentum értelmezésében tehát a szervezeti célkitűzések elérését fenyegető kockázatok kezelésére és megvalósításuk valószínűségének növelésére speciális rendszabályokat, tevékenységeket kell kialakítani, amelyek – más összetevőkkel együtt – egy összetett folyamatot alkotnak. A továbbiakban a két fogalom közül elsősorban a kontroll tevékenységre építünk. Ez az értelmezés szerepel a kockázatkezelés alapelveit rögzítő ISO 31000 nemzetközi szabványban is, amely szerint a *kontroll* olyan intézkedés, amely módosítja a kockázatot. [15, 6. o.]

A *biztonsági kontroll* (security control) a szervezeti célkitűzések megvalósulását biztosító kontrollok egyik, kiemelt szerepet játszó típusa, biztonsági kockázatok elkerülését, elhárítását, vagy minimálisra csökkentését szolgáló védelmi intézkedés (óvintézkedés, ellenintézkedés).

A biztonsági kontroll és a kontroll fogalmak megkülönböztetése a biztonsági kockázat és a kockázat fogalmak értelmezésétől függ. Amennyiben a kockázatot bizonytalan események hatásához kapcsoljuk (ahol a hatások lehetnek pozitívak és negatívak = lehetőségek és

[10] Control Objectives for Information and Related Technology = információs és kapcsolódó technológiára vonatkozó kontroll célkitűzések.

[11] Committee of Sponsoring Organizations of the Treadway Commission = A Treadway Bizottság Támogató Szervezeteinek Bizottsága (könyvvizsgáló szervezetek önkéntes együttműködése).

fenyegetések), a két kontroll fogalom tartalma között nincs különbség. Ilyen értelmezéssel találkozhatunk az ISO 31000 szabványban. [15, 1. o.] Amennyiben viszont a kockázatot a negatív, káros hatású események körére szűkítve értelmezzük, akkor a két fogalom rész-egész viszonyban áll egymással. Erre az értelmezésre épülnek az informatikai biztonsági dokumentumok. [1, 4. o.; 16, 222. o.] A továbbiakban mi is erre a szűkebb értelmezésre építünk.

A *biztonsági kontrollok osztályozása* számos különböző szempont szerint lehetséges. Ezek közül a következőkben a jelleg és a rendeltetés szerinti osztályozást mutatjuk be.

A *biztonsági kontrollok jelleg szerint* többféleképpen csoportosíthatóak, ahol a csoportosítás alapját a megvalósítás módjai, eszközei képezik. A COSO keretrendszer két átfogó típust különböztet meg: előírások ("mit kell tenni") és eljárások (az előírások megvalósítása). [13, 51. o.] Az ISO 27000 osztályozásában adminisztratív, technikai, vezetési és jogi kontrollok szerepelnek meghatározás nélkül. [1, 2. o.] A NIST dokumentumok három típust különböztetnek meg: vezetési, működési és technikai kontrollok. A vezetési (menedzsment) kontrollok a biztonság és a kockázatok kezelésére irányulnak, míg a működési kontrollok az elsődlegesen emberek által, a technikai kontrollok pedig a technikai eszközök által megvalósított eljárások. [17, B-9, B-6, B-8, B-11. o.]

Egy másik megközelítés szerint a biztonsági kontrollok három típusát az adminisztratív, a fizikai és a technikai (más néven logikai) kontrollok alkotják. Az adminisztratív kontrollok a szervezeti erőforrások megóvására irányuló szervezeti előírások, eljárások és más tevékenységek. A fizikai kontrollok közé a fizikai hozzáférést, beavatkozást megakadályozó technikai eszközök, megoldások tartoznak. Végül a technikai kontrollok a technikai eszközökben megvalósított logikai, eljárási jellegű megoldások. [18, 2., 18., 26. o.]

A *biztonsági kontrollok rendeltetés szerint* is csoportosíthatóak, ami egyben a biztonságot veszélyeztető (nem kívánt) esemény bekövetkezéséhez viszonyított megvalósulásuk szerinti csoportosítást is jelent. Két alapvető típus gyakorlatilag minden dokumentumban megjelenik. A megelőző (preventive) kontrollok rendeltetése a nem kívánatos események, eredmények megakadályozása, elkerülése azok bekövetkezése előtt. Az észlelő, feltáró (detective) kontrollok rendeltetése a már bekövetkezett nem szándékolt események, eredmények feltárása, azonosítása, jelzése a bekövetkezés alatt vagy után. [13, 120., 121. o.; 14, 60., 68. o.; 16, 220., 223. o.; 19, 20. o.]

Több alapvető dokumentumban szerepelnek a helyreigazító, helyesbítő (corrective) intézkedések is, amelyek rendeltetése a bekövetkezett nem kívánatos események káros hatásainak csökkentése, azonban definíció nélkül és nem kontrollnak minősítve. [16, 19] Más dokumentumokban találkozhatunk az elrettentő (deterrent) kontrollok fogalmával, amelyek rendeltetése a nem kívánatos – elsősorban szándékos – események bekövetkezési valószínűségének csökkentése, valamint a helyreállító (recovery) kontrollok fogalmával, amelyek rendeltetése a biztonságsértés előtti állapot visszaállítása. E két utóbbi típus a megelőző és a helyreigazító kontrollok altípusának is tekinthető.

Az *informatikai biztonsági kontroll* (information/IT security control) fogalmának értelmezése szorosan kapcsolódik az információbiztonság és az informatikai biztonság fogalmak viszonyához, értelmezéséhez, ami mindmáig eltérő szakmai megközelítések, nézeteltérések tárgya. A két fogalom és az alkalmazott kifejezések megkülönböztetése a releváns szabványokban, módszertanokban sem egyértelmű[12], általában csak a tartalom jelzi, hogy az adott dokumentumban szereplő értelmezés melyik megközelítéshez áll közelebb.

A továbbiakban jelen publikációban arra a megközelítésre építünk (részletesebben lásd 20), amely szerint az előbbi fogalom az információ és annak minden megnyilvánulási formája (emberek tudatában, hagyományos hordozón, információs tevékenységeket támogató

[12] Bár a vonatkozó ISO szabványok mindegyike (27000, 13335, 15408, 15443, 18045, stb.) az 'Information technology - Security techniques' szabványcsoportban szerepel.

eszközökben) biztonságához, míg az utóbbi az informatikai rendszerekben, eszközökben kezelt információk és maguk a rendszerek, eszközök biztonságához kapcsolódik. A biztonsági területen, a gyakorlatban a kettő egymástól valójában elválaszthatatlan, önmagában egyik sem jelent teljes körű megoldást.

A fentiek alapján informatikai biztonsági kontroll alatt az informatikai biztonsági kockázatok elkerülését, elhárítását, vagy minimálisra csökkentését szolgáló védelmi intézkedést (óvintézkedést, ellenintézkedést) értünk. Az informatikai biztonsági kockázat (information/IT security risk) erőforrások, erőforráscsoportok sérülékenységét kihasználó, a szervezetnek kárt okozó potenciális fenyegetés [1, 4. o.], ahol erőforrás minden, aminek értéke van a szervezet számára (információ, szoftver, hardver, szolgáltatások, emberek). [1, 2. o.]

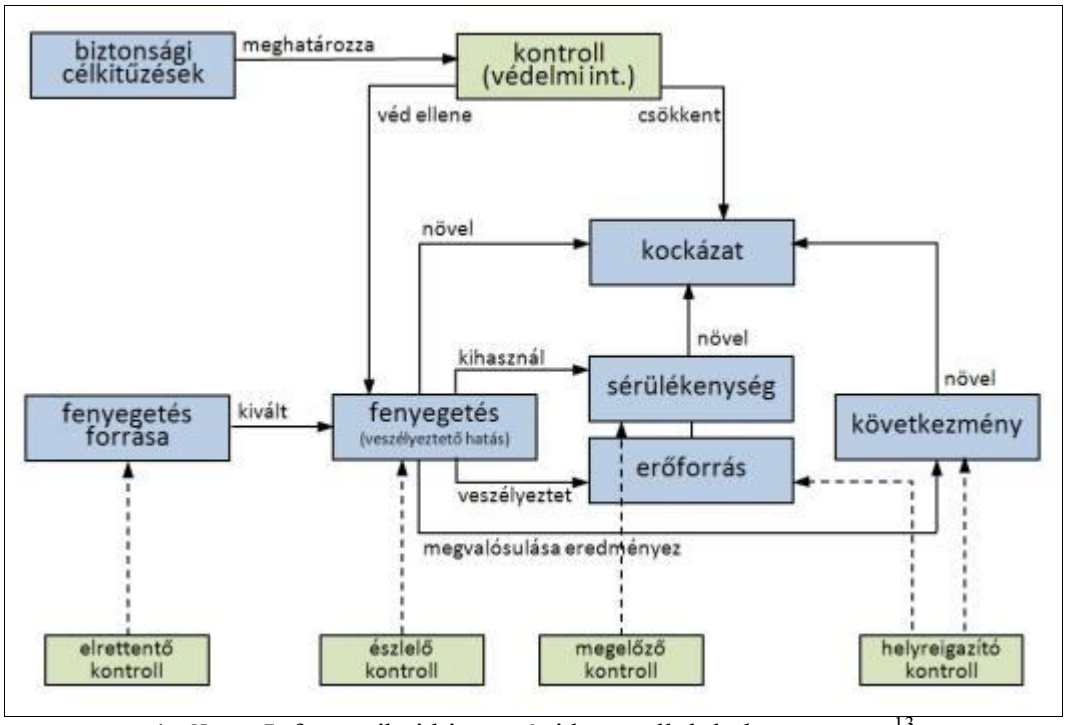
A korábban bemutatott jelleg és rendeltetés mellett az *informatikai biztonsági kontrollok osztályozása az általánosság-részletesség skálán* is lehetséges. Egy védelmi megoldás, intézkedés, eszköz ugyanis többféle szinten meghatározható, például:

- ISO 27002, 11.3.1: A felhasználóknak megfelelő jelszó választási és használati gyakorlatot kell követniük. [2, 64. o.];
- NIST 800-53, IA-5.1.a: Az informatikai rendszer megkövetel bizonyos jelszó-összetettségi előírásokat. [17, F-58. o.];
- CI4.5.3: biztosítani kell, hogy a jelszavak hossza meghaladjon egy minimális értéket, különbözzön a felhasználói azonosítótól, ne tartalmazzon kettőnél több azonos karaktert egymás mellett és ne tartalmazzon kizárólag alfabetikus, vagy kizárólag numerikus karaktereket. [21, CI4.5 o.]

Az általános kontrollok a jól bevált gyakorlatra épülő biztonsági útmutatókhoz kapcsolódnak, az egyes konkrét megoldások általánosításait tartalmazzák. Ezek az általános kontrollok (meghatározások) a különböző szervezetekben, illetve különböző biztonsági célkitűzések esetén történő felhasználhatóság érdekében célszerűen technológia- és megvalósítás-függetlenek. Mindez viszont szükségessé teszi, hogy konkrét megvalósításuk esetén az útmutatóban szereplő kontrollok részletezésre, kiegészítésre kerüljenek. Ennek alapjai és rendje részletesebben megtalálható a NIST 800-53 dokumentumban. [17, 7-8., 19-25. o.]

Az általános(abb) kontrollok testre szabását segíti, ha azok eleve tartalmaznak a szervezetek által meghatározható, vagy választható paramétereket (pld. jelszavak minimális hossza, jelszóváltás előírt gyakorisága, stb.). A részletezés azonban enélkül is megvalósítható (pld. legyen minimális jelszó-hossz előírás ~ a jelszó minimális hossza legalább 8 karakter legyen). Az általános kontrollok kiegészítése (control enhancement) további biztonsági funkciók megvalósítását, vagy a kontroll "erősségének" növelését szolgálja. [17, B-12. o.] Egy biztonsági útmutató az egyes kontrollokhoz több kiegészítést is tartalmazhat, amelyek közül a konkrét biztonsági követelmények függvényében lehet egyet, vagy többet választani. Emellett kiegészítéseket az adott szervezetek is megfogalmazhatnak.

Az *informatikai biztonsági kontrollok szerepe az informatikai biztonság megvalósításában* eszközjellegű. A kontrollok a biztonsági célkitűzések és a kockázatok elemzése, értékelése alapján kerülnek meghatározásra, majd megvalósításra. Rendeltetésük a kockázatok és ezzel a káros következmények bekövetkezésének, illetve mértékének csökkentése. A kontrollok kapcsolatrendszerét az informatikai biztonság (illetve általában a biztonság) más összetevőivel a következő ábra szemlélteti.



1. ábra. Informatikai biztonsági kontrollok helye, szerepe[13]

Adatbázis-biztonsági kontrollok alatt az adatok adatbázis rendszerekben történő tárolásával kapcsolatos biztonsági kockázatok elkerülését, elhárítását, vagy minimálisra csökkentését szolgáló védelmi intézkedéseket értjük.

Az adatbázis-biztonsági kontrollok esetében is végigkövethetők az előzőleg bemutatott csoportosítási lehetőségek. A technológia- és megvalósítás-független általános kontrollokat az általános adatbázis-biztonsági útmutatók tartalmazzák. A biztonság gyakorlati megvalósítása során szükséges az útmutatóban szereplő kontrollok részletezése, kiegészítése, testre szabása. Ennek a folyamatnak a végterméke lehet egy olyan biztonsági útmutató (vagy más néven ellenőrző lista), mely konkrét, specifikált biztonsági kontrollok gyűjteményéből áll. Természetesen ebben az esetben a kontrollok függnek az adatbázis-kezelő rendszer típusától, verziójától és a működési környezet tulajdonságaitól. Egy konkrét típusú és verziójú adatbázis-kezelő rendszerhez adnak ki (gyártók, illetve különböző biztonsági szervezetek) ellenőrző listákat, melyek a helyes telepítés, konfigurálás és működtetés technikai és működési elemeit fogalmazzák meg. A COSO keretrendszer által meghatározott előírások kategória az általános adatbázis-biztonsági útmutatók kontrolljaira jellemző, míg a specifikus adatbázis-biztonsági ellenőrző listák kontrolljai az eljárások kategória alá esnek.

Az 1. ábra osztályozását tekintve megállapíthatjuk (például [9] alapján), hogy az adatbázis-biztonsági kontrollok többsége a megelőző típusba tartozik. Ide sorolhatjuk – a teljesség igénye nélkül – az adatbázis-kezelő rendszer konfigurációs kontrolljait, a hitelesítéssel kapcsolatos kontrollokat, a hozzáférési jogosultságokat szabályozó kontrollokat vagy a titkosítás szabályozását biztosító kontrollokat. Észlelő kontroll kategóriájába tartozik a log menedzsment és elemzés, illetve az illetéktelen hozzáférések megfigyelésének kezelése. Helyreigazító kontrollok körébe az adatbázismentést és helyreállítást szabályozó kontrollok tartoznak. Az elrettentő kontrollok az adatbázis-biztonsági útmutatókra nem jellemzőek, az elrettentés feladatát adminisztrációs módszerekkel, intézkedésekkel lehetséges kezelni.

Az adatbázis-biztonsági kontrollok rendeltetés szerint besorolhatók a következő három kategóriába: technikai kontrollnak az adatbázis-kezelő rendszerben megvalósított biztonsági

[13] Készült az ISO 15408 Védelmi fogalmak és kapcsolatrendszerük ábrájának felhasználásával és kiegészítésével [25, 12.o.].

beállításokat, működési kontrolloknak az adatbázis-kezelő rendszer működtetésével, üzemeltetésével kapcsolatos, emberek által megvalósított eljárásokat, adminisztratív kontrollnak pedig a szervezeti erőforrásokkal kapcsolatos szervezeti előírásokat, eljárásokat értjük.

BIZTONSÁGI ÚTMUTATÓK ÉS KONTROLLOK SZEREPE A BIZTONSÁG MEGVALÓSÍTÁSÁBAN

A biztonsági útmutatók, kontrollok – mint korábban már többször megfogalmaztuk – kiemelt szerepet játszanak az informatikai biztonság megvalósításában, ennek keretében az informatikai biztonság irányításában, valamint szabályozásában. A következőkben a biztonsági útmutatók, kontrollok helyével, szerepével, felhasználásával kapcsolatos néhány alapvető kérdést vizsgálunk meg, ezen belül:

- elemezzük a biztonsági útmutatók, kontrollok helyét és szerepét az informatikai biztonság irányításában;
- meghatározzuk a biztonsági útmutatók, kontrollok helyét és szerepét az informatikai biztonság szabályozásában;
- végül körvonalazzuk az adatbázis-biztonsági útmutatók, kontrollok felhasználásának, kialakításának és továbbfejlesztésének rendjét, feladatait.

Az informatikai biztonság eredményes és hatékony megvalósítása – kialakítása és folyamatos fenntartása – *informatikai biztonsági irányítási rendszer* működtetését igényli, amelynek alapvető feladatai közé a következők tartoznak:

- az informatikai biztonsági követelmények meghatározása;
- az informatikai biztonsági kockázatok feltárása, értékelése;
- az informatikai biztonsági kontrollok (védelmi megoldások, intézkedések) kiválasztása és megvalósítása;
- az informatikai biztonság helyzetének figyelemmel kísérése, szükség esetén a követelmények módosítása, a kockázatok újra értékelése és a védelmi intézkedések újbóli meghatározása, továbbfejlesztése és kiegészítése. [1, 10. o.]

Az *informatikai biztonsági útmutatók, kontrollok a kockázatok feltárásában, értékelésében* (risk identification, analysis, evaluation) már szerepet játszanak. Az útmutatók közvetve járulnak hozzá a kockázatok feltárásához azzal, hogy általánosított módon – az útmutató alkalmazási területére vonatkozóan teljes körűen – tartalmaznak különböző szintű kontroll-célkitűzéseket, amelyek felhasználása segíthet kockázatok felismerésében. Emellett a kockázatok alapját a védendő erőforrások sérülékenységei és az ezeket kihasználni képes fenyegetések mellett a már létező védelmi megoldások, intézkedések (kontrollok) is képezik. Ezek ugyanis megszüntethetik, vagy csökkenthetik az erőforrások eredendő sérülékenységét, korlátozhatják a fenyegetések káros hatásait, ezzel befolyásolhatják a kockázatokat.

Az *informatikai biztonsági útmutatók, kontrollok a kockázatok kezelésében* (risk treatment) alapvető szerepet játszanak. Ennek során a kontrollok az egyik legfontosabb megoldást képezik. Amennyiben a döntéshozók nem a kockázatok felvállalását, elkerülését, vagy áthárítását választják, a kockázatok csökkentésére megfelelő védelmi intézkedéseket kell alkalmazniuk. [3, 42. o.] A védelmi intézkedések (kontrollok) kiválasztásának alapvető támogatását a biztonsági útmutatók nyújtják, amelyek a bevált gyakorlat alapján általánosan megfogalmazott biztonsági célkitűzéseket megvalósító kontrollokat biztosítanak alapként a konkrét célkitűzéseket megvalósító kontrollok meghatározásához. Természetesen védelmi

intézkedések (kontrollok) útmutatók nélkül is meghatározhatóak, ez azonban a gyakorlat meglévő tapasztalatainak, eredményeinek figyelmen kívül hagyását jelenti.

Az *informatikai biztonsági útmutatók, kontrollok a biztonság helyzetének értékelésében* is felhasználhatóak. A szervezeti szintű útmutatók, a bennük foglalt előírások megvalósulásának értékelése referencia-alapot képez a biztonsági helyzet értékeléséhez. Az általános (több szervezetben is hasznosítható) útmutatók felhasználási lehetősége kétoldalú. Egyrészt a tapasztalatok alapján frissített útmutatók új követelményekre, sebezhetőségekre és megoldásokra hívhatják fel az egyes szervezetek figyelmét, másrészt – mivel a biztonsági helyzet folyamatos figyelemmel kísérése, illetve ennek különböző megoldásai maguk is szerepelnek a kontrollok között – konkrét útmutatást is tartalmaznak. A legismertebb útmutatók (kontroll-gyűjtemények) mindegyikében megtalálhatóak a felülvizsgálatra, értékelésre irányuló kontrollok.[14]

Az *informatikai biztonság szabályozása* általános értelemben az informatikai biztonsághoz kapcsolódó szabályok – feladatok, felelősségi és hatáskörök, előírások és korlátozások – meghatározása. Mint minden szabályozás, elsősorban a rendszeresen ismétlődő tevékenységek végrehajtásának eljárási, szakmai, vagy technikai szabályait rögzíti. A szabályozás szintjét tekintve lehet nemzetközi, nemzeti, ágazati (szakterületi), vagy szervezeti, emellett megkülönböztethetünk jogi és önszabályozást is. A szabályozáshoz kapcsolódóan fontos szerepet játszanak a szabványok is.

A *biztonsági útmutatók közvetlen alkalmazása* nemzeti, ágazati, vagy szervezeti szinten azt jelenti, hogy az adott szabályozó a hatálya alá tartozó szervezetek, szervezeti elemek számára előírja kiválasztott útmutató(k)ban foglalt kontrollok, vagy azok egy meghatározott részének alkalmazását, megvalósítását. Ezek az útmutatók nemzeti szinten – a saját felügyelet érdekében – általában nemzeti szabványok, ajánlások. Erre példa az Egyesült Államok Szövetségi Információbiztonsági Törvénye [22], amely a szövetségi informatikai rendszerekre előírja a vonatkozó NIST dokumentumokban foglaltak alkalmazását. Ágazati (szakterületi) szinten szintén találkozhatunk közvetlen hivatkozással, például az ISO 27000 szabványcsalád egészségügyi informatikai tagja [23] az ISO 27002 útmutatóra épít. Szervezeti szabályozások előírhatják az alkalmazott rendszerekre, eszközökre vonatkozó gyártói útmutatók alkalmazását is.

A *biztonsági útmutatók közvetett alkalmazása* esetében az adott szabályozó közvetlenül nem hivatkozik útmutatóra, ehelyett – mintegy szakmai háttéranyagként – az abban (azokban) foglaltak kerülnek felhasználásra. Ennek során elsősorban az útmutató(k)ban található informatikai biztonsági célkitűzések – kontroll célkitűzések – kerülnek felhasználásra, mérlegelve az érintett terület biztonsági kockázatait és magas szintű biztonsági célkitűzéseit. Ez a felhasználás egyaránt előfordulhat nemzeti, ágazati és szervezeti szintű szabályozások esetében.

A *biztonsági útmutatók minőségbiztosítási alkalmazása a szabályozásban* elsősorban belső minőségellenőrzési és külső minőségtanúsítási előírásokra épül. Az informatikai biztonság területén régóta léteznek minőségértékelési, tanúsítási módszertanok, szabványok, útmutatók. Míg ezek korábban függetlenek voltak a biztonsági kontrollok gyűjteményét tartalmazó útmutatóktól, az ISO 27000 szabványcsalád esetében ez a kapcsolat már kiépült, a kidolgozás alatt álló szabványok egyike[15] kimondottan a biztonsági kontrollokhoz kapcsolódik.

A *biztonsági útmutatók szabályozási alkalmazásának jellegzetes területei* közé nemzeti szinten mindenekelőtt az e-közigazgatás, a védelmi szféra és a kritikus infrastruktúra védelem tartozik. Jelentős szabályozási terület a minősített adatok, illetve a személyes adatok védelme

---

[14] ISO 27002 [2]: 5.1.2, 6.1.8 és 15.2 kontrollok;
ISF SGOP [21]: SM3.5, SM7.1, CB5.4, CI5.5, NW4.5 és SD2.3 kontroll-csoportok (szekciók);
NIST 800-53 [17]: AU és CA kontroll-családok.

[15] ISO 27008, Guidance for auditors on ISMS controls = Útmutató ellenőrök számára a biztonsági kontrollokhoz.

is. Az ágazati, szakterületi – ezen belül mindenekelőtt az infokommunikációs területi – szabályozás alapvető jellemzője az önszabályozás, általában az ISO 27000 szabványcsaládnak történő megfelelés. A pénzügyi szolgáltatásokkal kapcsolatos magyar szabályozórendszer pedig jelentős mértékben épít a COBIT módszertanra. [24, 3. o.]

Az *adatbázis-biztonsági útmutatók felhasználása* – a fentiekkel összhangban – az adatbázis rendszerek biztonsági kockázatainak feltárásában és kezelésében, az adatbázis-biztonsági kontrollok kiválasztásának és alkalmazásának folyamatában és a biztonsági ellenőrzés, biztonsági audit folyamán lehetséges. Az adatbázis-biztonsági útmutatók tartalma kiterjed többek közt az adatbázis-kezelő rendszer és működési környezetének biztonságos beállításaira, az adatbázisok biztonságos beállításaira, illetve a működési folyamatok biztonságos kezelésére (például a felhasználók menedzsmentjére, a hitelesítés, mentés, helyreállítás, telepítés és log elemzés folyamataira).

Jelenleg hazánkban nemzeti szintű adatbázis-biztonsági szabályozás nem létezik, a jövőben azonban az e-közigazgatás és a kritikus infrastruktúra védelem területén szükség lehet ennek bevezetésére. A szerzők véleménye szerint a jövőben kialakítandói szabályozást érdemes lenne a következő többszintű modell mentén felépíteni.

A szabályozás egyik részét képezné a szervezet- és tevékenység-független általános adatbázis-biztonsági útmutató, mely rendszabályok rendezett listája lenne. Az általános adatbázis-biztonsági útmutató keretszabályozást jelentene, az adatbázis rendszerek üzemeltetésére, telepítésére, konfigurálására vonatkozó biztonsági kontrollokat szervezet-, tevékenység- és termék-független módon tartalmazná. A dokumentum mintaként szolgálna a szervezetek számára a saját adatbázis-biztonsági útmutató elkészítéséhez, mely már szervezet és tevékenység specifikusan tartalmazná a követelményeket, előírásokat. Az útmutató önmagában nem egy kötelező erejű jogszabály lenne, helyét magyar viszonylatban a Közigazgatási Informatikai Bizottság ajánlásai között tudnánk elképzelni. Használatát viszont meghatározott szervezetek számára egy kormányrendelet elrendelhetné.

A szabályozás másik része szervezet specifikus dokumentumokból állna. A szabályozás hatálya alá eső szervezetnek ki kellene dolgoznia a saját általános adatbázis biztonsági útmutatóját az előző pontban leírt útmutató adaptációjával. Ebben az adatbázis rendszerre vonatkozó követelményeket saját szervezetére vonatkoztatva kellene megfogalmazni. Továbbá a szervezetnek az általános biztonsági követelményeket át kellene fogalmaznia konkrét biztonsági kontrollok, ellenőrzési pontok halmazává, ami a saját adatbázis-kezelő rendszerére és az aktuális működési környezetre érvényes, ez lenne a szervezet adatbázis-biztonsági ellenőrző listája. Ebből a két dokumentumból épülne fel a szervezet adatbázis-biztonsági szabályzata.

Az adatbázis-biztonsági útmutatók felépítésére a gyakorlatban különböző példákat láthatunk. Egy általunk logikusnak vélt rendszerezés a biztonsági kontrollok rendeltetés szerinti csoportosításra épül. Ezek alapján megkülönböztetjük a technikai, a működési és az adminisztratív kontrollokat. Technikai kontrollnak az adatbázis-kezelő rendszerben megvalósított biztonsági konfigurációs beállításokat, működési kontrolloknak az adatbázis-kezelő rendszer működtetésével, üzemeltetésével kapcsolatos eljárásokat, adminisztratív kontrollnak pedig a szervezeti erőforrásokkal kapcsolatos előírásokat, eljárásokat értjük.

ÖSSZEGZÉS

Az *informatikai biztonsági útmutatók* és a kapcsolódó dokumentumok (ellenőrző listák) az informatikai biztonság kialakítását és fenntartását szolgáló védelmi megoldások, rendszabályok és tevékenységek kialakításának, illetve ellenőrzésének alapvető eszközei. Az útmutatók fő összetevőit a védelmi megoldások, intézkedések, biztonsági kontrollok képzik.

A szervezetek biztonsági szabályozórendszere három szintre osztható: felső szinten a biztonsági politika és stratégia, középső szinten átfogó és részterületi szabályzatok, míg alsó szinten a konkrét feladat- és szerepkörökre vonatkozó részletes biztonsági eljárások találhatóak. A biztonsági útmutatók a szervezetekben a középszintű szabályozóknak és az alsó szintű biztonsági feladatoknak az átfogó biztonsági politika és biztonsági célkitűzések alapján történő kialakítását támogatják, segítik. A biztonsági útmutatók általában több szervezet számára felhasználható módon, azokon kívül kerülnek kidolgozásra.

A *biztonsági ellenőrző listák* a biztonsági útmutatókban foglalt konkrét megoldások, tevékenységek megvalósulásának ellenőrzésére szolgáló dokumentumok. Az informatikai biztonsági területen jelentős szerepet játszanak a biztonsági konfigurációs ellenőrző listák, amelyek adott informatikai termékek javasolt, biztonságos beállításait, valamint az alkalmazott adminisztrációs megoldásokat, eljárásokat ellenőrzik.

A biztonsági útmutatók, ellenőrző listák felhasználásának lehetőségei három nagy területbe sorolhatóak. (1) A *biztonsági intézkedések kiválasztása, kialakítása során* történő felhasználás jelenti az alapvető felhasználási módot, ahol a biztonsági útmutatók elméletileg megalapozott és a bevált gyakorlatra épülő általános célkitűzés- és megoldás-gyűjteményként szolgálnak. (2) A *szabályozás során* történő felhasználás külső előírásokhoz kapcsolódik. Ennek során a szabályozás hatálya alá tartozó szervezetek számára előírják, hogy mely védelmi megoldásokat, intézkedéseket kell kötelező érvénnyel, vagy bizonyos feltételek fennállásának függvényében megvalósítaniuk. (3) Az *ellenőrzés céljára* történő felhasználás a biztonság állapotának ellenőrzéséhez, felülvizsgálatához, illetve a meghatározott követelményeknek történő megfelelés értékeléséhez kapcsolódik. A biztonsági útmutatókban foglaltak az ellenőrzés, értékelés során etalonként használhatóak fel annak megítéléséhez, hogy a meghatározott biztonsági célkitűzésekhez és kockázatokhoz megfelelőek-e a megvalósított védelmi intézkedések és megfelelő módon kerültek-e megvalósításra.

Az *adatbázis-biztonsági útmutatók* az adatbázis rendszerek telepítésére, konfigurálására, üzemeltetésére, illetve az adatbázis-kezelő rendszer működésére kiható, az informatikai rendszer egyéb összetevőire (operációs rendszer, hálózat, adatbázist elérő alkalmazások) vonatkozó biztonsági követelményeket és biztonsági kontrollokat tartalmazzák. A dokumentumokat két fő csoportra oszthatjuk a bennük található biztonsági kontrollok általános-részletes jellege alapján. Az egyik csoportot az általános adatbázis-biztonsági útmutatók alkotják, melyek az adatbázis-kezelő rendszer típusától függetlenül fogalmaznak meg biztonsági követelményeket. A másik csoportot az adatbázis-kezelő rendszer típusához készült útmutatók alkotják, melyek általában adatbázis ellenőrző lista elnevezést viselik.

Az informatikai biztonsági útmutatók összetevőit képző *biztonsági kontrollok* az informatikai biztonság kialakításának, fenntartásának és értékelésének alapvető eszközei, alapját képezik az informatikai biztonsági irányítás különböző módszertanának. *Informatikai biztonsági kontroll* alatt az informatikai biztonsági kockázatok elkerülését, elhárítását, vagy minimálisra csökkentését szolgáló védelmi intézkedést (óvintézkedést, ellenintézkedést) értünk. Az informatikai biztonsági kontrollok a biztonsági célkitűzések és a kockázatok elemzése, értékelése alapján kerülnek meghatározásra, majd megvalósításra. Rendeltetésük a kockázatok és ezzel a káros következmények bekövetkezésének, illetve mértékének csökkentése.

Adatbázis-biztonsági kontrollok alatt az adatok adatbázis rendszerekben történő tárolásával kapcsolatos biztonsági kockázatok elkerülését, elhárítását, vagy minimálisra csökkentését szolgáló védelmi intézkedéseket értjük.

Az általános adatbázis-biztonsági útmutatók technológia- és megvalósítás-független általános kontrollokat tartalmaznak. A biztonság gyakorlati megvalósítása során szükséges az útmutatóban szereplő kontrollok részletezése, kiegészítése, testre szabása. Ennek a folyamatnak a végterméke lehet egy olyan biztonsági útmutató vagy más néven ellenőrző

lista, mely konkrét, specifikált biztonsági kontrollok gyűjteményéből áll. Ekkor a kontrollok függnek az adatbázis-kezelő rendszer típusától, verziójától és a működési környezet tulajdonságaitól.

A biztonsági útmutatók, kontrollok szerepe az informatikai biztonság megvalósításában, ennek keretében az informatikai biztonság irányításában, valamint szabályozásában kiemelt jellegű. Az informatikai biztonsági útmutatók, kontrollok szerepet játszanak *a biztonsági kockázatok feltárásában, értékelésében*. Az útmutatók közvetve járulnak hozzá a kockázatok feltárásához azzal, hogy tartalmaznak különböző szintű kontroll-célkitűzéseket, amelyek felhasználása segíthet a kockázatok felismerésében. Az informatikai biztonsági útmutatók, kontrollok *a kockázatok kezelésében* alapvető szerepet játszanak. Ennek során a kontrollok az egyik legfontosabb megoldást képezik. A védelmi intézkedések, kontrollok kiválasztásának alapvető támogatását a biztonsági útmutatók nyújtják, amelyek a bevált gyakorlat alapján általánosan megfogalmazott biztonsági célkitűzéseket megvalósító kontrollokat biztosítanak alapként a konkrét célkitűzéseket megvalósító kontrollok meghatározásához. Az informatikai biztonsági útmutatók, kontrollok *a biztonság helyzetének értékelésében* is felhasználhatóak. A szervezeti szintű útmutatók, a bennük foglalt előírások megvalósulásának értékelése referencia-alapot képez a biztonsági helyzet értékeléséhez.

Az *adatbázis-biztonsági útmutatók felhasználása* az adatbázis rendszerek biztonsági kockázatainak feltárásában és kezelésében, az adatbázis-biztonsági kontrollok kiválasztásának és alkalmazásának folyamatában és a biztonsági ellenőrzés, biztonsági audit folyamán lehetséges. Az adatbázis-biztonsági útmutatók tartalma kiterjed többek közt az adatbázis-kezelő rendszer és működési környezetének biztonságos beállításaira, az adatbázisok biztonságos beállításaira, illetve a működési folyamatok biztonságos kezelésére (például a felhasználók menedzsmentjére, a hitelesítés, mentés, helyreállítás, telepítés és log elemzés folyamataira).

Jelenleg hazánkban nemzeti szintű adatbázis-biztonsági szabályozás nem létezik, a jövőben azonban az e-közigazgatás és a kritikus infrastruktúra védelem területén szükséges lehet ennek bevezetésére.

Felhasznált irodalom

[1] ISO/IEC 27000:2009 (E), Information technology – Security techniques – Information security management systems – Overview and vocabulary. First edition. – ISO/IEC, 2009.05.01.

[2] ISO/IEC 27002:2005 (E), Information technology – Security techniques – Code of practice for information security management. First edition. – ISO/IEC, 2005.06.15.

[3] Berkes Zoltán, Déri Zoltán, Krasznay Csaba, Muha Lajos: KIB 25. ajánlása, 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK). 25/1-1. kötet, Informatikai Biztonsági Irányítási Rendszer (IBIR). 1.0 verzió. Budapest: Miniszterelnöki Hivatal, 2008.

[4] NIST Special Publication 800-70, National Checklist Program for IT Products – Guidelines for Checklist Users and Developers. Revision 2. – National Institute of Standards and Technology, Gaithersburg, 2011 február.

[5] Special Publication 800 Series. – NIST. [csrc.nist.gov/publications/PubsSPs.html, 2011.08.10.]

[6] Security Technical Implementation Guides. – DISA. [iase.disa.mil/stigs/index.html, 2011.08.10.]

[7] Munk S., Fleiner R.:Az adatbázis-biztonság szabályozása és megvalósítása az Egyesült Államok haderejében– Bolyai Szemle, 2009 (XVIII.)/4. (81-102.o.)

[8] Database Security Technical Implementation Guide, Version 8, Release 1. – DISA, 2007. szeptember.

[9] Database Security Guideline. – Database Security Consortium, 2009.

[10] Security Configuration Benchmark For Oracle Database Server 11g. - The Center for Internet Security, 2008 szeptember
[cisecurity.org, 2011.08.10.]

[11] Oracle Database Security Checklist. – SANS Institute.
[www.sans.org/score/oraclechecklist.php, 2011.08.10.]

[12] Database Security Checklist, Version 7, Release 2.2. – DISA, 2006. október.

[13] Internal Control – Integrated Framework. Executive Summary. – Committee of Sponsoring Organizations of the Treadway Commission, 1992.

[14] INTOSAI GOV 9100, Irányelvek a belső kontroll standardokhoz a közszférában. (magyar fordítás) – INTOSAI Főtitkárság, Bécs, 2004.

[15] ISO 31000:2009(E), Risk Management – Principles and guidelines. First Edition. – ISO, 2009.11.15.

[16] COBIT 4.1 Magyar Változat. – Információrendszer Ellenőrök Egyesülete, 2007.

[17] NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations. Revision 3. – National Institute of Standards and Technology, Gaithersburg, 2009 augusztus.

[18] CERT Resilience Management Model, Version 1.0, Glossary of Terms. – Carnegie Mellon University, Software Engineering Institute, 2010 május.

[19] NIST Special Publication 800-30, Risk Management Guide for Information Technology System. – National Institute of Standards and Technology, Gaithersburg, 2002 július.

[20] MUNK Sándor: Információbiztonság vs. informatikai biztonság. – Robothadviselés 7 tudományos szakmai konferencia anyaga (2007.11.27.), Hadmérnök különszám.

[21] The Standard of Good Practice for Information Security. – Information Security Forum, 2007.

[22] Federal Information Security Management Act. (Title III of the E-Government Act) – 2002.

[23] ISO 27799:2008, Health informatics — Information security management in health using ISO/IEC 27002. – ISO, 2008.07.01.

[24] A Pénzügyi Szervezetek Állami Felügyeletének 1/2007. számú módszertani útmutatója a pénzügyi szervezetek informatikai rendszerének védelméről. – PSZÁF, Budapest, 2007 október.

[25] ISO/IEC 15408-1:2005, Information Technology - Security Techniques -Evaluation criteria for IT security - Part 1: Introduction and general model. Second Edition. - ISO, 2005.10.01.

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Kuris Zoltán
zoltan.kuris@bm.gov.hu

Faggyas Zoltán
zoltan.faggyas@bm.gov.hu

MINŐSÍTETT ADATOKAT KEZELŐ INFORMATIKAI RENDSZEREK KOCKÁZATÉRTÉKELÉSE ÉS KOCKÁZATMENEDZSMENTJE

Absztrakt

A minősített adatokat kezelő informatikai rendszerekben kezelt minősített adat bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása komplex védelmi intézkedéseket igényel a rendszer teljes életciklusában. Ezen intézkedések csak akkor lehetnek kellően hatékonyak, költségek szempontjából is optimalizáltak, ha azokat a biztonsági kockázatokkal arányosan tervezik és implementálják. Jelen cikkben a szerzők ismertetik a hazai nemzeti és külföldi minősített adatokat kezelő informatikai rendszerek kockázatértékelésére és kockázatmenedzsmentjére vonatkozó követelményeket, a megvalósításukkal kapcsolatos dilemmákat, valamint javaslatokat fogalmaznak meg a még nem szabályozott területein elveiket, módszereiket és eszközeiket illetően.

Providing for the confidentiality, integrity and availability of classified information that are handled in information systems dealing with classified information requires complex protective measures during the entire life-cycle of the system. Such measures can be efficient and cost-efficient only when they are designed and implemented with respect to the security risks. In this current article the authors demonstrate the requirements regarding risk assessment and risk management for information systems that handle national and international classified data, the dilemmas about their implementation, and they form recommendations about their principles, methods and instruments for the unregulated areas.

Kulcsszavak: *kockázatértékelés, kockázatmenedzsment, minősített adat, informatikai rendszerek, INFOSEC ~ risk assessment, risk management, classified information, information systems*

BEVEZETÉS

Korunkat globális fejlettsége alapján információs társadalomként szokás jellemezni. Az elmúlt évtizedek információtechnológiai fejlődése az információ előállításának, terjesztésének, használatának és kezelésének elveit, módszereit és eszközeit forradalmian átalakította, döntő hatást gyakorolva a társadalom gazdasági, politikai és kulturális működésére. Az információ érték, tudás, hatalom, az információvagyon szerepe folyamatosan felértékelődik, napjainkban egyre több területen legfontosabb erőforrássá válik. A magánszektor és a kormányzati szektor szereplőinek hatékony működéséhez, ügyfeleik kiszolgálásához egyaránt fontos, hogy a kellő információ, a megfelelő helyen és időben, a szükséges formában és minőségben könnyen hozzáférhető legyen, melynek érdekében informatikai rendszereiket és infrastruktúráikat folyamatosan fejlesztik, szolgáltatásaikat bővítik. Társadalmunk ezzel egyidejűleg egyre jobban függ ezek működésétől és szolgáltatásaitól, meghibásodásuk, megsemmisülésük, információik kiszivárgása üzemeltetőik és ügyfeleik számára is súlyos károkat okozhatnak. „Az információs társadalom szorosan kapcsolódik és függ a funkcionális információs infrastruktúráktól (pl. távközlő hálózatok, számítógép-hálózatok, távvezérlő rendszerek), melyek tevékenysége viszont nem lehetséges a támogató infrastruktúrák (pl. villamos energiaellátó rendszerek) hatékony működése nélkül.”[1]

Az informatikai rendszerek és infrastruktúrák biztonságának kritikusságát a vállalkozások, állami szervek és intézmények egyre nagyobb mértékben felismerik, a véletlen események (melynek hátterében legtöbbször nem megfelelő rezsimintézkedések vagy emberi mulasztások állnak) és szándékos támadások (adatlopás, kibertámadás, kémkedés, szabotázs, rombolás) bekövetkezési valószínűségének és hatásainak minimalizálására komplex védelmi intézkedések rendszerét alkalmazzák, amely személyi, fizikai, adminisztratív és elektronika biztonsági intézkedések alrendszereiből épül fel.

A komplex védelmi intézkedések rendszerének megvalósítását nemzetközi szabványok (az információbiztonság területén vezető ISO 2700x szabványcsalád), ajánlások (hazai viszonylatban legfontosabb a Közigazgatási Informatikai Bizottság 25. számú ajánlása) támogatják.[2]

Ahhoz hogy a komplex védelmi intézkedések kellően hatékonyak és költségek szempontjából is optimalizáltak legyenek, - a hatékony projektszervezet kialakításán túl - szükséges az alapos és körültekintő kockázatértékelés és jól működő kockázatmenedzsment a rendszerek teljes életciklusában. A kockázatértékelés egy olyan eljárásrendszer, amely azonosítja az informatikai rendszerek biztonsági kockázatait, azaz fenyegetettségüket és sebezhetőségeiket. Meghatározza nagyságukat és, hogy mely területeken szükséges a biztonság megerősítése vagy ellenintézkedés foganatosítása. A biztonsági kockázatmenedzsment pedig az a teljes folyamat, amely azonosítja, kontrollálja és minimalizálja a bizonytalan események lehetőségét, melyek a rendszer erőforrásaira kihatással lehetnek.

A KOCKÁZATÉRTÉKELÉS ÉS KOCKÁZATMENEDZSMENT JELENTŐSÉGE

Azt, hogy milyen gazdasági és politikai hatásokat okozhatnak informatikai rendszereket ért véletlen események (pl. természeti katasztrófa), illetve célzott támadások az alábbi néhány példa jól szemlélteti.

„A Katrina hurrikán 2005 augusztusában mind a vállalati vezetőket, mind az informatika felelőseit megdöbbentette. Ez a természeti katasztrófa súlyos csapást mért az USA déli

államainak informatikai struktúrájára és hálózati rendszereire, jószerével rendet vágott számos szervezet elsődleges és tartalék informatikai rendszerei között."[3]

A közelmúltban a Sony 70 millió felhasználójának adatait szerezték meg hackerek, személyes adatok mellett, bankkártya adatokat is, mely dollármilliárdos kárt okozott a cégnek, jelentősen megingatva piaci jó hírét és pozícióját.

Az USA egyik legnagyobb hadipari cége a Lockheed Martin május végén jelentette be, hogy kibertámadást kíséreltek meg ellene, a támadásnál a távoli elérést biztosító RSA SecurID hardverkulccsal támogatott authentikáció EMC által márciusban közzétett sebezhetőségét használták ki, a támadás sikerességével kapcsolatos hírek ma még ellentmondásosak.[4]

Irán elismerte, hogy jelentős károkat okozott nukleáris erőműveiben a Stuxnet féreg vagy vírustámadás, mely az iráni atomprogramban kulcsszerepet játszó urándúsító centrifugák vezérlését támadta, a hírek szerint a Stuxnet tevékenysége kapcsán az urándúsító centrifugák több mit 20%-a megsemmisült, melynek hatására a többi működését is leállították. A New York Times egy cikke és az iráni kormányzat szerint is a Stuxnet féreg az amerikai és izraeli titkosszolgálat közös fejlesztése.

Szakértők egyenesen orosz-észt kiberháborúként jellemezték a 2007-ben észt informatikai infrastruktúra fontos informatikai pontjait célzó támadást, mely az észt kormánynak egy szovjet hősi emlékmű áthelyezését érintő döntése után indult, internetes kibertámadások összehangolt sorozata volt. E mellett az interneten és mobiltelefon-üzeneteken keresztül folytatódtak, az intenzív propagandatámadások. Az internetes támadások megpróbálták megbénítani a különböző észt honlapok működését, súlyosságát jelzi, hogy az észt hálózaton az adatforgalom sokszor órákon át a normális ezerszerese volt. Az észt miniszterelnök kiberháborúról, külügyminiszterük orosz kormányszervek számítógépeiről érkező internetes terrortámadásokról beszélt.[5]

A Wikileaks nemzetközi nonprofit szervezet weboldalán tesz folyamatosan közzé minősített adatokat tartalmazó anyagokat, legnagyobb számban amerikai diplomáciai jelentéseket, iraki és afganisztáni katonai műveletekkel kapcsolatos dokumentumokat. A nyomozás megállapította, hogy az egyik legnagyobb kiszivárogtatás (köztük 250 ezer diplomáciai jelentés) elkövetője egyetlen személy volt, az amerikai hadsereg volt hírszerző elemzője Bradley E. Manning őrvezető, aki Irakban szolgált a 10. hegyi hadosztálynál és hozzáférése volt az amerikai külügy és hadügy közös SIPRNet[1] hálózatához, melyet „Titkos!" minősítési szintű adatok kezelésére is alkalmaznak.

A fent említett esetek jól példázzák, hogy még tőkeerős vállalatok, nemzetek fő prioritást élvező információs infrastruktúrái is sérülékenyek. A kockázati események bekövetkeztének valószínűsége, és hatásai gyakran alulértékeltek, legyen szó akár emberi mulasztásról, akár természeti katasztrófáról, vagy gazdasági és politikai érdekből vezérelt támadásról.

Az államok az információs infrastruktúráikat ért támadások megelőzésére egyre határozottabb elrettentő intézkedéseket is hoznak, 2011. május 31-ei cikkében a New York Times írta, hogy az USA új katonai stratégiája a kritikus infrastruktúráit ért kibertámadásokat egyenértékűnek fogja tekinti a hagyományos háborús cselekményekkel, és arra katonai csapással is válaszolhat.[6]

[1] Secret Internet Protocol Router Network

MINŐSÍTETT ADATOT KEZELŐ INFORMATIKAI RENDSZEREK KOCKÁZATÉRTÉKELÉSÉT ÉS KOCKÁZATMENEDZSMENTJÉT MEGHATÁROZÓ HAZAI SZABÁLYOZÁS

Felismerve azt, hogy a minősített adatok kezelésénél különösen fontos az egységes szabályozás és követelményrendszer, a külföldi minősített adatok védelme mellett a hazai minősített adatok védelme sem lehet másodlagos. A 2010. április 1-én hatályba lépett, a minősített adat védelméről szóló 2009. évi CLV. törvény (továbbiakban Mavtv.) és végrehajtási rendeletei a NATO és EU minősített adatok védelmével összhangban határozta meg a hazai minősített adatok védelmének rendszerét. A Mavtv. megalkotásának alapját az Alkotmány vonatkozó rendelkezései, az Alkotmánybíróság 34/1994. (VI. 24.) AB határozata, valamint az EU minősített adatok védelmére vonatkozó - az EU tagállamokban kötelező érvényű (a Tanács 2001/264/EK határozat a Tanács biztonsági szabályzatának elfogadásáról), továbbá a NATO minősített adatok védelmére vonatkozó - a NATO tagországokban kötelező érvényű (C-M (2002)49 NATO biztonsági politika) - normák és az euro-atlanti térségben általánosan elfogadott nemzetközi gyakorlat képezi.

A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet és a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet a hazai és külföldi minősített adatok védelmének személyi, fizikai, adminisztratív biztonsági szabályaira valamint minősített adatokat kezelő rendszerek elektronikus biztonságára egységes követelményeket határozott meg.

A korábban NATO és az EU minősített adatok védelméért és szakmai felügyeletért felelős Közigazgatási és Igazságügyi Minisztérium szervezeti keretében működő Nemzeti Biztonsági Felügyeletet feladata lett a minősített adat védelmének hatósági felügyelete, a minősített adatok kezelésének hatósági engedélyezése és felügyelete, valamint a nemzeti iparbiztonsági hatósági feladatok ellátása. A Mavtv. értelmében a minősített adat védelmi feltételeinek kialakításáért a minősített adatot kezelő szervek vezetője felelős, ezzel kapcsolatos feladatok végrehajtását és koordinálását a biztonsági vezetőnek kell végezni, ahol nagyobb mennyiségű minősített adatot kezelnek, ott a biztonsági vezető vezetésével külön szervezeti egységként helyi biztonsági felügyeletet is kijelölhető.[7]

A 161/2010. Korm. rendelet rendelkezik arról, hogy minősített adatot elektronikus rendszeren kezelő szerveknél szükséges kijelölni az üzemeltetett rendszer elektronikus biztonságáért felelős személyeket: rendszerbiztonsági felügyelőt, rejtjelfelügyelőt illetve rendszeradminisztrátort (rendszerbiztonsági felügyelet és rejtjelfelügyelet létrehozható, ha a minősített adatok mennyisége indokolja). Az elektronikus biztonságra vonatkozó definíciója „a rendszerekben alkalmazott biztonsági intézkedések - a személyi-, a fizikai-, az adminisztratív-, valamint a rendszer-, a kommunikáció- és a rejtjelbiztonság - összessége, amelyek biztosítják az elektronikusan kezelt minősített adat bizalmasságát, sérthetetlenségét és rendelkezésre állását”, utóbbi három fogalmat a Mavtv. Alapelvek alfejezetében2 definiálja.[8]

Minősített adatot a jogszabályok szerint csak NBF által kiállított adatkezelési engedély birtokában lehet („Korlátozott terjesztésű!” kivételével), elektronikus kezelésükhöz

2 2. § …(3) Bizalmasság elve: minősített adat illetéktelen személy számára nem válhat hozzáférhetővé vagy megismerhetővé.
(4) Sérthetetlenség elve: a minősített adatot kizárólag az arra jogosult személy módosíthatja vagy semmisítheti meg.
(5) Rendelkezésre állás elve: annak biztosítása, hogy a minősített adat az arra jogosult személy számára szükség szerint elérhető és felhasználható legyen.

rendszerengedély szükséges, melyet a kérelmező biztonsági vezetőnek kell hitelesítenie és büntetőjogi felelőssége tudatában kell nyilatkoznia arról, hogy a kérdőíveikben szereplő adatok a valóságnak megfelelőek. Az engedélyek kiadása előtt azt az NBF helyszíni bejárás keretében ellenőrizheti, illetve a már akkreditált rendszert is ellenőrizheti. (A törvény hatályba lépése előtt már működő minősített adat kezelések esetében a követelményeknek történő megfelelésre 2011. december 31., az engedélyek megszerzésére 2012. december 31. a törvény által előírt határidő.)

Minősített adatok elektronikus kezelése esetén követelmény a biztonsági dokumentáció elkészítése, amely a rendszerbiztonsági követelmények („Bizalmas!" és magasabb minősítési szintű adatot kezelő rendszer esetében, valamint internetre vagy más nyilvános hálózathoz kapcsolódó „Korlátozott terjesztésű!" minősítési szintű adatot kezelő rendszer esetében) és az üzemeltetés-biztonsági szabályzat, továbbá - ha a minősített adatot elektronikus rendszeren kezelő szerv rejtjeltevékenységet folytat – a rejtjelszabályzat, a működtetési szabályzat és a kezelési utasítás.

Kockázatértékeléssel és kockázatmenedzsmenttel kapcsolatosan a 161/2010. Korm. rendelet 58. § (2) bekezdése rendelkezik arról, hogy „a biztonsági vezető a rendszer életciklusának kezdeti szakaszában megkezdi a biztonsági dokumentáció kidolgozását, és a rendszer megvalósítása során, valamint a rendszer életciklusának további szakaszaiban, kockázatelemzés és kockázatértékelés alapján a szükséges mértékben kiegészíti vagy módosítja", továbbá R2 4. § (1) d) alpontja hogy az NBF d) „útmutatást ad és konzultációt folytat a biztonsági kockázatelemzéssel, kockázatkezeléssel és az elfogadható kockázattal kapcsolatos kérdésekben".

A nemzeti és külföldi minősített adat személyi, fizikai és adminisztratív biztonságával kapcsolatos követelményeket a hazai jogszabályok teljes körűen szabályozzák, ugyanakkor az elektronikai biztonság tekintetében a nemzeti minősített adatokra vonatkozó követelmények közül csak a kisugárzás biztonság (TEMPEST) követelményei lettek az NBF által kiadott dokumentumban meghatározva.

A jelenlegi gyakorlat szerint az elektronikus biztonság többi területén – az NBF állásfoglalására való tekintettel - a NATO követelményeknek való megfelelés az elvárt. A külföldi minősített adatok hazánkban elsődlegesen EU illetve NATO minősített adatok, melyekre vonatkozóan irányadó az EU-s illetve különösen a NATO-s szabályozás, amelyek lényegesen részletesebb szabályozást tartalmaznak az elektronikai biztonság tekintetében. A fentiekben kifejtett anomáliák indokolják, hogy a cikk következő fejezetében a kockázatértékelés és kockázatmenedzsment EU-s és NATO-s irányelveit átfogóan bemutassuk.

KOCKÁZATÉRTÉKELÉS ÉS KOCKÁZATMENEDZSMENT EU ÉS NATO IRÁNYELVEI

Az EU minősített adatok kezelésére friss jogszabály a Tanács 2011. március 31-i 2011/292/EU határozata az EU-minősített adatok védelmét szolgáló biztonsági szabályokról, amely 2011. május 27-én lépett hatályba, hatályon kívül helyezte a Tanács biztonsági szabályzatának elfogadásáról szóló 2001. március 19-i 2001/264/EK tanácsi határozatot. Az új szabályozás a korábbinál is hangsúlyosabban kezeli a biztonsági kockázatértékelést. A korábbi szabályozás is tartalmazta azt, hogy EU minősített adatokat kezelő kommunikációs és információs rendszerek rendszerbiztonsági követelményeit megállapító dokumentumnak (SSRS), mely „EU Bizalmas!" és magasabb minősítésű rendszerek akkreditációjához követelmény, a Tanács biztonságpolitikáján és kockázatértékelésen kell alapulnia, az SSRS-sel kapcsolatban számos követelményt meghatározott, ugyanakkor a kockázatértékelés folyamatát nem részletezte.

Az új szabályozás előírja, hogy Az EU-minősített adatokat fenyegető kockázatokat folyamatként kell kezelni. A folyamat célja az ismert biztonsági kockázatok feltárása, az ilyen kockázatok elfogadható szintre történő csökkentésére irányuló biztonsági intézkedések meghatározása a határozat alapelveivel és minimumszabályaival összhangban, a benne meghatározott elveknek megfelelően. Ezen túl kimondja, hogy ezen intézkedések hatékonyságát folyamatosan értékelni kell. Az EU-minősített adatok teljes életciklusuk alatti védelmét szolgáló biztonsági intézkedéseknek arányban kell állniuk különösen az adatok biztonsági minősítésével, az adat vagy anyag formájával és mennyiségével, az EU-minősített adatok tárolására használt létesítmények elhelyezkedésével és felépítésével, valamint a szándékos károkozás és/vagy bűncselekményekből - a kémkedést, a szabotázst és a terrorizmust is ideértve - eredően helyi szinten fennálló fenyegetéssel. A biztonsági kockázatkezelés a kommunikációs és információs rendszer (CIS) meghatározásának, kialakításának, működtetésének és fenntartásának szerves részét képezi. A kockázatkezelést (értékelés, tulajdonképpeni kezelés, elfogadás, kommunikáció) ismétlődő folyamatként kell elvégezni, a rendszertulajdonosok, projekthatóságok, működtető hatóságok és biztonsági jóváhagyó hatóságok képviselőivel közösen, egy kipróbált, átlátható és teljes mértékben érthető kockázatértékelési folyamat alkalmazásával.

A CIS alkalmazási körét és eszközeit a kockázatkezelési folyamat kezdetekor egyértelműen meg kell határozni. Az illetékes hatóságoknak át kell tekinteniük a CIS-t fenyegető potenciális veszélyeket, valamint naprakész és pontos, az aktuális működési környezetet tükröző fenyegetésértékeléssel kell rendelkezniük. A változó információtechnológiai környezettel való lépéstartás érdekében folyamatosan frissíteniük kell a sebezhetőségi kérdésekkel kapcsolatos ismereteiket, és rendszeresen felül kell vizsgálniuk a sebezhetőségi értékeléseket. A biztonsági kockázatkezelés célja olyan biztonsági intézkedések alkalmazása, melyek eredményeképpen kielégítő egyensúly teremthető a felhasználók igényei, a költségek és a fennmaradó biztonsági kockázatok között. Egy adott CIS akkreditálásának vonatkozásában a megfelelő biztonsági akkreditációs hatóság által meghatározott különös követelményeknek, nagyságrendnek és részletességnek arányban kell állnia a valamennyi vonatkozó tényező figyelembe vételével - a CIS-ben kezelt EU-minősített adatok minősítési szintjét is beleértve - megállapított kockázattal. Az akkreditáció magában foglalja a fennmaradó kockázat hivatalos megállapítását és a fennmaradó kockázatnak a felelős hatóság általi elfogadását.

A CIS-t fenyegető veszélyek enyhítése érdekében mélységi védelem szükséges, amely technikai és nem technikai biztonsági intézkedések végrehajtását jelenti. Szigorúságuk mértékét kockázatfelmérés alapján kell meghatározni, melyek többszörös biztonsági réteget (elrettentés, megelőzés, észlelés, ellenálló képesség, helyreállítás) alkotnak. Meghatározza továbbá, hogy a Főtitkárságnak és a tagállamoknak együtt kell működniük a CIS-en kezelt EU-minősített adatok védelmére vonatkozó legjobb gyakorlat kialakítása érdekében. A legjobb gyakorlatra vonatkozó iránymutatások tartalmazzák a CIS-szel kapcsolatos, az adott fenyegetésekkel és sebezhetőségekkel szemben bizonyítottan hatékony technikai, fizikai, szervezeti és eljárási biztonsági intézkedéseket. A CIS-ben kezelt EU-minősített adatok védelme az információvédelemben részt vevő - az EU-n belüli és kívüli - szervezetek által levont tanulságokra épül.[9]

A NATO Biztonsági politikája (CM(2002)49) B (Alapelvek és minimális biztonsági előírások) és F (INFOSEC) mellékletében rögzíti, hogy civil és katonai szerveinél ahol minősített adatot kezelő rendszereket üzemeltetnek, azokat kockázatértékelésnek és kockázatelemzésnek kell alávetni a biztonságpolitika támogató irányelveinek követelményei szerint. Összhangban az INFOSEC elsődleges irányelvei, INFOSEC menedzsment irányelvei, valamint műszaki és kivitelezési irányelvek követelményeivel a biztonsági kockázatmenedzsment elveit és módszereit akkor is alkalmazni kell, ha NATO

kommunikációs és információs rendszert kapcsolunk más CIS-hez (beleértve az internetet vagy más hasonló nyilvános hálózatot). A biztonsági kockázatmenedzsment elveit és módszereit szintén befogadhatják a nemzeti biztonságot jóváhagyó hatóságok.[10]

A NATO AC/35-D/2004-REV2 (Iránymutatás CIS-ek biztonsági jóváhagyására vagy biztonsági akkreditációjára) dokumentum a biztonsági jóváhagyás/engedélyezés első elemeként nevesíti a kockázatértékelési eljárás felülvizsgálatát és az ebből származó információkat, továbbá vizsgálja a biztonsági dokumentációban rögzített rendszer teljes életciklusára kiterjedő biztonsági intézkedések részeként a kockázatmenedzsmentet és az azonosított fennmaradó kockázatokat.[11]

A NATO kommunikációs és információs rendszerek (CIS) biztonsági kockázatértékelésére és kockázatmenedzsmentjével kapcsolatos iránymutatások, általános irányelveit illetően megállapítható, hogy a kockázatértékelés és a kockázatmenedzsment szerepét kiemeli, a minősített adatot kezelő informatikai rendszerek teljes életciklusára kiterjedő folyamatok, feladatok részletes szabályozását várja el. Kockázatértékelési módszertan választását illetően nem tartalmaz megkötéseket, ugyanakkor megalapozott módszertant vár el, illetve automatizált kockázatértékelő szoftver alkalmazását javasolja.

Az automatizált kockázatértékelő szoftverek előnyei:

- könnyű rögzítés, módosítás és hozzáférés az adatbázisokban tárolt összeállított kockázatértékelő információkhoz;
- képes szemléltetni azokat a hatásokat, melyek tárgyi eszközök vagy információvagyon elvesztéséből erednek, ellenintézkedések kombinációinál;
- segítségükkel gyorsan bevihetünk változásokat a kockázati környezetbe és azonosíthatók a változások a szervezet kockázati pozíciójában.

A fenti munkához nyújt támogatást a NATO AC/35-D-1020 (Áttekintés a CIS-ek fenyegetéseinek jellegéről és mértékéről és CIS-ek sebezhetőségéről) dokumentum. Figyelemmel arra, hogy ez NATO „Korlátozott terjesztésű!”, nyílt publikációban nem elemezhető.

KOCKÁZATÉRTÉKELÉS ÉS KOCKÁZATMENEDZSMENT FOLYAMATAI

Minősített adatot kezelő kommunikációs és információs rendszerek kockázatértékelés és kockázatmenedzsment végrehajtásához a legjobb alapokat a NATO biztonsági politika, irányelvek és útmutatások adják, melyek a nemzeti és EU minősített adatok komplex védelmét biztosító intézkedések kialakítására is jól alkalmazhatók. A NATO INFOSEC menedzsment irányelve rögzíti, hogy a kockázatértékelési és a kockázatmenedzselési eljárásokat közösen kell végezniük a CIS elektronikus információbiztonságát tervező és kivitelezéséért felelős (ök) nek, a működtetéséért felelős(ök)kel, a biztonsági felügyelettel, valamint a projekt tagokkal és a biztonságot jóváhagyó hatósággal/hatóságokkal.

A kockázatértékelési és kockázatmenedzselési eljárásoknak követnie kell a strukturált megközelítést (kivitelezhető mind manuálisan, mind automatizált eszközökkel) és tartalmaznia kell a következő szakaszokat:

- a kockázatértékelés hatókörének és célkitűzéseinek meghatározása;
- a tárgyi eszközök és az információvagyon azonosítása;
- a tárgyi eszközök és az információvagyon értékének meghatározása;
- a meglévő ellenintézkedések azonosítása;
- a szükséges ellenintézkedések meghatározása, összehasonlítása a meglévő intézkedésekkel;
- a kockázatot és a javasolt ellenintézkedések felülvizsgálata;

- kockázatkezelési (kockázatmenedzselési) jelentés elkészítése, mely tartalmazza a végrehajtandó ellenintézkedések leírását és a fennmaradó kockázat leírását. [6.]

A kezdeti kockázatértékelésből származó információkat meg kell őrizni és alapul kell használni a jövőbeli frissítésekhez, az újraértékelések követelményeinek összhangban kell lennie a biztonságot jóváhagyó hatóság/hatóságok követelményeivel, vagy amint az egyeztetve lett a biztonsági jóváhagyó vagy akkreditáló eljárásban.

Kockázatértékelési eljárás

A kockázatértékelés az eljárás azonosítja a CIS-ek biztonsági kockázatait, azaz fenyegetettségüket és sebezhetőségeiket, meghatározza nagyságukat és meghatározza, hogy mely területeken szükséges a biztosítás megerősítése vagy ellenintézkedés. A kockázatértékelés hozzájárul ahhoz a döntéshez, hogy mely biztonsági intézkedéseket kell megkövetelni, és hogy ezek technikai vagy más biztonsági intézkedések egyensúlyával hogyan valósíthatók meg, és elfogulatlanul értékeli a fennmaradó kockázatot. A kockázatértékelésből származó haszon a fokozott/megnövekedett biztonsági tudatosság, amelynek nyilvánvalónak kell lennie minden szervezeti szinten a felső vezetéstől a működtetésen át a kisegítő személyzetig bezáróan. Mivel azok a biztonsági intézkedések, amelyeket a CIS rendszer bevezetésekor határoznak meg bizonyítottan hatékonyabbak, mint azok, amiket később hoznak meg, a kezdeti kockázatértékelést végre kell hajtani a projekt kezdeti tervezési szakaszában és nagyobb részletességgel ki kell terjeszteni, amikor a követelmény meghatározások szövegezésre kerülnek.

A kockázatértékelés, mint feladat nem zárható le véglegesen egy rendszer bevezetésekor. Időszakosan végre kell hajtani azon követelmények szerint, melyeket a biztonsági jóváhagyás vagy akkreditációs eljárás során elfogadásra kerültek, annak érdekében, hogy naprakészen viszonyuljon a változó fenyegetettséghez és sebezhetőségekhez, valamint a szervezet küldetéséhez, információvagyonához, létesítményeihez és eszközeihez. Fő erőforrása az idő és a képzett munkaerő, valamint lehetőség szerint egy automatizált kockázatértékelő eszköz (szoftver) mely megalapozott módszertant alkalmaz. Gyakorlati tapasztalataink alapján a projektek vagy szervezetek első kockázatértékelése igényli a legtöbb erőforrást. Megállapítható, hogy a kockázatértékelésre fordítható erőforrásoknak arányosnak kell lennie a célokkal.

A NATO irányelvek szerint a kockázatértékelés sikere nagyban függ a felső vezetés szerepétől az eljárásban. Vezetői egyetértésnek kell lennie a kockázatértékelés céljaira és hatókörére vonatkozóan, kinyilvánítva, hogy azt a szervezeten belül minden szinten támogatja, ezen túl a vezetésnek felül kell vizsgálnia és jóvá kell hagynia a kockázatértékelés eredményeit.

A kockázatmenedzsment

A kockázatmenedzsment foglalkozik a kockázat kezelésének lehetőségeivel, amely lehet a csökkentés, az áthárítás, a megszüntetés, az elkerülés és az elfogadás. A kockázatot csökkenti a jól szervezett rendszer architektúra, ahol hatásosak a fizikai biztonsági, személyi biztonsági, információbiztonsági és INFOSEC intézkedések. A kockázatmenedzsment magába foglalja a tervezését, szervezését, irányítását és felügyeletét az erőforrásoknak, biztosítva hogy optimális költségeknél a fennmaradó kockázat elfogadható mértékű legyen. A kockázatmenedzsment olyan együttműködési folyamat, amelyet a különböző érdekcsoportok képviselői közösen dolgoznak ki, megértve és mérlegelve a követelményeket és a lehetőségeket. Meggyőződésünk, hogy az így kialakuló fokozott tudatosság erősíteni fogja a biztonságot és jobban megfelel a felhasználói igényeknek.

Irányadó szakemberek szerint és álláspontunk szerint is, a CIS rendszerek kockázatmenedzsmentjénél különös nehézséget jelent a kockázati tényezők dinamikus jellege

és a gyors technológiai fejlődés. Ha a biztonsági kockázatok hibásan nem a megfelelő módon és időben kerülnek felismerésre, szükségtelen, hatástalan költséges intézkedéseket eredményezhetnek.

A kockázatértékelési eljárás kimenete (eredménye) tartalmazza azokat a részleteket, amelyeket bele kell foglalni a biztonsági dokumentációba, amely megkövetelt a biztonsági védelmi intézkedések jóváhagyási vagy akkreditációs eljárásnál (pl. a rendszer specifikus rendszerbiztonsági követelmények szövegezése egy konkrét CIS-re).

Kockázatértékelés és kockázatmenedzselés a CIS-ek életciklusában

A CIS tervezés során kell a kockázatértékelési követelményeket és az alkalmazandó kockázatértékelési és kockázatmenedzselési módszertant meghatározni (felelős szerve – biztonsági felügyelet, koordinálva a CIS tervező szervvel és projekt munkatársakkal.) Majd meg kell kezdeni a kezdeti kockázatértékelést a biztonsági felügyelet követelményei szerint (felelős szerv – CIS tervező szerv/projektcsapat (az INFOSEC technikai és kivitelezési szempontjaiért), koordinálva a biztonsági felügyelettel). Ezt követi a kezdeti kockázatértékelés eredményének jóváhagyása (felelős szerv – biztonsági felügyelet.

A CIS tervezés és beszerzés során aktualizálni kell a kockázatértékelést a biztonsági felügyelet követelményei szerint (felelős szerv – CIS tervező szerv/projektcsapat, kapcsolatot tartva a biztonsági felügyelettel), következő lépcső a finomított kockázatértékelés eredményének jóváhagyása (felelős szerv – biztonsági felügyelet).

A CIS kivitelezés és biztonsági jóváhagyás/biztonsági akkreditáció során kell meghatározni és megegyezi az elfogadható maradék kockázatokról (felelős szerve – biztonsági felügyelet, kapcsolatot tartva a CIS üzemeltetéséért felelős szervvel), a folyamatos kockázatmenedzsment eljárásairól (felelős szerve – biztonsági felügyelet, kapcsolatot tartva a CIS üzemeltetéséért felelős szervvel).

A CIS működtetés során végre kell hajtani a folyamatos kockázatmenedzsment eljárásait (felelős üzemeltetéséért felelős szerv, kapcsolatot tartva a biztonsági felügyelettel).

A CIS bővítésekor pontosítani kell a kockázatértékelést a biztonsági felügyelet követelményei szerint (felelős szerv – CIS tervező szerv/projektcsapat, kapcsolatot tartva a CIS működtető szervvel és a biztonsági felügyelettel), következő lépcső a finomított kockázatértékelés eredményének jóváhagyása (felelős szerv – biztonsági felügyelet) követ. Felül kell vizsgálni és meg kell egyezni az elfogadott maradvány kockázatról (felelős szerv – biztonsági felügyelet, kapcsolatot tartva a CIS üzemeltető szervvel), valamint a folyamatos kockázatmenedzsment eljárásairól (felelős szerv – biztonsági felügyelet, kapcsolatot tartva a CIS működtető szervvel).

A kockázatértékelés menedzsmentje

A kockázatértékelés sikeressége nagyban függ a felső vezetés projektben betöltött szerepétől, ezért szükséges hogy:

- a felső vezetés kinyilvánítsa a projekt támogatását a szervezet minden szintjén;
- a felső vezetés egyetértsen a kockázatértékelés célkitűzéseivel és hatókörével;
- a felső vezetés szakértői kockázatértékelés és kockázatmenedzselés felügyeleti munkacsoportot hozzon léte hivatalos megbízással a hatáskörére és a felelősségére;
- a felső vezetés felügyelje és hagyja jóvá a megállapításait a kockázatértékelő munkacsoportnak és a felügyeleti munkacsoportnak.

A kockázatértékelés tervet úgy kell kialakítani, hogy minimálisan az alábbi szempontokat tartalmazza:

- a CIS rendszer bemutatását;
- a kockázatértékelés hatókörét és célkitűzéseit;

- a kockázatértékelésnél alkalmazott módszertant;
- a kockázatértékelés menedzsmentjét, beleértve a kockázatértékelő munkacsoport és a felügyeleti munkacsoport létrehozását, a jelentések követelményeit.

A kockázatértékelési tervet a CIS tervező és kivitelező szervnek/CIS működtető szervnek/projektcsapatnak kell szövegbe foglalnia, jóváhagyni a biztonsági felügyeletnek kell.

A kockázatértékelő munkacsoport és a vezetés felülvizsgálati munkacsoportja

A kockázatértékelő munkacsoportot személyi, fizikai, adminisztratív és elektronikai biztonságért felelős szakterületeket képviselő szakemberekből szükséges összeállítani, akik saját szakterületük komplex védelemre gyakorolt hatását illetően is felkészültek. A NATO irányelvei szerint a munkacsoport vezetőjét és tagjait a kockázatértékelés végrehajtása alatt teljes munkaidőben e feladatra kell foglalkoztatni. Külső szolgáltatók bevonhatók a kockázatelemzésbe a hatékony erőforrás felhasználás érdekében, ugyanakkor a szervezeteknek maguknak is tisztában kell lennie a kockázatértékelés folyamataival. A kockázatértékelés időigényes folyamat, amit nem szabad siettetni, korábbi tapasztalatok, illetve korábbi kockázatértékelésből származó információk nagyban támogatják a kockázatértékelés eredményeit. Tapasztalati tény, hogy sokszor a munkacsoport tagjaira nyomást gyakorol az őket delegáló szervezeti egység, sietteti őket, hogy térjenek vissza napi munkafolyamataikhoz, ezért súlyponti kérdés az, hogy a kockázatértékelésre fordított erőforrásokat gondosan tervezzük.

A vezetés felülvizsgálati munkacsoportjának hatásköre és felelőssége mind a kezdeti mind a finomított kockázatértékelés eredményének (kimentének) felülvizsgálata és jóváhagyása. Annak észszerűségét, szervezeti információbiztonsági politikához és szervezethez igazodását szükséges felülvizsgálnia. A felülvizsgálati munkacsoport felelős a végső jelentés szövegezésért és elfogadásáért, mely a szervezet felső vezetése és a biztonságot jóváhagyó hatóság számára szükséges előállítani.

A kockázatértékelési eljárás

A kockázatértékelési eljárás egy adatgyűjtő és értékelő gyakorlati eljárás, amely két alapvető kérdéssel foglalkozik:

- mi az értéke a kockázatértékelés tárgyának;
- mi valószínűsége a hatásnak vagy következménynek, mely azonosított fenyegetések bekövetkeztéből ered.

Célja tehát meghatározni egy CIS biztonsági profilját, a kockázatokkal arányosan. A kimenete a kockázatértékelésnek egy biztonsági stratégia mely gondoskodik a CIS elemeinek (értékek) megfelelő védelméről.

A kockázatértékelési eljárás tartalmi elemeit illetően az alábbi lépésekre bontható:

- meghatározni a hatáskörét és célját a kockázatelemzésnek, a céljáról egyeztetni kell a CIS INFOSEC tervező és végrehajtó szervnek/ CIS működtető szervnek/ biztonsági menedzsmenttel/projekttagoknak és a biztonsági felügyeletnek
- Meghatározni a tárgyi eszközöket és információvagyont, melyek hozzájárulnak egy CIS feladatának teljesítéséhez vagy egy szervezeti küldetés teljesítéséhez.
- Meghatározni az értékét a tárgyi eszközöknek, beleértve a hardvert, szoftvert, a környezetben alkalmazott berendezéseket és kapcsolódó dokumentációt.
- Meghatározni az értékét az információvagyonnak a következő hatásokra: közzétételük, módosulásuk, elérhetetlenségük, megsemmisülésük.

- Azonosítani a fenyegetéseket és sebezhetőségeket a kockázati környezetben, és azok szintjét
- Azonosítani a létező ellenintézkedéseket.
- Meghatározni a szükséges ellenintézkedéseket és összehasonlítani a meglévő ellenintézkedésekkel, azonosítani a már meglévő ellenintézkedéseket, meghatározni a javasolt ellenintézkedéseket.
- Felülvizsgálni a kockázatot és az javasolt ellenintézkedéseket, figyelembe véve a következő lehetőségeket, megfelelve a szabványos védelem minimumkövetelményeinek:
    - kockázat megszüntetése: a cél teljesen kiküszöbölni a valós vagy potenciális sebezhetőségeket, teljes körű ellenintézkedések végrehajtásával;
    - tárgyi eszközök és információvagyon káreseményeinek elhárítása: a cél olyan ellenintézkedések bevezetése, melyek megelőzik a kárt amennyire csak lehetséges;
    - tárgyi eszközök és információvagyon káreseményének minimalizálása: a cél olyan ellenintézkedések bevezetése melyek a káresemények hatásait elfogadható szintre csökkentik;
    - tárgyi eszközök és információvagyon káresemény kockázatának elfogadása: lehet olyan döntés, ami elfogad egy kockázatot és következményeit, például ha a káreseménynek a költsége/hatása nem jelentős, vagy a káresemény kockázata elég kicsinek ítélt, vagy az ellenintézkedések költsége sokkal magasabb, nem arányos a káresemény költségével/hatásával.
- Kockázatmenedzsment jelentés elkészítése, amely tartalmazza a megvalósított ellenintézkedések leírását és a fennmaradó kockázat leírását.

Elsőként a kockázati környezet meghatározásánál meg kell szerezni a rajzokat és vázlatokat az adott esthez kapcsolódó szervezeti létesítmények fizikai elrendezéséről. Emellett rajzot kell készíteni az elektromos hálózat, fűtés, szellőztetés és légkondicionálás berendezéseiről. Sokat ezek közül csak egyszer a kezdeti kockázatelemzéskor kell elkészíteni, és a későbbiek során lehet, hogy kevésbé kell aktualizálni. A kockázati környezetben minden fizikai eszközt és információvagyont azonosítani kell és fel kell jegyezni.

Ezt követi az információvagyon értékének megállapítása. A tárgyi eszközök (hardver, szoftver, környezetben alkalmazott berendezések és kapcsolódó dokumentációik) értéke azok cseréjének vagy helyreállításának költsége. Az információvagyon értékét az adatgazdával, vagy az információvagyont ismerő meghatalmazott illetékesekkel, folytatott interjú alapján lehet megállapítani. Az érték megállapításának, mely lehet minőségi tényező is (például alacsony, közepes vagy nagy), az adatgazdától vagy képviselőjétől kapott tájékoztatásból kell származnia, értékelve az információvagyont ért alábbi, legrosszabb forgatókönyv bekövetkezte esetén ért, hatásokat:

- megsemmisülése;
- elérhetetlensége;
- illetéktelken személy általi megismerése;
- illetéktelken személy általi módosítása.

Következő lépésben a kockázatértékelő munkacsoportnak kezdeti konzultációt célszerű folytatnia az illetékes biztonsági jóváhagyóval (biztonsági vezetővel) vagy akkreditációs hatósággal, hogy naprakészre frissítsék ismereteiket a kockázatértékelésben, és szerezzenek

egy átfogó listát a lehetséges sebezhetőségekről. Ezen felül más helyi kockázatértékelése megszerzése a megfelelő hatóságoktól szintén előnyös lehet a kockázatértékelő munkacsoport számára. A kockázatértékelésnek foglalkoznia kell a szándékos fizikai és elektronikai támadási fenyegetettségekkel, és tartalmazniuk kell a természeti katasztrófák fenyegetettségeit is, például tűz, árvíz, villámkár, vihar, földrengés (NATO minősített adatok esetén ehhez már a AC/35D1020 dokumentum alkalmazása is követelmény.) A potenciális sebezhetőségek átfogó listájának, minden elemével kell foglalkoznia az adott kockázati környezetben, és értékelést kell készíteni a potenciális sebezhetőségek bekövetkeztének valószínűségéről. Ez végrehajtható a létesítmény tényeges felmérése alapján vagy a megfelelő személyekkel folytatott interjúkkal.

Ezt követően azonosítani és dokumentálni kell a létező ellenintézkedéseket (személybiztonság, fizikai biztonság, információbiztonság, iparbiztonság, INFOSEC területén levő).

Miután meghatározásra (azonosításra) került a kockázati környezet minden tárgyi eszköze, teljes információvagyona és azok értéke, a következő lépés meghatároznia a javasolt ellenintézkedéseket. Ezt történhet úgy, hogy megvizsgálunk minden egyes tárgyi eszközt, és az információvagyon elemeket vagy csoportosíthatjuk is ezeket, tanulmányozva a fenyegetéseket és sebezhetőségeket, valamint meghatározni az ellenintézkedés (eke)t. Vagy fordítva úgy, hogy azonosítunk minden egyes fenyegetést és sebezhetőséget és azokhoz rendeljük azokat a tárgyi eszközöket és információvagyon elemeket, melyeket érinthet, és utána meghatározzuk a biztonsági ellenintézkedést. Meg kell azonban jegyezni, hogy csak azon fenyegetéseknek van jelentősége, melyeket érintően van olyan sebezhetőség, amelyet kihasználhat egy csapás (szándékos vagy természeti). Fordítva, egy sebezhetőség csak akkor válik jelentőssé, ha van olyan fenyegetettség, ami kihasználhatja azt a sebezhetőséget.

Az ellenintézkedések meghatározásához figyelembe kell venni, hogy a minimális szabványelőírások hazai és külföldi minősített adatok kezelésénél is meghatározottak. A Mavtv. rendelkezik arról, hogy a minősített adatok nyilvánosságra hozatalának, jogosulatlan megszerzésének, módosításának vagy felhasználásának, illetéktelen személy részére hozzáférhetőségének, valamint az arra jogosult részére hozzáférhetetlenné tételének kárértéke alapján kell a minősítési szintet („Korlátozott terjesztésű!”, „Bizalmas!”, „Titkos!”, „Szigorúan titkos!”) megállapítani. A „Szigorúan titkos!” minősítési szintű, minősített adatok bizalmasságának, sértetlenségének és rendelkezésre állásának kompromittálódása súlyosan veszélyeztetheti többek között a nemzet biztonságát, jelentős érdekeit vagy nagyszámú emberéletet.

A folyamat eredménye ként képződik egy lista a biztonsági ellenintézkedésekről melyet összehasonlítunk a meglévő ellenintézkedésekkel és ebből származtatjuk a javasolt ellenintézkedések halmazát. A folyamat utolsó szakaszaként felül kell vizsgálni a kockázatokat és a javasolt ellenintézkedéseket. Ezt a műveletet közösen kell végeznie a projekttagoknak, az adatgazdáknak, a CIS működtető szervnek és a biztonsági felügyeletnek vagy az akkreditáló hatóságnak.

Amikor a kockázatértékelés befejeződik és egyezség születik a végső ellenintézkedések halmazáról, a kockázatértékelés eredményét és a kockázatértékelési eljárás végrehajtásából származó lényeges információkat bele kell foglalni a biztonsággal kapcsolatos dokumentációba (pl. rendszer specifikus biztonsági követelmények ismertetése dokumentum, rendszer-összekapcsolások biztonsági követelményeinek ismertetése)

Kockázatkezelési jelentés

A kockázatértékelés befejezéséhez egy kockázatkezelési (kockázatmenedzsment) jelentést kell készíteni, a következő szempontok szerint:

- kockázatértékelés célja és hatóköre;

- a kockázat értékelési módszertan és a terv;
- az azonosított eszközállomány (tárgyi eszközök és információvagyon), hatások, fenyegetések és sebezhetőségek
- a minimumkövetelményeknek való megfelelésre;
- az elfogadott fennmaradó kockázatokat;
- a folyamatos lévő kockázatmenedzselési folyamatokat.

A kockázatértékelési eszközöknél körültekintően kell ellenőrizni, azt hogy alkalmasak-e a tervezett feladatra, a kockázatértékelő eljárásban levő végleges használatuknak vezetői döntés tárgyának kell lennie.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Napjainkban egyre több területen válik az információ a legfontosabb és legértékesebb erőforrássá, az alkalmazásukat támogató informatikai rendszerek és infrastruktúrák szolgáltatásaitól egyre jobban függ a társadalom, ezzel egyidejűleg ezek emberi mulasztásból, környezeti katasztrófából, vagy szándékos támadásból eredő kárai egyre súlyosabbak mértékűek lehetnek, melyeket általános és minősített adatok kezeléséhez kapcsolódó példákkal szemléltettünk. Ezek megelőzése érdekében komplex – személyi, fizikai, adminisztratív és elektronikai – védelmi intézkedések alkalmazása szükséges, amely hazai és külföldi minősített adatok informatikai rendszeren történő kezelésénél követelmény, és jogszabályokban van meghatározva.

Megállapítató, hogy mind a nemzeti és külföldi minősített adatok kezelésére vonatkozó jogszabályok is kötelező elemként határozzák meg a kockázatértékelést, fontos elemét képzik a CIS-ek biztonsági követelményeinek, a biztonsági dokumentáció részeként szövegbe foglaltan előírtak.

Kijelenthető, hogy a NATO a minősített adatokat kezelő rendszerek komplex védelmének érdekében a kockázatértékelés és kockázatmenedzsment szerepét súlyának megfelelően kezeli, szigorú követelmények határoz meg, azok megvalósítását biztonsági politikája, irányelvei, útmutatásai kellő mértékben segítik.

Az EU minősített adatok védelmét szolgáló új szabályozásában a leghangsúlyosabb új elemek a kockázatértékeléshez kapcsolódnak, követelményeit kellő mértékben részletezi, ugyanakkor folyamataira nem ad olyan részletes útmutatást, mint a NATO-s biztonságpolitika, és az azt támogató számos irányelv és iránymutatás.

Tekintettel arra, hogy a kockázatértékelés és kockázatmenedzsment NATO-ban alkalmazott gyakorlata összhangban van a hazai és EU-s követelményrendszerrel is, a cikk súlyponti részét képezően ezt ismertettük legrészletesebben. Megállapítható, hogy az alkalmazott eljárásrend, amely NATO minősített adatok vonatkozásában most is kötelező, a nemzeti és EU minősített adatokra vonatkozó követelmények teljesítéséhez is jól alkalmazható, az a gyakorlatban is megvalósítható. E munka sikeressége nagyban függ a felső vezetés elkötelezettségétől, ezért a szakterületi vezetők fontos feladata, hogy jelentőségét kellően tudatosítsák. Végrehajtása a személyi, fizikai, adminisztratív és elektronikai biztonsággal foglalkozó szakemberek munkacsoportban történő együttműködését igényli.

A megfelelő anyagi erőforrások biztosításán túl fontos, hogy erre a védendő rendszer fontosságával és kritikusságával arányos kellő időkeret legyen biztosítva. Ennek eredménye ként kielégítő egyensúly teremthető a felhasználók igényei, a költségek és a maradvány biztonsági kockázatok között. Fontos, hogy a megvalósítandó ellenintézkedések nyomán fennmaradó biztonsági maradványkockázatokról a felső vezetés pontos információkat kapjon, és az ellenintézkedések megvalósulása a biztonságot akkreditáló hatóság által elfogadott követelmények alapján folyamatos kockázatmenedzsmentben biztosítva legyen.

A szükséges és elégséges mértékű befektetett anyagi erőforrásokon túl, a kockázatértékelési munkába befektetett erőfeszítések és szakértelem jelentőségét nem szabad lebecsülni, mert az pozitív hatással van a projekt eredményességére, a teljes beruházási költségekre és az időkeretre is.

Felhasznált irodalom

[1] Haig Zsolt: Az információbiztonság komplex értelmezése. Hadmérnök különszám, Robothadviselés 6. tudományos szakmai konferencia 2006. november 22. http://hadmernok.hu/kulonszamok/robothadviseles6/haig_rw6.html

[2] Közigazgatási és Informatikai Bizottság 25. számú ajánlása. Magyar Informatikai Biztonsági Ajánlások, http://www.ekk.gov.hu/hu/kib/ajanlasok

[3] Fekete Gizella: A katasztrófa utáni helyreállítási stratégia újragondolása. Business Online, 2008. február 24., http://bonline.hu/cikk/65920/

[4] Dajkó Pál: Támadás érte az USA hadiipari beszállítóinak biztonsági rendszereit. IT Café, 2011. május 28. http://itcafe.hu/hir/usa_lockheed_martin_emc_rsa_securid_hacker_cracker.html

[5] Muha Lajos: Kiberháború az orosz-észt viszony kapcsán. Hacktivity konferencia, 2007. 09. 22-23.

[6] David E. SANGER, Elisabeth BUMILLER: Pentagon to Consider Cyberattacks Acts of War. New York Times, 2011. május 31. http://www.nytimes.com/2011/06/01/us/politics/01cyber.html?_r=1

[7] 2009. évi CLV. törvény a minősített adat védelméről

[8] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

[9] A Tanács határozata (2011. március 31.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (2011/292/EU)

[10] Security Within The North Atlantic Treaty Organisation (NATO) (C-M(2002)-49). North Atlantic Council, http://www.nbf.hu/anyagok/jogszabaly/C-M(2002)49.pdf

[11] Primary Directive on INFOSEC (AC/35-D/2004-REV2), NATO Security Committee

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Vizi Pál
vizip@rmki.kfki.hu

OKOSTELEFONOK BIZTONSÁGI KIHÍVÁSAI

Absztrakt

A haditechnika egyik legfontosabb és legérdekesebb kérdése a számítógépes hálózatok folyamatosan fejlődő eszközei biztonságos alkalmazásának megteremtése. A cikk kitér az új mobil okostelefonok gerjesztette kihívásra és megoldásra. A szerző áttekinti az eredményeket, a vizsgálati és kutatási módszerek helyét, szerepét, problematikáját a fentiek néhány kérdésében.

Designing a safe environment for a special operating place like continuously evolving computer networks and implementation is one of the very important and interesting questions of military engineering technology. Subject of this article is about some Smartphones generated challenges and solutions. The author gives an overview about methods, results of checking up, the system of research works and problems in point of view of some problems of above described questions.

Kulcsszavak: *okostelefon, mobil számítógépes hálózatok ~ smartphones mobile computer networks*

BEVEZETÉS

Szerző ebben a cikkében röviden összefoglalja a számítógépes hálózatok és azok támadásának újdonságait, különös tekintettel a globális méretű mobil Internettel ellátott okostelefonokra. Bemutatja az új eszközöket, azok lehetőségeit és arányát a számítógépes hálózatokban. Igyekszik összegyűjteni az új állapot alakította kihívásokat és ezek kutatási irányát. Megoldásokat keres és próbál nyújtani a felmerült veszélyekre.

SZÁMÍTÓGÉPES HÁLÓZATOK TÁMADÁSA

A számítógépes hálózatok támadása a számos különböző esetben szerepel szakirodalomban. A különféle diszciplínák alapvetően hasonlóan, de a saját specialitásuknak megfelelően értelmezik a témakört.

Az evolúcióban a támadás, a térnyerés a túlélés egyik feltételeként azonosított. Ha matematikai modellen leegyszerűsítjük támadóra és támadottra, akkor a klasszikus a róka-nyúl differenciálegyenlet-rendszer alapján a korlátlan támadó jelleg nem kifizetődő az egymástól globálisan függő, egymással szimbiózisban élő populációban. Tehát a világ, az emberiség jelen történelmi álláspontja szerint a támadást a jog alapvetően bűncselekménynek vagy katonai eszköznek tekinti. A támadás tárgya jelen esetben a számítógépes hálózatok.

A rendőrségi bűnmegelőzés szempontjából definiálva a számítástechnika szerepe a bűnözésben lehet:

- hagyományos bűncselekmények végrehajtása;
- digitális adattartalmak jogszerűtlen felhasználása;
- informatikai eszközök manipulálása;
- számítógépes hálózatok támadása.

A számítógépes hálózatok elleni támadás szereplői a jótól a rossz felé haladva az etikus hackerek, hackerek, crackerek. Céljuk a jogosulatlan belépés, adatok megszerzése (hacker) vagy ezen lehetőségek felderítése (etikus hacker), illetve rosszabb esetben adatok megváltoztatása, törlése és tönkretétele (cracker)

- információk megszerzése kémkedési céllal;
- vagyoni haszonszerzés jogosulatlan banki átutalással;
- vagyoni károkozás adatok törlésével;
- erkölcsi károkozás honlapok megváltoztatásával. [1]

A katonai szempontok szerint definiálva:

Számítógép-hálózati hadviselés helye az információs műveletekben a következőkkel írható le. A védelmi szektorban az információt két területen alkalmazzák. Egyrészt az információt, mint a vezetés eszközét használják fel a hadviselésben, másrészt az információt, mint un. nem kinetikus energiát felhasználó „fegyvert” alkalmazzák az információs műveletekben. Az információs műveletek alkotóelemei a következők:

- műveleti biztonság;
- katonai megtévesztés;
- pszichológiai műveletek;
- információs infrastruktúrák, vezetési objektumok fizikai pusztítása;
- elektronikai hadviselés;
- számítógép–hálózati hadviselés;

Kapcsolódó elemei pedig:

- polgári–katonai együttműködés;
- tömegtájékoztatás.

Az összetevő elemeken kívül az információs fölény kivívásában és fenntartásában fontos szerep hárul a vezetési információs rendszerekre és az összadatforrású felderítésre, melyek az információs műveletek támogató elemeit jelentik. [2]

A számítógépes hálózatok támadását, mint más hasonló információs műveletet komoly törvényi, jogi háttér szabályozza. Normál esetben jogszabályba ütköző tevékenységet végrehajtani, például lehallgatni csak szigorú törvényi feltételek mellett, az erre esetileg feljogosított állami szervek lehetnek jogosultak és az adatkezelés szintén szigorú előírásai vonatkoznak rájuk.

Napjaink új kihívása azonban az okostelefonok és a mobil számítógépes hálózatok kihasználása, exploitja.

OKOSTELEFONOK – SMARTPHONES, MINT A SZÁMÍTÓGÉPES HÁLÓZATOK TÁMADÁSÁNAK ÚJ ESZKÖZEI

Napjainkban a következő okostelefonok terjedtek el. Az egy gyártótól (Apple) származó IPhone, IPad és IPod termékek. Ezek arányaikban drágák. A több gyártótól származó hardveren egységesen működő Google Android nyílt rendszer alapú okostelefonok, relatíve olcsóak. Vagy a Microsoft zártabb rendszerű Windows Mobile verziói és a Symbian operációs rendszer, amely jellemzően napjainkra a Nokia készülékeken fut és valószínűleg a Microsoft fogja uralni ezt a terepet. Valamint a BlackBerry rendszerű mobilkészülékek, amelyek kellő biztonsággal rendelkezhetnek, de ennek ára van, amelyet a jó ár/teljesítmény igényű piac szűk része értékelhet, de mintha elrohanni látszana a többi megoldás a BB mellett.

Az jó ár/teljesítmény arány miatt tehát várhatóan a legdinamikusabban az Android rendszerek terjednek el. Bár a cikk írásának idején az Oracle pert indított a Google ellen az Android operációs rendszerben felhasznált, a Google állítása szerint részben nyílt rendszerként, részben licencszelt Sun Java alkalmazások kerültek beépítésre. [3] Az Oracle vásárolta fel a Sun-t és így a Java platform tulajdona is a kezébe került. [4] Bármi legyen is a per kimenetele, a legalább részben nyílt rendszerű operációs rendszer tűnik jelenleg nyerőnek. Annak ellenére, hogy a Microsoft a SkyPe felvásárlása után a Nokiával kötött szerződésével is legfeljebb a második lehet. [5] A nyílt rendszer jellemzője, hogy döntően több szoftver készül rá, és ezek jobban elérhetőek. A továbbiakban tehát az Androidon futó programok kerülnek górcső alá. Funkciójukban hasonló, vagy teljesen azonos szoftverek a többi operációs rendszereken is létezhetnek.

ANDROID PROGRAM ESZKÖZÖK

Hálózat szkenner

A Network Mapper program a szerzők szerint egy nagyon gyors szkenner hálózati adminisztrátorok részére, amely átvizsgálja a hálózatot az irodában és egy CSV fájlként exportálni tudja GMail-en keresztül, feltérképezi, hogy milyen eszközök vannak a LAN-on.

Tartalmaz egy portscannert biztonsági audit ellenőrzésére és egy MAC adatbázist a NIC gyártók azonosítására. Észlelni képes a tűzfallal ellátott és rejtőzködő számítógépeket. Nagyon hasznos, ha meg kell keresni egy windows/tűzfalat, ami nem látható a hálózaton. Előnyös, ha FTP, SSH, SMB stb. szervereket kell megtalálni a hálózaton, és segít diagnosztizálni a hibákat. A vizsgálat eredményeit, mint egy CSV fájlt lehet elmenteni,

amelyet Excel / OpenOffice / LibreOffice programokba lehet importálni. A leírása szerint „Azért készült, hogy gyors és megbízható legyen. Nem dob el semmit, és meg tud birkózni a 3G hálózatokkal is” [6]

Az erősáramú hálózatokban és a kismegszakítós biztosítóval rendelkező kis és nagyfeszültségű hálózatokban alkalmazott szakaszolás módszerével egy konkrét IP és MAC című gép megkereshető. Nem feltétlenül az Android Network Mapper fog ebben jeleskedni, de kisebb hálózati problémák megoldására alkalmas segédeszköz lehet.

Kamera programok

Valós idejű közvetítés - SECuRET Camera WiFi LiveStream

Video kamera stream közvetlenül egy okostelefonról, amely a Wi-Fi hálózaton valós időben nézhető és távolról irányítható egy web böngésző segítségével. Reklámja szerint használható baba felügyeletre, komolyabb felügyeleti eszközként vagy egyszerűen csak a móka kedvéért! Illetve, amit a leírás is tilt, illegális tevékenységre.

Adatfolyam valós idejű közvetítés egy Android telefon kamerájáról egy webböngészőre. Használata egyszerű mindenki számára, mert semmilyen konfigurációs beállítások nem szükségesek. A kamera vezérelhető, az állóképek vagy mozgó videók a böngésző segítségével készíthetők, érhetők el és letölthetőek. Java felületet igényel. Számos további beállítással testre szabható, a választható felbontás a 320x200 képponttól a kamera maximális felbontásáig terjed. A jelen változatot csak WiFi hálózathoz hirdetik, de a LogMeIn, a TeamViewer IP cím független protokolljainak ismeretében a saját vagy harmadik féltől származó fejlesztők a teljes Internetre kiterjeszthetik az elérési lehetőséget. További funkciók fejlesztés alatt, beleértve hang közvetítését.

Képes álcázott működésre érintőképernyő zár funkcióval, így a valódi működés nem észlelhető. Ez a már beépített funkció okozhat kellemetlenséget illetéktelen felhasználás esetén. A Livestream alkalmazás elérhető az Android Marketen is. [7]

Titkos exponálás - Super Spy Camera+

A fejlesztő célja egy olyan kamera program volt, amely nem árulja el a felvétel készítőjéről, hogy képet vagy videó felvételt készít. Az okostelefon normál képernyőjének mutatása közben ikonméretnyi vezérlőgombokkal és áttekintő képpel operál. Zárhangot sem ad ki. A képeket nem a szokásos DCIM alkönyvtárban tárolja, hanem egy véletlen elnevezésű és mélységű alkönyvtárban, amelyről azért tájékoztatja a felhasználóját. A „védelem” eme foka természetesen csak ez egyszerű kíváncsi szemek elől titkolja el a foto anyagot. [8]

A lopakodó működés miatt a fejlesztő a honlapján ki is zár minden jogtalan felhasználásból eredő felelősséget.

Vonalkód és eltérítés - Barcode

Barcode Scanner El tudja olvasni a hagyományos ár vonalkódokat, a kétdimenziós mátrixkódokat (UPC-A és UPC-E, EAN-8 és EAN-13, Code 39, Code 128, QR kód, Data Matrix, PDF 417, ITF) Segítségével megoszthatók a kapcsolatok, alkalmazások, könyvjelzők a QR-kód segítségével. A kapcsolatok megosztása engedély köteles. [9]

Veszélye, kihívása a vonalkód reklám eltérítés például nyomtatott fali reklámok eseten a plakát saját kódjának átmatricázásával. A támadó saját céljára irányit, ami lehet saját oldal. Vagy akár lejárató cél, azaz a támadó ellenfele oldalára ugrat. Azt akarja elérni, hogy pl. eljárás induljon az ellenfelével szemben. A matricák elhelyezése megvalósulhat leolvasást imitálva, vagy távolról, célba találó módszerrel, elkerülendő a lebukást a bekamerázott helyszíneken. Jelentősége a kis helyre viszonylag rövid ideig összpontosult sok potenciális leolvasó mobileszköz esetén van. Azaz például nagy létszámú ifjúsági események, sportrendezvények stb. alatt.

Távoli asztal programok

Az alább felsorolt programok a TeamViewer, LogMeIn, Remote Desktop Client for Android és a VNC client megbízható gyártóktól származó megbízható alkalmazásoknak tűnnek. A számítástechnikai történelem során számos olyan feltörést végeztek már, ahol kisebb módosításokkal betörésekre alkalmas módosítások születtek.

VNC client – hátránya, és egyben előnye, hogy közvetlen IP címekre képes eljutni, nincs mögötte egy szerverközpont, ahonnan routereken és tűzfalakon át lehetne eljutni a célgépig. A nyílt forráskódja miatt veszélyes lehet, mert rosszindulatú kezek káros irányban módosíthatnak bele.

Remote RDP (Remote Desktop Protocol) client – Teljes elérés, szöveg Copy / Paste a helyi és a távoli gép között. A lokális memóriakártya hozzáköthető a távoli számítógéphez, ahol a lokális zenefájlok a távolban lejátszhatók. A demo verzió nem jár le.

A fenti szoftverekre érvényes, hogy a tűzfalon port forwarding beállítása szükséges, viszont nincs a háttérben szerver.

DROID - VPN (Virtual Private Network) beépített Android VPN.

Xtralogic Remote Desktop Client - Távoli asztal ügyfél Androidra – billentyűzet, egér és képernyőelérés, teljes Microsoft Remote Assistance kompatibilitás. Tömörítéssel sávszélesség kímélő alkalmazás.

Wyse PocketCloud RDP/VNC – RDP, VNC vagy WMware protokollokkal képes kommunikálni

TeamViewer – létezik szerverközpont, így routereken és tűzfalakon át lehetne eljutni a célgépig, ahol nem is a célgépet érjük el közvetlenül, hanem a célgép van kifelé bejelentkezve ugyanarra a szerverre, amelyen keresztül a kapcsolat létrejön.

LogMeIn Ignition – Logmein saját accounton belül a regisztrált gépek névszerinti keresésére és belépésre biztosít lehetőséget. Teljes elérés a számítógép eszközeihez, nem csak a fájlelérések, hanem beleértve a hangcsatornákat is.

ShowMyPC Remote Support hozzáférés [10]

Veszély, hogy nem csak a nyílt forráskódúaknál várhatóak törések, amelyek szabad hozzáférést adhatnak gépekhez akár egy mobilnethez kötött izmosabb Android készüléken keresztül is.

OKOSTELEFON VESZÉLYEK

Védett WiFi – külvilág összekapcsolása

Az egyik veszély az okostelefon mobilnet szolgáltatós és belső védett wi-fi közti kapcsolódása. Ehhez többnyire célszerűen nyílt forráskódú távoli asztal programok módosításait használják, összekötve más teljesen legális programok illegális célú használatával. A felhasználható programokat a „Távoli asztal programok” fejezetben tartalmazza ez a cikk.

Az egyik legveszélyesebb lehetőség a védett hálózatok területén belül a tűzfalakon kívüli Internetre kapcsolás, routolás.

Online lehallgatás

Másik veszély az online lehallgatás, amelyet gyors reagálású döntéshozatalok eseten vethetnek be.

Alkalmas időzített megzavarásra is.

Idáig is be lehetett hallgatni mobiltelefonok közti beszélgetésekbe, különösen a 450MHz-es mobiloknál volt ez egyszerű. A hivatalos megoldás csak állami szervek számára adott, a telefon és a mobil hálózat erőforrásaival. Az internetes elérés növeli a lehetőségeket, mert a háttérben futhat egy alkalmazás vagy szolgáltatás, amely a GSM sávon folytatott beszélgetést

egyszerűen felveszi és továbbítja az Internetes elérésen, akár a beszélgetéssel egyidőben, vagy utána.

Okostelefon zombi hadsereg

Harmadik veszély egy ismert tűzfalon belüli rendszer fizikai területén belül került számos okostelefon, amelyek fel tudnak jelentkezni belső WiFi-kre vagy a külső mobil Internetre. Az elterjedtség arányai miatt zombi hadsereg leginkább Android tagokból állhat. Hosszabb idő alatt, előre megszervezetten komolyabb támadást lehetne végrehajtani néhány okostelefonnal, például egy több fős zárt ülés alatt. Megoldást jelenthet, ha az ülés alatt az okostelefonok akkumulátor nélküli állapotban a folyosón várakoznának, de a munkaszervezés miatt valószínűleg épp használatban vannak, prezentációra, naptári, előjegyzési funkciókra, jegyzetelésre, netán hangfelvételre, ha ezt engedik. Ha a hálózatról le is kapcsolják, és csak jegyzetelésre használják, az ülés végén újra rákapcsolódik a netre és a trójai programnak lehetősége van elküldeni az elmúlt időszakban rögzített anyag kivonatát.

Nagyobb veszély, ha a zárt ülés résztvevői már előre megírt anyagai okostelefon/tablet-en vannak és ezek célzottan előre leolvashatók például egy tőzsdei ármozgást befolyásoló helyen és időpontban. A támadók egy igazgatótanácsi ülés alatti stratégiai módosításokat az üléssel párhuzamosan hatástalaníthatnak, vagy fordíthatnak kedvezőtlen irányba. A notebookok, netbookok, tabletek és okostelefonok a felsorolás sorrendjében egyre valószínűbben kapcsolódnak és tűnhetnek fel zárt tárgyalások ideje alatt vagy annak időbeli közelében nyilvános mobil hálózatokon.

Adatforgalom korlát.

A kémkedés korlátja az adatforgalom és a sávszélesség korlát. A hirdetések adatmennyisége elviszi a forgalom 80%-t.

Megoldandó (volt) az kémkedéshez elegendő extra forgalom biztosítása a különböző, Internettel nem teljesen lefedett, nem együttműködő országok területén: FaceBook, Twitter (nem véletlen a régi "csipogó" névazonossággal).

Ezek a reklámokon keresztül a felhasználók saját zsebéből finanszírozott, önkéntes információ (es dezinformáció) közlő helyek. A jelen egyensúlyt a piac alakította ki. A szükséges reklámfolyam tartja fönn a kémkedők számára ingyenes és önkéntes adatáramlást.

Tehát a felhasználókra zúduló a felhasználó által kifizetett (!) adatfolyam tartja fönn a rendszert. Jól jár az ügyfél, mert megkapja az adatokat a normál ügy- és üzletmenetkor. Jól járnak a szolgáltatók, mert hozzájutnak a HW fedezetén túli nyereséghez és jól járnak a kémszervezetek is, mert az önkéntes-nyilvános adatokból jól tudnak szemezgetni. [11]

Pozíció meghatározottság

A legtöbb okostelefon rendelkezik pozíció meghatározó eszközökkel.

A cikk a komplex hálózatok matematikája fejezetben is foglalkozik a pozíció meghatározással és követéssel.

Pozíció GPRS,GPS, WiFI WLAN alapján meghatározható.

A GPS és a kiegészítő elemekkel ellátott AGPS pontos lefülelést, meglepést tesz lehetővé.

Célpontként: GPS pozícióra küldött megsemmisítés, futár, kommandó, rakéta, vagy IED (Improvised Exploding Device) stb.

Megtévesztő célpontként: a célpont szándékos megtévesztésre használhatja, ál-hamis (fake) célpontként, ha az általa feltételezett ellene irányuló akció során szándékosan fals pozíciót sugall, például az addig ismertként használt mobil eszközt egy logikusan kiválasztott vonatra, idegen autóra stb. helyezi, lehalkított módban. Ezzel ésszerűen nagyjából egyidőben egy másik mobilkészüléket kezd el használni, amelyet kis idővel előbb kapcsol be. Vagy egész egyszerűen egy vadonatúj készüléket vásárol.

Szinkronizációs problémák

Szinkronizációs problémák - asztali, laptop, notebook, netbook, tablet, palmtop vagy okostelefon szinkronizációk, e-mail szerver problémák.

A klasszikus matematikai alapprobléma egy elektronikus levél írásánál, ha a kiindulási gépen íródik a levél és ez nem kerül át a többi használatban lévő gépre, akkor az író lemaradhat egy adatfolyamról. Azaz ha egy másik gépen van épp, amikor az általa kezdeményezett levélre válaszolnak neki, de a válasz nem tartalmazza az általa írtakat, vagy rosszabbik esetben kárára MÓDOSÍTVA tartalmazza, akkor már komoly bajba kerülhet. Ezt a problémát áthidalhatja egy szerver, mint egy klasszikus webes e-mail, amely a kimenő levelet is elmenti. Míg a beérkezett leveleket a POP szerver tárolja, lehet(ne) hasonló, amely az elküldött levelet tárolja. Anélkül, hogy a küldőnek önmagának is kellene küldenie egy másolatot, hogy az általa küldött levelek megjelenjenek bármely általa használt gépen. Ezt kezdettől nem oldották meg az e-mail rendszerek. Mára túlhaladott, mert az egyéb kommunikációs lehetőségek felülmúlják, mint az azonnali üzenetküldők, vagy a közösségi oldalak.

Hiányosságok javítása

Becslést adhatunk a következőkre, hogy a zárt kódú rendszerek hiányosságait idővel közzéteszik, részben a dolgozók (80%), részben a véletlenszerű támadásokkal derítik fel (15%) vagy az abszolút váratlan esetekben derülnek ki (5%).

Kutatási eredményként talán megjegyezhető, hogy a nyílt forráskódú rendszerek forráskód állapotban áttekinthetőek, így szakemberek számára meggyőzően biztonságos programok keletkezhetnek. Ugyanakkor a nyílt forráskódú rendszerekbe a megfelelő helyeken rosszindulattal bele lehet módosítani és így máris egy trójai, vagy rés kerülhet be az eredetileg megbízható alkalmazásba, amely felfedezéséig védelem nélkül garázdálkodhat.

KOMPLEX HÁLÓZATOK MATEMATIKÁJA

Komplex hálózatok matematikája - Barabási Albert László erdélyi származású Amerikában élő magyar professzor. A vele készült riportban vetették fel neki, hogy kevesen tudják, hogy az internet és a mobiltelefon használatával milyen irtózatos mennyiségű adattömeget szolgáltatunk magunkról. A választ a könyvében találhatjuk meg: "Manapság jóformán mindannak, amit teszünk, marad digitális lenyomata valamilyen adatbázisban. E-mailjeinket megőrzik a szolgáltatók naplófájljai, telefonbeszélgetéseink pontos időponttal ellátott adatai ott nyugszanak a telefontársaságunk hatalmas merevlemezein" – írja Barabási Albert László - Villanások című 2010-es könyvében. [12]

Az emberek, akik a mobil okostelefonokat mobil internettel; a későbbiekben majd egyszerűen fogalmazva mobil kommunikációval ellátott eszközöket használják, mozognak a Földön. Mozgásuk közben a legkülönfélébb módon pozíciójukról információkat küldenek szerte, adatbázisokból kutathatóan. A jogszerű kutatásokkal is érdekes megfigyelések tehetők magukról az emberekről. A cikkben helyhiány miatt csak összefoglalva néhány eredmény.

Az emberek többsége az otthonuk és nappali tartózkodási helyük között mozog és e két helyen tartózkodnak a legtöbbet. Megfigyelték, hogy aki időben közelebb - ez úgy 20 és 30 perc – lakik, az a két fő tartózkodási helyen felül több időt tölt kisebb bolyongással e két hely közelében. Aki időben távolabb lakik, az sokkal kevesebbszer végez, „enged meg magának” egyéb bolyongásokat a munkanapokon. Ellenben éppen ők mozognak a szabadnapokon inkább távolabb. Itt a kertvárosi lét és a jómód korrelációjára lehet gondolni. Jellemzően a dolgozó átlagemberek a hétvégi illetve szabadságolási időszakban a szabadidős illetve üdülési övezeteket keresik fel. A rokonlátogatás is jól látható a mozgások statisztikájában, ahol

családonként jellemzően néhány más lakóövezeti helyet keresnek fel. Az üzletemberek mozgása jellegzetes. Általában egy-két, néha tízes nagyságrendbeli helyet keresnek fel. Repülőút esetén jellemzően repülőterek közelében „tűnnek el" a hálózatról és jelennek meg más repülőterek közelében, vagy jellemzően szállodai illetve irodai negyedekben, ha csak ott kapcsolják vissza a készülékeiket.

A számítógépes hálózatok támadása szempontjából ezek az információk döntőek és az egyes készülékek jellemzői, mint MAC address, oprendszer verziószám, használt e-mail címek, kommunikációs szoftverazonosítók alapján globális méretű számítógépes hálózati elemként funkcionálnak és támadhatóak.

Jelenleg tervezik a hackertámadások hagyományos fegyveres megtorlását, kilátásba helyezését.[13] Külön kutatási terület keletkezik így, amely az elrettentés vagy a (szándékosan) téves ellencsapás kérdésköre.

AZ ÚJ VESZÉLYEK KIHÍVÁSAI

A fentebb összefoglalt problematikák és programok sajátja, hogy a fejlesztők képesek és meg is közelítik olyan szoftverek fejlesztését, amelyek könnyen kiegészülhetnek valódi kémprogramokká. Például olyan komplexé, amely egyszerre közvetít és felvesz hangot és mozgóképet (akár takarékosan, csak akkor, ha épp aktuális), elküldi a GPS, vagy a mobiltornyok és WiFi-k kiegészítő információi alapján a pozíciót, monitorozni engedik a felhasználó billentyűzet leütéseit és a képernyőtartalmat, legyen az szöveg vagy kép illetve ezek kombinációja, sőt a pixelgrafikus képeken levő szövegeket OCR kiegészítőkkel karakteres formába is átdolgozzák.

A lehetőség mindenesetre ott van ezekben a készülékekben, együtt mozognak a hordozójukkal, tulajdonosukkal, aki akár lehet „célszemély", követve őt a normál üzemen kívül az üzleti, a munkahelyi titkok világába, továbbá a magánszférába a hálószobától a toalettig. Ha némi józanságra ébred a vásárlói társadalom, ragaszkodni fog a kameralencsék mechanikus eltakarásához, a mikrofon mechanikus némításához, az okostelefon valós árnyékolásához, például a fém cigaretta tartókhoz hasonló tokok, amelyek megvalósíthatják a kommunikációs csatorna frekvenciájára jellemző Faraday-kalitka árnyékolást. A technológiai kihívásokon túl pszichológiai és erkölcsi, de mindenesetre társadalomtudományi és bölcsészeti problémákat vetnek fel a jelenlegi technológia és a magánszféra új kihívásai. Mindezeken keresztül támadhatóak a számítógépes hálózatok és nem csak a technika, azaz a hardver és a szoftver, hanem az emberi tényező, ahol az ember a naiv, jószándékú, vagy alapvetően jószándékú felhasználó, aki ha néha ugyan csalafintán használna stikában fényképező programokat, amelyek a rendelkezésére is állhatnak, de a jóízlés megakadályozza ebben, önmaga éppen eshet áldozatául mások kémkedési szándékainak.

Ez az új kihívás a számítógépes hálózatok támadásának új dimenziója és bár a téma a nevéből fakadó definíció szerint szűkebbnek tűnik, ha katonai feladatra gondolunk, ahol az élőerő megkímélése a cél, akkor a nem halálos fegyverarzenálban fontos, új és egyre fejlettebb szerepe lesz-van a számítógépes hálózatok támadásában.

Kutatási eredményként megállapítható, hogy míg a hagyományos számítógép hálózati elemek alapvetően helyhez kötötten működtek, a jelen eszközei kiegészültek olyan mozgó készülékekkel, amelyeken keresztül nőtt az esély a helyhez kötött, jól védett eszközökbe bejutni.

Intelligens telefonok - buta alkalmazások

Különböző vállalkozások célozzák meg a belső felhasználóikat és ügyfeleiket okostelefon alkalmazásokkal, mint például az Apple iPhone és a Google Android. Sok ilyen alkalmazás anélkül készült, hogy alaposan figyelembe vennék az alkalmazásuk következtében kialakuló

biztonsági vonatkozásokat. Ezek megsértése mind az egyéni felhasználókra mind intézményekre, vállalkozásokra egyaránt hatással lehet. Támadóként kihasználhatják a kiterjesztett hozzáférést az érzékeny adatokhoz és hálózati szolgáltatásokhoz. Az előadás tárgyalja az újonnan megjelenő okostelefon alkalmazások üzemeléséhez kapcsolódó fenyegetéseket, és áttekintést nyújt a fenyegetések modellezésének folyamatairól.

Az előadás példaként végigvezet néhány alkalmazáson ahol a támadó szemszögéből bemutatja milyen típusú információkat képesek kinyerni, amelyek lehetővé teszik a további fejlettebb támadásokat. [14]

EMBERI TÉNYEZŐK

A számítógépes hálózatok támadása témában a fent leírtak alapján is levonható a következtetés, hogy az emberi tényezők döntő szereppel bírnak.

Az alábbiakban megkísérlünk összefoglalót, becslést és értékelést adni, továbbá néhány példát bemutatni a napjainkban élesben megvalósult okostelefonos számítógép hálózati eseményről.

Hackerek és crackerek, amatőrök és profik

Megpróbálhatunk egy becslést adni az alábbi tényezőkre, mint „hacker – cracker” vagy „önkéntes, profi és megfigyelő”. Ha a közelmúlt hírei a hacker és egyéb befolyásoló cselekményeket végrehajtók életkoráról igazak, akkor egy csúcsirányú 5-ös skálán a fiatalkorúak jellemzői az alábbi érdemjeggyel értékelhető:

Affinitásuk a következő irányokban, mint hacking: 4,5, cracking: 5, jogi ismeret 2 (a befolyásolt részéről) – 4 (befolyásoló részéről).

Tudásuk és képességeik: Tehetség 4.5, érzék 4, veszélyérzet és jogi tudás 2, amire csak a rendőrségi vagy személyes szabadság korlátozás kilátásba helyezése hat.

Várható, vagy már megvalósult a profi (katonai) szervezetek beépülése a fiatalkorúak közé. Ez még fiatal, önkéntes és finoman szólva rablóból lett pandúr tagokkal valósulhat meg, ahol az idősebb szereplők inkább a biztos hátteret, a gyors kivonást, visszavonulást támogatják. A beépített fiatalok 100% azonos habitust mutatnak, kell mutassanak, mint egy focicsapat, kivéve módosító akció idején.

Taktika: A hacker és cracker csoportok mutathatják magukat erősebbeknek, vagy gyengébbnek. Békeidőben gyengébbnek, felkészüléskor jóval gyengébbnek, vagy épp erősebbeknek mutathatják magukat, közte visszaesésekkel, de jól idomulva az elérendő célhoz.

A riválisi csoportok között spontán, vagy kívülről irányítottan kitörhet harc, ahol a külvilág járhat egyaránt jól vagy rosszul. Jól jár, ha "megeszik" egymást. Rosszul, ha a harcuk során megerősödnek, vagy egy újabb, erőteljesebb és erőszakosabb csoportosulás jön létre, amely elméletileg előre jelezhetően várható is.

Információk és dezinformációk közösségi médián, okostelefonok közreműködésével

A FaceBook-on illetve blogbejegyzésekben könnyen keletkeztethetők álhírek, dezinformációk. Maga a Facebook létrejötte is maga egy nagy álhír lenne, még egy játékfilm is készült róla. A lerágott csont „sufnicég”, két testvér, még ha igaz, akkor is mesébe illik. Szóba se jöhet az információs fölényre törekvés... Miért is maradt ily erősnek a Twitter és a FaceBook, valamint a jelenleg még háttérben felnövekvőben lévő Google közösségi csúcsalkalmazás?

Hillary Clinton szerint a hidegháború végén csökkentették a költségvetési támogatást, amely kommunikációs szempontból hatalmas károkat okozott. Ennek ellensúlyozására,

valamint a közelmúlt közel-keleti és észak-afrikai eseményeinek hatására az adminisztráció az internetes közösségi oldalakra helyezte a hangsúlyt és farszi, valamint arab nyelvű Twitter-oldalakat is indított. [15]

Éppen a mobil eszközök léte teszi lehetővé, hogy valós, friss hírértékű helyzetek kerüljenek fel közösségi médiára, azt elemezve, visszahatva információs harcosok befolyásolhatják a TÁVOLI csoportosulás működését. Mérsékelhetik vagy erősíthetik a hatásokat, információkkal vagy dezinformációkkal láthatják el a helyszínen levő mobil okostelefonokkal kommunikáló résztvevőket.

Az információs harcosok [16] várhatóan közel ötven virtuális identitást képesek kezelni egyszerre és igyekeznek befolyásolni valódi eseményeket a kibertéren keresztül.

Más cikkek pedig beszámolnak róla, hogy, „most már bizonyos, hogy a 2011 tavaszi szíriai forradalom egyik ismert alakjává váló, leszbikus Amina Arraf nem létezik, és egy Skóciában élő amerikai férfi írta a nő híressé vált blogbejegyzéseit. Ezt a férfi felesége e-mailben erősítette meg a Guardiannek. A hír hallatára többen is bírálták a férfit, aki azzal védekezik, hogy nem számított ekkora figyelemre."

Elhitték neki, hogy a helyszínen mobil internetes okostelefonnal van jelen. „Shakira szól az iPodomon" állította. [17]

Pszichológiai behatások

Az intrika mobbing, csúfolódás bullying, pszichomotorok ereje jelentős a közösségi hálózatokon és a mobil számítógépes hálózatok támadásával még áttekinthetetlenebbé válhat az emberek ilyen tulajdonságából fakadó tevékenység, vagy a szándékosan létrehozva utánzott ilyen eljárás.

Távoli diszciplínák

Napjaink jelenségei, akár szimpatikusak, akár nem, akár elfogadhatóak, akár megváltoztatandóak, de tények. A hétköznapi ember számara távoli diszciplínák összekapcsolására alkalmas példa a "valóvilág" kísérletek, ahol szimpatikus-erőszakos elfogadott viselkedésformák kutatása folyhat, részben közpénzből, részben a „köz" pénzéből, hisz önkéntes reklámfaló közönség előtt folyik.

Az eredmények felhasználhatók nagy populációk mozgatására, irányítására.

A "nyertes" részben "sajáterős", saját újonnan megszerzett tudása-tehetsége segítségével tör előre, részben előre szerződött forgatókönyvet követ.

Elszigetelt földrajzi, nyelvi, írásjeli populációk, világvallások esetében eltérő finomhangolt paraméterekkel végezhetnek műveleteket. Közelítő példaként az azonos franchise televíziós műsorok jól megfigyelhető terepek. A közösségi tartalom megosztó oldalakon, mint például a Youtube földrésznyi távolságokból tekinthetünk bele azonos nevű és célú műsorokba, és megfigyelhetjük a helyi sajátosságokat. Azon is elcsodálkozhatunk, ha kell ezen egyáltalán, hogy a videón látható emberek kezében ott vannak az okostelefonok, amelyek láthatóan Internet eléréssel is rendelkeznek, így mozgó részét képezik a globális számítógépes hálózatoknak.

ÖSSZEFOGLALÁS

Szerző cikkében röviden megpróbálta összefoglalni a számítógépes hálózatok és azok támadása egy szegmensének újdonságait, különös tekintettel a globális méretű mobil internettel ellátott okostelefonokra. Bemutatta az új eszközöket, azaz az okostelefonokat, ezek lehetőségeit és dinamikus arányát a számítógépes hálózatokban. Igyekezett összegyűjteni az új állapot alakította kihívásokat és ezek kutatási irányait. Megoldásokat próbált keresni és igyekszik nyújtani a felmerült veszélyekre.

Felhasznált irodalom

[1] Dr. Szabó Henrik - Számítógépes bűnözés - bunmegelozes.uw.hu/szamitogepes.pdf - (2011.06.20.)

[2] Dr. Haig Zsolt - Számítógép hálózati hadviselés rendszere az információs műveletekben http://www.hadmernok.hu/xx/06_Haig_Zsolt.pdf - (2011.06.20.)

[3] Dávid Imre: Rekordkártérítést kérhet az Oracle a Google-től

[4] http://computerworld.hu/rekordkarteritest-kerhet-az-oracle-a-google-tol-20110622.html - (2011.06.22.)

[5] Kodolányi Balázs: Az Oracle megveszi a Sun Microsystemst http://computerworld.hu/az-oracle-megallapodasra-jutott-a-sun-microsystems-szel.html - (2011.06.20.)

[6] Dávid Imre: A Microsoft ma jelenti be a Skype felvásárlását http://computerworld.hu/a-microsoft-ma-jelenti-be-a-skype-felvasarlasat-20110510.html - (2011.06.20.)

[7] Android Network Mapper http://www.androlib.com/android.application.org-prowl-networkmapper-xtDn.aspx - (2011.06.20.)

[8] Android Market › Photography › SECuRET SpyCam https://market.android.com/details?id=com.dooblou.SECuRETSpyCam - (2011.06.20.)

[9] Android Market › Photography › Super Spy Camera+ https://market.android.com/details?id=com.snoweye.spycamera - (2011.06.20.)

[10] Android Market › Shopping › Barcode Scanner https://market.android.com/details?id=com.google.zxing.client.android - (2011.06.20.)

[11] Sunalini Rana: 10 Best Android Remote Desktop Apps - SloDive - http://slodive.com/freebies/android-remote-desktop-apps/ - (2011.06.20.)

[12] Barabási Albert László - Villanások (Bursts) - Nyitott Könyvműhely, 2010 p4

[13] Háborús cselekedetnek minősülhetnek a komoly hackertámadások - http://htka.hu/2011/06/02/haborus-cselekedetnek-minosulhetnek-a-komoly-hackertamadasok/ - (2011.06.20.)

[14] Dan Cornell, Principle, Denim Group - Smart Phones with Dumb AppsNAISG HouSecCon - THE Houston Security Conference - http://houstonseccon.com/media/archives/hacking-track-presentations/ - (2011.06.20.)

[15] CNN Wire Staff - Voice of America internet site hacked by Iranians - http://articles.cnn.com/2011-02-22/world/iran.voa.hacking_1_voice-cyber-attack-muslim?_s=PM:WORLD - (2011.06.20.)

[16] Dr. Kovács László – Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmazhatósága a Magyar Honvédségben – Doktori értekezés - http://193.224.76.4/download/konyvtar/digitgy/phd/2004/kovacs_laszlo.pdf - p24 - (2011.06.20.)

[17] Visnovitz Péter: Lehet, hogy sosem létezett a szíriai forradalom leszbikus hőse - http://www.origo.hu/nagyvilag/20110608-amina-arraf-a-sziriai-forradalom-leszbikus-blogger-hose-portre.html - (2011.06.20.)

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Faragó László
farrago.laszlo@ke.hu

THE SUPERVISORY ROLE OF THE GUERRILLA-MEDIA IN THE HORIZONTALLY AND VERTICALLY EXPANDING NEW VIRTUAL PUBLIC SPACE

Absztrakt/Abstract

Az új média szereplőinek, elsősorban az erőszakos cselekmények kapcsán kialakult csoportját utcanyilvánosságnak nevezem. Az utcanyilvánosság szereplői, akik saját kommunikációs eszközeiket felhasználva képi, hang vagy szöveges információt osztanak meg egymás közt, vagy ezeket eljuttatják valamelyik hírügynökséghez. Legaktívabb tagjai a netriporterek, akik képesek – tudatosan - eseményt tudósítani és dokumentálni, de ezzel együtt részei lehetnek a „hírgyártásnak" is. Az utcanyilvánosság abban más a formális médiához képest, hogy a fogyasztókkal mellérendelt kapcsolatot tart fenn, a szerepek pedig felcserélhetők. A gerillamédia az engedély nélküli rádiókhoz hasonlóan hozzájárulhat a társadalmi változásokhoz. Mindezek alapján megállapítható, hogy az új média, az utcanyilvánosság sem képes maradéktalanul betölteni az információk ellenőrző szerepét.

The new media actors, particularly in the context of violent events I called street-formed group of public simply: street publicity. The street-public actors who use their tools of communication, and who share their imagery, sound or text information with each other, or send this to news agencies. Most active members of the net-reporters who are able to report and document incidents consciously, and they can be a part of the "news manufacturing". The medial structure of street publicity differs from the formal media, in the co-ordinated relation and roles interchange ability. The activity of public discourse is increasing by the effect of violence and ban. The guerrilla-radios like the radios without a license in the media contribute to social change. All these suggest that the new media, the street publicity can't be the control of information alone.

Kulcsszavak/Keywords: *utcanyilvánosság, virtuális média, gerillamédia, netriporter, telefontanú ~ street-formed group of public, street publicity, virtual media, cyberspace, guerrilla-media, netreporter, phone witness*

INTRODUCTION

The conscious use of the media players has expanded in recent months in a great extend wiht new-media playersI call street publicity.[1] On this basis, the media-space boundaries have not expanded but disappeared. The real-time news make sense instead of pre-and posteriority events and there is an endless need for the real-time news. Today the limitation period of the news are measured in seconds.

My thesis is dealing with mainly the actors of virtual media-space surrounding the violent events.

The naturaly status of the street publicity players are restless, the high level of interest and specticism.

In my opinion the the street-formed group of public is named the new public, street publicity can be used to monitoring role of formal media. The members of society, in a democracy or pre-democracy can be essential in the participation of information. The members of public space contribute to the multi-layered analysis of the publicity and they document and published the events in cyberspace. The street-public actors who use their tools of communication, and share their imagery, sound or text information with each other, or send this to news agencies: huge or smaller radios, tv or web editors. The activity of street-public actors is outstanding in violent situation, or at least significantly increases with the danger of the risk of violence.

It's typicall that CNN began the 21-hour news summary on 15 April 2011 (in the Central European time zone) with an amateur video shared shortly before.

Agreeing with Feintuck and Varney (2010: 14-17.) opinion: the strictest limitation of the freedom of the press is the pre-censorship or prevention of the appearance. So an amateur recording can be really a counterpoint.

The boundaries of media-space is significantly has expanded and doesn't coincide with the national borders. The street publicity, as the management of media space is still nowhere to be attempted, the network is not suitable for block.

In my paper I examine the contents of significant news sites.I have not compared the news appeared on different surfaces, but I've typed the say of amateur journalists.

THE NARRATIVES OF STREET PUBLICITY

In recent months the events of the Arab world have made absolutely clear that the formal media is forced to cooperate with virtual space's player, who does not work for order in most cases. However, we do not believe that the information shared by the public street is intended to reflect reality. I must agree with Umberto Eco who believes: you can easily understand the sequence of events if they are coherent interpretation (Eco, 2007).

The blog of Manual Rubiales (2011) I regard as a startingpoint. He said that everyone has a duty to control the line of democratic misled to understand what is happening around us. The Spanish Rubiales compares the Internet with the REI (Radio España Independiente), which is a seventy years old guerrilla radio.

I will return to this, but during the paper writing the virtual public interested in the case of Straus-Kahn. He was the head of IMF and his affair was published first by a Montreal student on Twitter.

The French-Canadian boy, his friend and his father reject the charge that the young man would have-played any role to overthrow the head of the IMF bank.

---

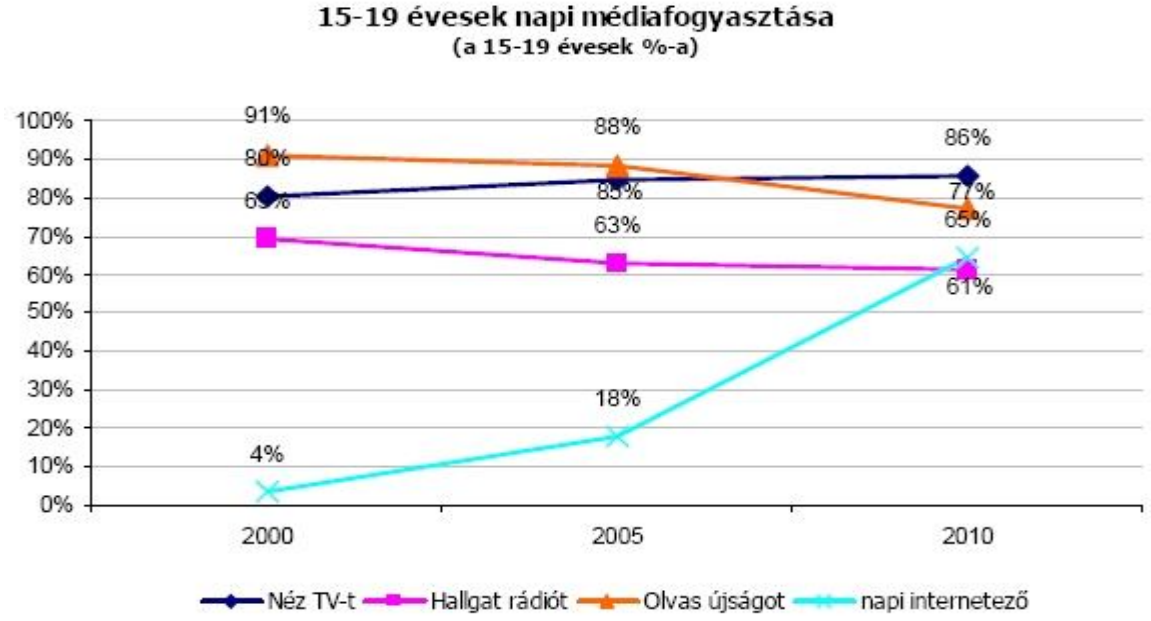
1 The first concept is the 2011th March 4 was used in Tirgu Mures, new media, real and virtual spaces'conference / Sapientia-EMTE /. The following paper extends the performance and the revised version

To prove the above statement is not the topic of this thesis, anyway, it would be difficult to do and question whether that will ever be found. However, can be concluded in the foregoing that the virtual public square would be converted in an incredibly fast by topics of public-discourse and it can be also defined globally.

The new-media creators, editors, reporters and „guard dogs" have become massive media consumers resently, besides the current editorial workl. Strarting from this it, there is the chance that the new media content creators not only hold a mirror to the society, but whether consciously or less consciously influenced by the viewer, reader, and listener. The new media player may be active eyewitness only. However I have called it the street publicity, but I would prefer phone-witness, who share with friends unknown and upload mainly pure text messages, images, audio or video too, and it prepares to accommodate to the cultural differences. I'm sure the opinion bloggers are new media players too. The street publicity may be part of the guerrilla-media. On the other hand is the hate speech (Hargitai 2009), which is done in order to hostile influence, specifically. Very high rate of information flow nowaday, therefore it can not easily reflect in the editorial boards of professional. Based on these one of the basic most important journalistic rule is surely violated, namely compromised the control of complementary information. The third representative of the streets publicity is the net-reporters. It can be found in the personality of net-reporter apperance in willingness, interested in the high-degree of actuality news and able to articulate the information obtained.

The new media supplemneted with netreporters, consequently increased of players in street publicity, and the public actors use more and better smartphone. Create a virtual agora where the internet is essentially present, people use it daily in their smartphone. You can find a common narrative of the media messages and a common value system. The players do not necessarily need to be fixed place.

However, 4.1 to 5 thousand million mobile phone user are worlwide currently, based on data from The Washington Post there are. Internet use in Hungary has incresed 4% to 65% in the last ten years, according to the National Media Analysis: examining the 15-19 age group. (Source: GfK Hungária - Ipsos, National Media from 2000 to 2010)



Internet use in Hungary has incresed 4% to 65% in the last ten years, according to the National Media Analysis: examining the 15-19 age group. (Source: GfK Hungária - Ipsos, National Media from 2000 to 2010), ligh Blue shows the use of internet[2]

In my opinion they can also generate social change which move dynamically, organize and transform in the virtual space, assists in the process of democratization. Willy-enter the street publicity engages involuntary citizens of society that become active players of expression. The new media are keeping on dynamic move the social structure of the public.

The medial devices will not only change, they go through the change of function, but also very fast and continuous convergence is observed. As a result of a foregoing develop a new tool that integrates the earlier ones, added to the basis of the needs and generate additional transformation. (McLuhan, Marchall 2001)

The new public media events are created and carried beyond by street-reporters to inform, confirm social solidarity. They have a key role in shaping values, as written in formula a theory of ritual communication by Dayan and Katz (ARNOLD, Molnar 2009). The network communication of equal operators is not in itself ground for conversation, but also a cultural melting pot, on the other hand a group organizer as well.

The following features, impact and dynamics of street publicity is typed by public properties and various internet contents. Concluded that the current political power can be terrified by the dynamics of a virtual public space. The authority in China, after Egypt, Tunisia and Libya took action dramatically against a virtual space of public discussion: slowed down, filtered, or completely eliminated the use of internet.

In my opinion, virtual guerrilla-media is created with the power compared with the power of censorship attempts establish.

The Spanish word Guerrilla comes from ‘la guerre’ means little war, the struggle of irregular elements, which directed against the reigning power. The virtual guerrilla-media actors can be a telephone witness and the opinion blogger. The third representative of guerrilla-media is net players who lead to a moral panic with false news and hate speech. Let's call them web-Help.

Based on experience, the guerrilla media working without licence and prohibition, at least as effective as guerrilla marketing. The guerrilla media can be a particularly intense effect in particular, where there are attempts to limit the power of it. The authorities limit or completely prevent the effect of new networks and organizing media, where media consumers are not careful enough range. In other words, they pose a threat, which does not occur in the conscious media citizen (Császi 2009).

The guerrilla media is in many respects similar to the XX. Century guerrilla radios. Among other things the guerrilla media affects the public to restructure and simultaneously the social multiplier effect can not be underestimated either.

„LA VOZ DE LA VERDAD”

The Radio España Independiente (La Pirenaica)3started broadcasting seventy years ago. Five years after the Spanish Civil War (1933-1936) and two years after the Franco dictatorship gave decree so called "No source of news". From that time the political power has censored private radios and the state radio became official news source. REI was guerrilla radio, which broadcasted alternative information against the unilateral dictatorship across borders, even if REI was committed communist and it was on the left. „The effect of La Pirenaica far superior to other, similar unlicensed guerrilla radio: connected people and

2 http://kozmedia.blogspot.com/2010/10/nemzeti-mediaanalizis-10-ev-alatt-4-rol.html (Last Downloded: 23th April 2011)

3 The REI in 1941 from 22 July 1977 to 14 July was the first time Moscow and Bucharest, aired from 1955 to

organized the resistance against violence.” It should be noted, - Plans wrote - that the REI-mediated information was sometimes exaggerated, biased. In spite of this, REI published information, which4Spanish public media didn’t (Plans 2011).

The radio sound archives are serving as a historical source for millions of Spaniards. The guerrilla channel gave an opportunity to express their views which would not have been possible elsewhere in dictatorship. (Pamies, 2007 23-31) The REI's information was taken by people, so-called Palomas. “Pigeons” carried news on sound track, orally, in writing, no later than one week they have reached out to the editorial. Today I would say that these messengers were phone witness. The seventy years old guerrilla radio had formal monitoring role of the dictatorship. It should be noted that guerrilla radio had close ties to left-wing so can not be called biased.

1. figure. “REI logo”, photomontage made by José Renau by Pcasso's peace dove

Still far from being clear that the "Twitter Revolution" (for others is called the Facebook revolution) what role in the transfer of power in Tunisia. But it is clear that as a group organizer had an impact on the development of events.

Mark Lynch (2011), a political science professor known at Forigne Policy believes that the social networking sites and the effect of television together have led to the transformation of the structures of power.

However it should be reported that the medial space of street publicity is traditional media. But of course is not, because the actors of cyberspace share news and information with each other. This may be influencing factor: the street-public actors send messages only to each other. At other times they can be a control of formal media.

The new-media is the fifth branch of power by Bajomi-Lazar.

Montesquieu wrote the three - traditional - branches of power, legislative, executive and judicial power, as is well known. Edmund Burke – 18th century English politician – called journalist the fourth branch of power (The Fourth Estate). They took a sit in the parliament gallery "up there" and Burke suggested that the journalists of the inspectors of democracy. We have to agree with Bajomi: the fifth branch check to the traditionally democratic societies and can controll the censored official media. The street publicity (so called fifth branch) carries out its function that they communicate unpredictably in real time and documented and enunciation more diverse opinion.

4 With Spanish Communist Party (PCE), a historical archive of recordings preserved in the REI, the radio messages sent to more than 15 thousand is a letter, containing recordings of the radio catalog consists of more than 12 boxes. (Hoya, 2011)

The Telegraph's online interface using twitter writes that the main weapon was broom after revolution on Cairo's main street. Suggest that the protesters organized the clean up of waste and debris on the community site because cleaning service didn't work.

As part of the self-organized society is participate in street cleaning.

The new virtual "weapon" is the smart phone. It's able to cause social changes and influence social control while we use it alone or with other media.

TO LIVE TOGETHER WITH THE APPARENT NEWS

The professional media is now added to the street publicity. The newly-created virtual public space is fundamentally different from the previous medial square: faster, more reliable, more diverse and has got co-ordinated structure. Previously is believed to be unchangeable hierarchical relationship between journalist and the media customer. Instead of the street publicity has been a future of the juxtaposition of subordination and the network connection lately.

Everyone can be a bit of photography, editor and reporter; the next moment can be an active media consumer. All the while the roles are mixed up naturally, of course, as is demonstrated in the juxtaposition of subordination characteristic. One of Tunisian cyber-fighter is quoted by Denes Baracs by the French Le Monde newspaper based in, who says literally: "we were on the streets day and by night in front of the screen." Baracs, 2011)

The new interactivity is much more creative and means much more active participation in the former media, as well. Participation in this media I've called input, while access to the media is an output. Media consumers not only interested in news and the values conveyed by media, but media consumer wants to take part in shaping society's values, increasingly. On this basis, one must understand the statement that the new media build path to audience which continues to grew. (Istvánffy 2005)

He did not say any chance that was created a global, but a single media-space. The groups in the virtual agora are organized with common narrative; they become interested in the topics. Lynch mentioned earlier, for example, makes reference to a WP article an "Arabic, or Al Jazeera narrative."

But able to determined public opinion (net-atmosphere) any crash, catastrophe or shocking case and able to construct a common narrative. There are those who do not deal with the Middle East crisis, of course. They are completely indifferent to the issue of the Arab world. While others are relates to the virtual community of the world remote corners of the neighbourhood or even street.

But why? What it takes someone to the moment of explosion, Domodedovo turn on the phone's camera? Why make a record that covers the face of our eyes. What could be the purpose of the close up photographs of a police action, and then share the video, or send an editor.

Connected to the former, one of the most important question to be answered - in my view as to why is activated the phone witnesses, particularly in violent situations?

LET US CONSIDER WHAT MOTIVATED THE STREET PUBLICITY

I. The telephone witnesses (net-reporters) are:

- messaging
- media coverage, vanity
- anonymity
- to satisfy the immediate hunger for news: the real-time monitoring to attract people
- documentation, to obtain most accurate and are transmitted
- media control, to say what others can not
- avoidance of physical, psychological, relational violence, to obtain the best possible position
- consolidating our position on their own

II. The Web Help:

- causing panic
- anonymity
- influence the opinions and heuristic decisions, for its oew sake
- media coverage vanity
- making money
- avoidance of physical, psychological, relational violence, to obtain the best possible position

Among the motivations can be found so-called conscious elements that are characteristic of the mediacitizens, according to Lajos Császi. This group's members are the ones who are able to assess accurately, that they live their life what media are built (Császi 2009), but also have the opportunity to make choices and therefore "transmit" and debated. But the business objective is a conscious element since a sizable sum of money to get. (In Blikk newspaper, or the online edition paid thousand Hungarian forint to striking image, for example, when one politician left in the car park of disabled, a vigilant passer-by photographed.)5
The motivations have instinctive elements such as survival instinct; we can see all of phone witnesses, and web help, too.

VIOLENCE ONLINE - THE ROLES ARE INTERCHANGEABLE

The most popular European, English-language online news portal's first text message lets you know that either sms or e-mail, text, picture can contact with them in mid January 2011, at nine o'clock in the morning. And as soon as possible, they also contributed to give this information. Obviously, everyone suspects that there is a filter where news go through, but it's not at all deterred from phone-witnesses to report the death of their relatives.

"Sara, a young woman in Tripoli, has told the BBC World Service her cousin and a friend were shot dead by security forces on Sunday, and she is very worried about her three brothers, who have told her by phone that they have also been shot. She says it is not safe for her brothers to return home at the moment. "Since last night, I have been worried and pray that

5 http://www.blikk.hu/blikk_aktualis/tilosban-parkolt-luxusautojaval-lazar-janos-2044263?nocache (Last Download 26th febr 2011.)

their phone cards don't run out. Because once they lose all their credit, we can have no communication."

I have an important note to BBC: the events can be followed minute by minute, that does not need to refresh the webpage. That is really real-time participation; I will not miss anything if I do not click to another page. 6

We read a similar message on CNN site, which warns that we can find unstructured news in this section.

In most cases the phone media-witnesses behave as citizens who are not content with information delivery but form an opinion, and plays a role in shaping society's values. The phone-witness is not satisfied with passivity of transmission instead of they would like to participate in journalistic rite. Bajomi-Lazar notes (Bajomi-Lazar 2010) to Daniel Dayan and Elihu Katz's theory of media-event (1992). The real-time events "people are so attracted because they feel like a participant." This is necessary because the majority of people is looking for orientation, they want other confirm what is order and chaos. It is not a coincidence that a number of televisions also gave a live broadcast about street confrontation in 2006 in Budapest, or riots in Paris, or conflict in the Middle East, North Africa producing a large television.

It is similar to the motivations of phone-witnesses. It also may be true because in interchangeable roles people feel obliged to share violent scenes with professional media. In fact he is very happy looking at it, even if watching own film he horrified in the evening.

The "spectacle of violence is not necessarily alarming, but also meets a need for some kind of ancient." Bajomi-Lazar notes that the "medial space and the spectacle of violence are inseparable since the beginning of human civilization. Ancient requirements related to the reproduction and survival. In other words, they are in an advantageous position to assess the ground, they become predictable in oral or physical violence, and they receive a greater chance of survival (Toth 2007).

Császi believes that violence is symbolic representation of the cultural community in protecting its members to physical violence. The spectacle of violence in society also agreed to strength our system of norms, standards. The acceptance depends on what are their reactions when they are breached. The more deeply rooted in a moral norm, the more intense reaction will be if it is breached. Finally, we can state that the violence in each cases depends on the culture medium.

MEDIA LITERACY, RISK

Live broadcast and documentation of violence, - as a moral panic (Császi, McRobbie) - serve as a deterrent. We should test what the political power can do or get adequate support the mass (so called opposition), which stretches the boundaries of social norms? The media literacy is a constantly moving front line, where the power and the street publicity magnifies and distort events from the perspective of their own. The dynamics of official media and street publicity represents a control over.

The media coverage is the major motivation for Twitter users, uploaders - videos and messages - and sharing group. It's not relevant to them to hear their voice, show their face on TV, or read their messages, although this is one aspect among many. It's enough if the recording will be valuable to others, gives rise to a shared video and they can be proud of it.

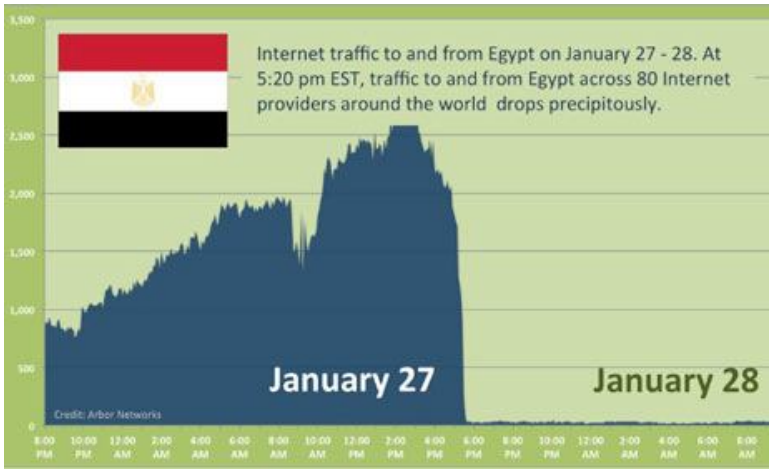
[6] Welcome to iReport, where people take part in the news with CNN. Your voice, together with other iReporters, helps shape how and what CNN covers every day. So you know: iReport is the way people like you report the news. The stories in this section are not edited, fact-checked or screened before they post. Only ones marked 'CNN iReport' have been vetted by CNN. http://ireport.cnn.com/ (Last Download: 01th Marc 2011)

The shared message (official media, net-citizens) for the people to influence their own as well7: "I promise to get back tomorrow." This sentence is worth much more on BBC's online interface broadcasting as if someone had sent an SMS to a friend. According to Aronson, someone who has consistently engaged (Aronson, E. 2008) rather keep the promise for others (towards myself). The effectiveness of persuasion depends on the extent to which I am involved in the virtual space.

Also there is a risk of spreading the wealth of information in cyberspace: one can read dozens of false news, other information was deliberately misled, similar to the Rwandan hate-radio (RTLM 1993-1996) which could call the people for violence with an amazing efficiency (Hargitai 2009). Efficacy was that the recipients were not media-conscious citizens. First time of emission the RTLM was called by the American ambassador is the best source of information and the radio broadcast music which could not be heard in the formal, boring public radio.

Similarly the guerrilla radio can also be a best source of information, all the more American statistics show that among Egyptian young, educated and urban population increased the number of net users one percent to 21 in late January (Sheridan 2011).

However it's out of questions possible that the majority of them have become active net citizens in a few days. The following chart shows the period when the Egyptian authorities limited internet use on 28 January 2011. (Labovitz 2011)



2. figure. Egypt cuts off most internet and cellphone service on January 27-28 2011

The falls or less verifiable data is given in connection with Buazizi Muhammad's volunteer fire death, which many say started the Arab revolutions. The 26-year-old boy who was selling vegetables, he is revered as a hero in the world. However, at least there are as many obscure points in the history as we are sure: the part of street legend is the alleged young's university education, is being unfairly punished for that, that his car in which the vegetables are offered was really seized? (HVG Online, 2011) HVG reported that a street named after him in Paris shortly and is expected to make a history film about him. All these suggest that the new media, the street publicity can't be the control of information alone.

Doesn't seem that there is, but it is, and it shows, we can translate of Walter Lippmann's idea: is not the place to look at something and decide what we see, but we decided what we see and then let's see. All of these, it seems does not help that opinion on what they say, the order of magnitude more people than ever see.

7 Jeel Ghathub tweets: "It's important to note, We Are Not pushing for the old Monarchy or any is to come backo nly for the Advancement Political Persons Libya FREE" @ Tripolitanian tweets: "@ rstripolina Yea ITS quieting down, Still some people out, they're really tired, lots dead, promising to come bk out tmrw tho 'http://www.origo.hu/itthon/20000223betiltottak.html (Last Download 2011th Feb. 25)

The new media, street publicity according to the characteristics carry the possibility of marketing, as well as the guerrilla media. News and advertisement are business. The CEPT (Conference Européenne des Administrations des Postes et des Télécommunications, ie the monitoring of the European telecommunications organization) which brings together twenty European countries, has a report from 2006. According to this 800 unlicensed radio worked only the Netherlands, most of which were created for commercial purposes. (Farago, 2011) During the Arab revolution the following advertisement appeared on social networking sites: A nice play on "revolution" with "evolution" on this T-shirt as pointed out by Pakinamamer on Twitter. 8

3. figure. One of the many T-shirts ordered from internet

SUMMARY

I've called the new media players, particularly in the context of violent street-formed group of public simply: street publicity, which is suitable to fill the role of formal control media. The street publicity can be observed in the social media space but is able to fully apply only with the formal media. The most active members of it are the net-reporters who are able to report and document incidents consciously, and they can be a part of the "news manufacturing".

The new virtual "weapon" is the smart phone. It's able to cause social changes or social controll while we use it alone or with each media. The medial structure of street publicity differs from the formal media, in the co-ordinated relation and roles interchange ability. The groups in the virtual agora are organized with common narrative; the geographical location is not a factor in generally.

The activity of public discourse is increasing by effect of violence and ban. The censorship and media licenses deprivation lead to create a guerrilla media. The guerrilla media can be a particularly intense in particular, where there are attempts to limit it by the power.

The virtual guerrilla-media is a tool that does not have a license or permit a legal attempt to use the covert messages to share. Guerrilla-media may also be created when the power is trying to block, ban or censor the internet network, organized street publicity.

8 http://www.zazzle.com/egypt_tshirt-235316776064147879: Last Download 27th Febr. 2011.)

The conscious use of the media is a constantly moving front line, where the state and the street publicity deliberately exaggerates and distorts the events their own perspective. The dynamics of official media and street publicity may represent a control over each other. All these suggest that the new media, the street publicity can't be the control of information alone.

References:

[1] Aronson Eliot (2008): A társas lény, Akadémiai Kiadó

[2] Bajomi-Lázár Péter (2010): Média és politika, Antenna könyvek, PrinXBudavár Zrt

[3] Briggs, Asa – Burke, Peter (2004): A média társadalomtörténete, Napvilág

[4] Császi Lajos (2009): A médiaerőszak, mint a társadalmi erőszak szimbolikus helyettesítője, A médiaerőszak; Tények, mítoszok, viták, MCC-Századvég Kiadó

[5] Feintuck, Mike – Varney, Mike (2010): Médiaszabályozás, közérdek, törvény. AKTI-Gondolat>

[6] Hargitai Henrik (2009; 169-192): A gyűlöletrádiók; A médiaerőszak, Századvég kiadó, Budapest,

[7] Pamies Terese (2007): La Pirenaica, Cossetánia Edicions, Valls, (Espana) ISBN: 978-84-9791-259-4

[8] Stachó László, Molnár Bálint szerkesztők (2009): A médiaerőszak; Tények, mítoszok, viták, MCC-Századvég Kiadó

[9] McLughan, Marshall (2001): A Guttenberg-galaxis, A tipográfiai ember létrejötte, Budapest, Trezor Kiadó

[10] Baracs Dénes: Tunézia az első sikeres online forradalom? Emasa, online kiadás; Istvánffy András (2005; 79-88): A terror rítusai, Beszélő, 10/ 8,

[11] Tóth Péter (2007, tél): A médiahatás-kutatás problémái: agresszió és az erőszak rekonceptualizálása, Médiakutató,

[12] Faragó László (2006): Társadalomformáló kalózrádiók és a közhatalom reakciói, Társadalom és honvédelem, X/3, p:187-205.

[13] Rubiales, Manuel: La Pirenaica, de nuevo (por Ramon Reig), blog, 2011th Marc 2 http://minombre.es/manuelrubiales/2011/03/22/la-pirenaica-de-nuevo-por-ramon-reig/, Last Download: 2011th Maj 29

[14] Crespo, Huan Franco:
Entrevista a Victoria Pujolar, exlocutora de Radio España Independiente, 'La Pirenaica', Last Download: 2011th Apr 9

[15] Hoya, Julian Sanz: El Correo de la Pirenaica o el PCE y la historia social del antifranquismo,
http://www.pce.es/mundoobrero/mopl.php?id=251 (utolsó letöltés: 2011thMay 29)

[16] PERITZ , Ingrid and Thanta Ha, Hu: The IMF chief, the Canadian-born student – and the tweet that rocked the world The Globe and Mail:
http://www.theglobeandmail.com/news/national/the-imf-chief-the-canadian-born-student-and-the-tweet-that-rocked-the-world/article2024864/
Last Download: 2011th Maj 30

[17] http://www.natureduca.com/radioblog/?p=111http://www.emasa.hu/cikk.php?id=7943
Last Download: 2011th Febr 24

[18] Sheridan, Mary Beth: U.S. warns against blocking social media, elevates internet freedom policies, Washington Post, January 28, 2011; 2:57 PM http://www.washingtonpost.com/wp-dyn/content/article/2011/01/28/AR2011012804554.html

[19] HVG 2011th Febr 23 http://hvg.hu/vilag/20110222_arab_forradalmak_bouazizi#utm_source=hvg_daily&utm_medium=email&utm_campaign=newsletter2011_02_23&utm_content=normal; Last Download: 2011th Febr 27

[20] http://www.washingtonpost.com/wp-dyn/content/article/2011/01/28/AR2011012804554.html, Last Download: 2011th Febr 21

[21] http://lynch.foreignpolicy.com/posts/2011/01/15/tunisia_and_the_new_arab_media_space, Last Download: 2011th Febr 21

[22] http://www.origo.hu/itthon/20000223betiltottak.html Last Download: 2011th Febr 25

[23] Labovitz, Craig (2011) http://asert.arbornetworks.com/2011/01/egypt-loses-the-internet/ Last Download: 2011th Maj 30

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Resperger István
resperger.istvan@zmne.hu

Pataki János
janos.pataki@audi.hu

EINFÜHRUNGSAUFGABEN DER SICHERHEITSMASSNAHMEN DER SICHERHEITSBEHÖRDE DER UNGARISCHEN EU-RATPRÄSIDENTSCHAFT IM ERSTEN HALBJAHR 2011

Absztrakt/Abstract/Abstrakt

A szerzők felmérik azokat a tényezőket, amelyek alapjául szolgálnak Magyarország EU elnökségével kapcsolatos biztonsági kérdések elemzésének, különös tekintettel a globális biztonsági kihívásokra és biztonsági intézkedésekre Magyarországon és külföldön egyaránt.

The authors surveys the efforts that provide a basis for the analysis of security issues related to the presidency, with special focus on global security challenges and the execution of security operations in Hungary and abroad.

Die Autoren untersucht jene Bestrebungen, anhand derer wir die Sicherheitsfragen der Ratspräsidentschaft untersuchen können, mit besonderer Berücksichtigung der globalen Sicherheitsherausforderungen, sowie der Durchführung in- und ausländischer Sicherheitsoperationen.

Kulcsszavak/Keywords: *Európai Unió, EU-elnökség, Magyarország, kihívás ~ European Union, EU-Presidency, Hungary, Challenge ~ Europäische Union, EU-Ratspräsidentschaft, Ungarn, Herausforderungen*

"Dann, wenn das Auge geblendet ist und der Mond sich verfinstert
und die Sonne und der Mond miteinander vereinigt werden,
an jenem Tage wird der Mensch sagen:
"Wohin (könnte ich) nun fliehen?" [1]

EINFÜHRUNG

Der Europäische Rat wird durch den Ratspräsidenten geleitet [2]. Der Vorsitz wechselt halbjährlich zwischen den Mitgliedsstaaten, wobei die Ratspräsidentschaft die Mitgliedsstaaten vertritt, indem der betreffende Staat der Europäischen Union „Gesicht und Stimme“ verleiht. Der Europäische Rat bestimmte für den Zeitraum 2005 bis 2020 eine Rotationsreihenfolge der Präsidentschaft[3]. Zu den Aufgaben des Ratspräsidenten gehört unter anderem die Organisation und Abwicklung der Sitzungen des Europäischen Rates, sowie im Rat der Europäischen Union die Leitung der Sitzungen auf Ministerebene, bzw. die Repräsentanz des Rates in anderen europäischen Organisationen und Institutionen sowie in der Europäischen Kommission und im Europäischen Parlament. Der Ratspräsident versieht außerdem die Vertretung der Europäischen Union in verschiedenen internationalen Organisationen bzw. tritt gegenüber Drittstaaten außerhalb der EU auf.

Die Republik Ungarn versieht im ersten Halbjahr 2011 erstmals die Aufgaben der Ratspräsidentschaft. Die Verrichtung dieser Aufgaben nimmt Ungarn im Rahmen einer Gruppenpräsidentschaft gemeinsam mit Spanien und Belgien wahr. In den ersten sechs Monaten dieser 18-monatigen Ratspräsidentschaft – ab 1. Januar 2010 – versieht Spanien, im zweiten Halbjahr Belgien und schließlich ab dem 1. Januar 2011 Ungarn die Aufgaben des Ratspräsidenten.

Im Sommer 2007 wurde eine Kommission zur Vorbereitung der ungarischen EU-Ratspräsidentschaft gegründet, deren Leiter der Ministerpräsident ist und zu der als Mitglieder die Leiter des Außenministeriums, des Justizministeriums, des Finanzministeriums und des Ministeriums für Soziales bzw. der Staatssekretär für Personalfragen gehören. Im Jahre 2007 hielt dieses Gremium mehrere Besprechungen und Rundtischgespräche ab, in deren Verlauf die durch die Ratspräsidentschaft gebotenen Möglichkeiten und Verpflichtungen erörtert wurden.

ZIELSETZUNGEN

Die Arbeitsstudie skizziert jene Bestrebungen, anhand derer wir die Sicherheitsfragen der Ratspräsidentschaft untersuchen können, mit besonderer Berücksichtigung der globalen Sicherheitsherausforderungen, sowie der Durchführung in- und ausländischer Sicherheitsoperationen. Heute erhält der Sicherheitsaspekt der Ratspräsidentschaft in Ungarn keine seinem Gewicht entsprechende Aufmerksamkeit.

Diese Arbeitsstudie stellt jene politischen und militärischen Aufgaben bzw. Aufgaben der nationalen Sicherheit und der öffentlichen Ordnung vor, die für die restlose Verwirklichung der mit der Ratspräsidentschaft einhergehenden Aufgaben erforderlich sind.

Für die Vorbereitung der Ratspräsidentschaft sind eine enge Zusammenarbeit der staatlichen Organe, Institutionen und Behörden, sowie die Einbeziehung der im Sicherheitsbereich involvierten zivilen Unternehmungen notwendig. Das Ziel der Erstellung dieser Arbeitsstudie ist es, dass die verschiedenen „Sicherheitsorgane und -behörden“ die für sie definierten Sicherungsaufgaben und deren Verknüpfungspunkte sowie die Anwendung der für die Sicherung der Veranstaltungen erforderlichen neuen Techniken und taktischen Elemente einheitlich interpretieren.

METHODEN

Unter Anwendung von Analysen zeige ich anhand von konkreten Fällen jene Überlegungen und Interessenverschiebungen, mit deren Hilfe sich Trends bei der Verwirklichung von Sicherungsoperationen in Bezug auf die Ratspräsidentschaft Ungarns bestimmen lassen.

Die Rollenübernahme in künftigen Sicherungsoperationen hat die Grenzen der Möglichkeiten der ungarischen Ordnungsorgane erreicht. Aufgrund des Personalmangels empfehle ich die Einbeziehung der Ungarischen Armee in die Sicherung der Veranstaltungen während der Zeit der Ratspräsidentschaft. Im Bestand der Ungarischen Armee dienen Soldaten mit spezieller fachlicher Ausbildung, die bei der Abwicklung von Veranstaltungen einer vergleichbaren Dimension eine entsprechende Unterstützung für die Ordnungsorgane gewährleisten können. Die gültige Verfassung lässt einen Inlandseinsatz der Ungarischen Armee allerdings nicht bzw. nur in Extremfällen zu.

GLOBALE SICHERHEITSHERAUSFORDERUNGEN

Der Zukunft der Europäischen Union widmet das Dokument eine besonders große Aufmerksamkeit. Der NIC[4] ist der Ansicht, dass die EU zwar über das Potenzial zur Großmacht verfüge, an einem Aufstieg aber durch mehrere Faktoren gehindert werde. Zu den wichtigsten gehören die katastrophalen demographischen Indikatoren, z.B. die alternde Bevölkerung. Deshalb müsse die Lage der Frauen am Arbeitsmarkt verbessert werden und sind die Wohlfahrtssysteme – insbesondere in Deutschland – auf eine umfassende Reform angewiesen. Wegen der ungünstigen demographischen Lage ist eine entsprechende Integration der Einwanderer von Relevanz, wobei zu berücksichtigen ist, dass die muslimische Bevölkerungszahl in der EU auf der Grundlage von Schätzungen im Jahre 2025 40 Millionen Personen ausmachen dürfte.

Der Energiebedarf der EU wird zunehmen, weshalb sie enge Beziehungen zu Russland und den Staaten Nordafrikas unterhalten muss. Den NIC-Experten zufolge könnte es passieren, dass die EU – sofern sie eine eigene militärische Kapazität aufstellt – nicht auf das militärische Potenzial der NATO angewiesen sein wird, was zur Schwächung der euroatlantischen Beziehungen führen kann, während die Gemeinschaft gleichzeitig einen neuen Verbündeten in China sucht.

Die Europäische Union ist aufgrund ihrer eigenen Bedrohtheit aktiver Teil des Kampfes gegen den internationalen Terrorismus. Eine der wichtigen Aufgaben des 21. Jahrhunderts besteht in einer breit angelegten internationalen Zusammenarbeit, weil in der sich globalisierenden Welt kein einziger Staat alleine imstande wäre, entsprechende Antworten auf die regionalen Bedrohungen und die globalen Herausforderungen zu geben.

Der entscheidende Akteur des internationalen Terrorismus ist der islamische Fundamentalismus, dessen Tätigkeit die größte Gefahr für die Europäische Union bedeutet. Das damit einhergehende Risiko muss erfasst werden, wobei wir uns auch darüber im Klaren sein müssen, mit welcher Art von Bedrohungen wir rechnen müssen.

Inhalt und Dimension der Sicherheit haben sich geändert. Die Gefahr eines weltweiten Konflikts ist auf ein Minimum gesunken, wohingegen die Zahl der Sicherheitsherausforderungen neuen Typs zugenommen hat [5]. Auf diese neue Sicherheitsrisiken mit sich bringenden Probleme kann man nur unter Anwendung neuartiger Strukturen und Mechanismen entsprechende Antworten finden. Dieser Fakt ist deshalb wichtig, weil die Europa bildenden Nationalstaaten unter Berücksichtigung ihrer Sicherheitsrisiken ihre Zusammenarbeit ständig vertieft haben, woraufhin sich eine

gemeinsame Außen- und Sicherheitspolitik und später auch Verteidigungspolitik herausbilden konnte.

SAMMELN INTERNATIONALER ERFAHRUNGEN ÜBER VERGLEICHBARE POLIZEIEINSÄTZE

Innerhalb des Innenministeriums (im Weiteren: Ministerium) müssen das ORFK und der Kommandant des Wachregiments der Republik die „Projektgruppe EU27" bilden. Die Verantwortung liegt beim Minister.

Im Jahre 2008 muss die „Projektgruppe EU27", im Weiteren EU27, mit anfänglich 4 Mitgliedern gegründet werden. Ihre Aufgabe besteht in der Vorbereitung der Sicherheitsaufgaben der Ratspräsidentschaft. Sie arbeitet das „Rahmenkonzept" der Sicherungsaufgaben der Ratspräsidentschaft aus, in der hinsichtlich der örtlichen und Landespolizei sowie der sonstigen Sicherheitsorgane definiert wird, welche Maßnahmen diese zu ergreifen haben.

Die ersten Schritte der EU27 sind das Sammeln von Erkenntnissen, vergleichbare Analysen über ungarische Polizeieinsätze und andere Spitzenereignisse, wie das Gipfeltreffen der G8 2007 in Deutschland sowie über die Erfahrungen Sloweniens mit der Ratspräsidentschaft 2008.

Nach meiner Ansicht sollte als nächster Schritt im September 2009 eine Ordnungskonferenz abgehalten und dort das „Rahmenkonzept" vorgestellt werden.

Wenn die Ordnungskonferenz ihre Meinung zu dem Material gebildet hat, sollte sie einen Vorschlag an den Minister unterbreiten. Das ausgearbeitete und durch die Konferenz angenommene Konzept wird durch den Minister wiederum dem Verteidigungs- und Ordnungsausschuss des Parlaments vorgelegt.

Nach Bewilligung durch den Ausschuss wird die zur Sicherung der Aufgaben der Ratspräsidentschaft geschaffene, provisorische Organisationseinheit *„Spezielle Vorbereitungsorganisation"* – im Weiteren *SVO* – gebildet, deren Kommandant durch den Minister für Justiz und öffentliche Ordnung benannt wird. Ihre Aufgaben bestehen in der Ausgestaltung der Struktur und Funktionsbedingungen der SVO.

Der SVO-Kommandant wird durch einen Führungsstab unterstützt, welcher Stab sich in mehrere untergeordnete Organisationseinheiten gliedert, wie beispielsweise die Gruppen zur Unterstützung des Stabs (USt).

Empfohlene Gruppen zur Unterstützung des Stabs:

- UST 1 Humangruppe
- UST 2 Aufklärergruppe
- UST 3 Operationsgruppe
- UST 4 Logistikgruppe
- UST 5 Mediengruppe
- UST 6 Führungsgruppe

In die Entscheidungsbefugnis des SVO-Kommandanten fällt es, die Aufgaben der ungarischen Verteidigungs- und Sicherheitsorgane zu bestimmen. Den provisorisch um- und untergeordneten Organen und Truppen sind klare und erfüllbare Ziele zu definieren.

Der Kommandant und/oder Leiter des Sicherheitsorgans auf einer bestimmten Ebene muss in jedem Fall die von ihm geleitete Organisation kennen. Er muss die unterstellten, um- und untergeordneten sowie verstärkenden Kräfte bzw. die Struktur der unterstützenden Einheiten, ihre Kräfte und Techniken, Möglichkeiten und Fähigkeiten kennen. Die vom SVO-Kommandanten erhaltene Aufgabe muss – nach Analyse der entstandenen Situation –

entsprechend unter den untergeordneten Personen – in Zeit und Raum – aufgeteilt werden bzw. müssen die Aufgaben der untergeordneten Personen – nach Zweck, Ort und Zeit – bestimmt werden. Die unterstellten Kommandanten, Leiter und Stäbe haben zu verstehen, dass sie diese Aufgaben mit den zur Verfügung stehenden Kräften und Techniken in der vorgegebenen Zeit zu erfüllen imstande sein müssen.

Die definierten Ziele und Aufgaben müssen also klar formuliert sein und im Verhältnis zu den Fähigkeiten und Möglichkeiten der diese ausführenden Sicherheitsorgane stehen.

Klare und erfüllbare Ziele bedeuten gleichzeitig auch, dass die Kommandanten und Leiter das wichtigste Ziel vorgeben und die Kräfte und Techniken festhalten, die zur Erfüllung dieses Hauptziels benötigt werden.

Um die vorgegebenen Ziele zu erreichen, sind die gemeinsamen Anstrengungen und die Kooperation sämtlicher an den Operationen teilnehmenden Sicherheitsorgane notwendig, was sich durch die Vorgabe klarer und erfüllbarer Ziele realisieren lässt.

Die Definition des Ziels unterstützt die Führung, weil sich eine auf Haupt- und Teilaufgaben bzw. Teilziele gegliederte Tätigkeit durch die unterstellten Kommandanten, Leiter und Stäbe leichter steuern und führen lässt. Selbstverständlich wirkt sich die Festigkeit der Führung auch auf den moralischen und psychischen Zustand des Personalbestands aus. Die Ziele werden durch die Kommandanten und Leiter der entsprechenden Ebenen rechtzeitig markiert, damit die Ausbildung und Vorbereitung der involvierten Sicherheitskräfte und -organe zeitgerecht vorgenommen werden kann. Das hat einen bedeutenden Einfluss auf die erfolgreiche Ausführung der Aufgabe.

Wirtschaftliche und effektive Nutzung der Kräfte und Techniken

Die wissenschaftlich-technische Entwicklung hat die Entwicklung und Wartung der Sicherheitsorgane erheblich verteuert. Nicht einmal in den modernsten westlichen Ländern stehen die Ressourcen unbegrenzt zur Verfügung. In Ermangelung unbegrenzter Ressourcen müssen jedoch – mit Ausnahme der Hauptaufgaben – auf anderen Gebieten sinnvolle Risiken eingegangen werden. Für die Durchführung der zweitrangigen Aufgaben sind gerade noch ausreichende Kräfte anzuwenden. Das Wirtschaften mit den Kräften und Techniken bedeutet eine zweckgerichtete Verteilung und zeitlich angepasste Anwendung der Kräfte und Techniken.

Das Prinzip der Wirtschaftlichkeit des Kräfteeinsatzes besteht darin, die für die maximale Erfüllung der Aufgaben notwendigen Kosten zu minimalisieren.

Die Ausbildung ist das effizienteste Grundelement der Wirtschaftlichkeit. Allein ein entsprechend ausgebildeter Personalbestand ist imstande, die Vorstellungen und Entscheidungen des Kommandanten und/oder Leiters restlos auszuführen. Ein gut ausgebildeter Personalbestand ist imstande, unter fachgerechtem Einsatz der technischen Instrumente, die Zahl der Fehler zu senken, und ist ebenso imstande, verletzten Kameraden fachgerechte Hilfe zu leisten und die ihm zur Anwendung anvertraute Technik auf die entsprechende Art und Weise einzusetzen.

Nach meiner Meinung kann mit der restlosen Umsetzung der Ausbildung ein wirtschaftlicher und effizienter Einsatz der Kräfte und der Technik erheblich gefördert werden. Selbstverständlich bezieht sich die Wirtschaftlichkeit auch auf das Wirtschaften mit den Humanressourcen.

Feste und einheitliche Führung

Eine feste, einheitliche, zuverlässige und stabile Führung gewährleistet während des Planungsprozesses im Interesse der gesetzten Ziele die Verteilung der Aufgaben, die Organisation der Tätigkeit und die Vorbereitung der Unterstellten bzw. während der

Anwendung die maximale und effektive Ausnutzung der Möglichkeiten der Sicherheitsorgane.

Die Führung ist dann fest und einheitlich, wenn die Kommandanten und/oder Leiter und Stäbe ihre für die zur Ausübung ihrer Position erforderlichen Kenntnisse laufend auffrischen bzw. die verschiedenen Tätigkeiten üben. Während der Übungen sind auch die während der verschiedenen Operationstätigkeiten auftretenden, nicht vorhersehbaren Ereignisse und die Reaktionen auf diese Situationen zu behandeln.

Die Kommandanten und/oder Leiter und Stäbe sollten jederzeit Klarheit über die entstandene Lage haben, ihre Entscheidungen rechtzeitig treffen und diese flexibel an Lageveränderungen angepasst umsetzen.

Die Kommandanten und Leiter der verschiedenen Führungsebenen sind persönlich verantwortlich für ihre Entscheidungen, für den zweckmäßigen und effektiven Einsatz der unterstellten Organisationen, für das Erreichen der gesteckten Ziele, die Erfüllung der übertragenen Aufgaben, sowie für die Ergebnisse bzw. die Erfolglosigkeit.

Es liegt in der Verantwortung der Kommandanten und Leiter, mit ihren Unterstellten in einer ständigen, laufenden und zuverlässigen Verbindung zu stehen, die eine Weiterleitung der benötigten Daten und Informationen sicherstellt.

Kommandanten und Leiter sollten eine vernetzte Operationsführung anstreben, den Unterstellten Möglichkeiten einräumen, selbst die Initiative zu ergreifen, bzw. die gewählten sinnvollen Risiken einzugehen, sowie dass die von ihnen geführten Organe ihre Aufgaben entschlossen und mit Initiativgeist wahrnehmen.

Sicherung der Operationen und Kooperation

Die Sicherung der Operationen ist die Gesamtheit der durch die Kommandanten, Leiter und Stäbe angeordneten Maßnahmen, die im Interesse der Verwirklichung der bei der Vorbereitung und Durchführung der Operationen für die Organe definierten Aufgaben unter den günstigsten Umständen organisiert werden.

Ziel der Sicherung ist es, die Organe gegen nicht vorhersehbare, potenzielle Bedrohungen zu schützen bzw. eine kontinuierliche, zuverlässige und effiziente Tätigkeit der Organe zu ermöglichen.

Die Sicherungsaufgabe (Operation) ist gemeinsame Aufgabe sämtlicher Sicherheitsorgane. Die Abstimmung der Tätigkeiten der verschiedenen Sicherheitsorgane, darunter speziell die Planung und Organisation der Zusammenarbeit, sowie deren Erhalt während der Durchführung, bzw. die Koordinierung sind Aufgaben der Kommandanten, Leiter und Stäbe.

Die Zusammenarbeit bedeutet im Zuge der Durchführung der Operationen eine abgestimmte Tätigkeit der an der Operation beteiligten Kräfte und Technik gemäß Aufgabe, Ausrichtung, Ort und Zeit.

In Bezug auf eine moderne Operationstätigkeit kann der Erfolg nur über einen Zusammenschluss der Kräfte und Technik der daran beteiligten verschiedenen Sicherheitsorgane, sowie eine enge und laufende Zusammenarbeit erreicht werden.

Die technischen Mittel verfügen über verschiedene Eigenschaften, spezifische Anwendungsgebiete und Möglichkeiten. Während der Operationen führen diese ihre Aufgaben zeitgleich bzw. sich gegenseitig unterstützend aus, und ergänzen einander. Der gemeinsame Einsatz technischer Mittel, die über erheblich divergierende Anwendungsmöglichkeiten verfügen, sollte vermieden werden, weil die Abstimmung der Tätigkeiten der Organe und deren Effizienz die restlose Umsetzung der Operation nicht gewährleistet.

Die Zusammenarbeit muss vom Beginn der Operationstätigkeit bis zu deren Abschluss kontinuierlich verlaufen. Bei einer Unterbrechung ist jeder Kommandant und Leiter verpflichtet, die Zusammenarbeit wiederherzustellen und neu zu organisieren.

Mit einer laufend unterhaltenen Zusammenarbeit lassen sich die Verluste bei den Organisationseinheiten verringern bzw. die psychische Belastbarkeit des Personalbestands erhöhen, während gleichzeitig die Anwendungsmöglichkeiten für Kräfte und Technik effizienter werden.

Hauptaufgabe:

- die Sicherheit der Staatsgäste und der außerordentlich gefährdeten weiteren Teilnehmer am Gipfeltreffen ist zu garantieren;
- die reibungslose Abwicklung des Gipfeltreffens ist zu gewährleisten;
- nicht vorhersehbare Straftaten und Rechtsverstöße sind zu verhindern bzw. dabei anfallende Beweisstücke aufzubewahren und sicherzustellen;
- Ordnungsstörungen sind rechtzeitig zu identifizieren und zu verhindern bzw. abzuwenden und Attacken abzuwehren;
- die Behinderung außenstehender Dritter ist auf ein Minimum zu beschränken;
- die Grenzkontrollen sind vorübergehend wiederherzustellen (Option);
- Zusammenarbeit zum Schutz öffentlicher Betriebe;
- Zusammenarbeit mit zivilen Sicherheits- und sonstigen Firmen.

Bei der Untersuchung meiner Hypothese stellte ich fest, dass eine Rollenübernahme bei künftigen Sicherheitsoperationen (Ratspräsidentschaft) die Grenzen der den ungarischen Ordnungsorganen gegebenen Möglichkeiten sprengen wird (Option). An dem akut werdenden Personalmangel konnte auch die Integration von Polizei und Grenzwache nichts ändern. Die Ungarische Armee verfügt über Soldaten mit spezieller fachlicher Ausbildung, die bei der Abwicklung wichtiger Veranstaltungen eine entsprechende Unterstützung für die Ordnungsorgane erbringen könnten. Die geltenden Gesetze lassen einen Inlandseinsatz der Ungarischen Armee nicht zu (mit Ausnahme der Unterstützung bei der Abwendung von Katastrophen), was einzig sensible Perioden ausschließt.

LITERATURVERZEICHNIS

[1] Koran (75:7-10)

[2] Gazdag Ferenc: Európai integrációs intézmények, Verlag Osiris, Budapest 2002,128 p.

[3] http://www.pmtkht.hu/eip/62_hatter.html (Heruntergeladen: 01.04.2009)

[4] http://www.cia.gov/nic/NIC_globaltrend2020.html(Heruntergeladen: 2009.10.01.)

[5] Gazdag Ferenc: Biztonságpolitika, Budapest, SVKH, 2001, 41-67 p.

HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Pataki János
janos.pataki@audi.hu

Sulányi Péter
speter@suprex.hu

LAGE- UND ANALYSEZENTRUM BEI EINEM INTERNATIONALEN UNTERNEHMEN

Abzstrakt/Abstract/Abstrakt

A publikáció célja, hogy bemutassa a vállalatoknál alkalmazható technikai objektumvédelem megvalósításának lehetőségeit. A védelem egyes elemei (az operatív központ, a központi vezérlőegység, a periférián pedig a különböző feladatokat és funkciókat ellátó alrendszerek) biztosítják azt, hogy a vállalat biztonsági helyzete mindig a megfelelő és még elfogadható kockázati szinthez igazodjon.

The publication aims to show the possibility of technical protection of companies. The certain aspects of protection (operations center, the central control unit, the various sub-tasks and functions in the periphery) ensure that the company's security situation is still appropriate and in line with acceptable risk level.

Bei Unternehmen wird der technische Objektschutz verwirklicht. Zusammen mit seinen Bausteinen (Lagezentrum als zentrale Steuereinheit, und an der Betriebsperipherie angesiedelte und unterschiedliche Aufgaben und Funktionen wahrnehmende Subsysteme) gewährleistet er das Anpassen der Sicherheitssituation der Unternehmen an einen entsprechenden und noch akzeptablen Risikograd.

Kulcsszavak/Keywords: *geoinformációs rendszer, helyzetelemző központ, operatív központ ~ geoinformation system, situation center, operational center ~ Lagezentrum, Geoinformationssystem, Schutz des Lagezentrums*

LAGE- UND ANALYSEZENTRUM[1]

Funktionen des Lage- und Analysezentrums

Die EU nahm kurz nach dem Terrorangriff vom 11. September 2001 mehr als 70 Aktionspläne an. Der Europäische Rat gab am 25. März 2004 in Brüssel eine überarbeitete Erklärung mit dem Titel „Erklärung über den Kampf gegen den Terrorismus“ heraus, in der sieben strategische Ziele formuliert wurden. Der ausgearbeitete Aktionsplan ist die Basis für ein gemeinsames Auftreten gegen den Terrorismus2.

Die herausgegebene Anlage bekräftigte in ihrer VII. Zielstellung die Rolle des SitCen3 in Bezug auf Drittstaaten. Das SitCen erhielt eine wichtige Aufgabe auf dem Gebiet der Bedrohungsbewertung, denn es geht nun darum, jene Fähigkeiten zu entwickeln, die sich für eine Analyse und Bewertung der Antiterror-Aktivitäten von Drittstaaten eignen.

Das SitCen wird rund um die Uhr an allen sieben Tagen der Woche betrieben. Egal an welchem Punkt der Welt ein Ereignis, eine Katastrophe und/oder anders geartete Gefahrensituation eintritt, die Mitarbeiter im SitCen halten die Informationen fest und erfüllen gleichzeitig damit ihre Alarm- und Berichtspflicht.

Auf der Grundlage der zur Verfügung stehenden Informationen können sie entscheiden, welche Organisationen die Information betreffen bzw. interessieren könnte. Informationsquellen können die verschiedenen maßgeblichen Nachrichtenportale sein. Natürlich kann unter Umständen auch der Einsatz von Übersetzern notwendig sein, wenn für das Verständnis der Nachrichtenquelle eine fachgerechte Übersetzung benötigt wird. Deshalb ist es unvermeidlich, dass für diese Personen ein Bereitschaftsdienst angeordnet wird.

Die wichtigen Informationen sind sofort weiterzuleiten. Dem SitCen stehen sämtliche Kommunikationskanäle (Telefon, Fax, E-Mail, Radio) zur Verfügung. Selbstverständlich dürfen die sensiblen Informationen nur auf kodierten und/oder geschützten Leitungen weitergereicht werden.

Die Mitarbeiter des SitCen unterrichten in den im Alarmplan festgelegten Fällen die betroffene(n) Person(en), bevor aufgrund einer von deren Seite getroffenen Entscheidung der schon im Vorfeld definierte Krisenstab einberufen wird.

Die SitCen-Systeme:

- GIS[4]
- Galileo[5]
- Videoüberwachungsanlage zur Kontrolle der frequentierten Gebiete des Werkes, der Umzäunungen von Objekten und Einrichtungen sowie deren Toreinfahrten
- EDR[6] zwischen Polizei, Feuerwehr, Rettungskräften und zivilen Sicherheitsdiensten
- Telefongeräte als wichtigste Kommunikationsmittel
- Einbruchmeldeanlagen
- Brandschutzsystem
- Zutrittskontrollsystem

---

[1] Lage- und Analysezentrum (Situaton Centre), im Weiteren: SitCen

[2] Bundesakademie für Sicherheitspolitik: Sicherheitspolitik in neuen Dimensionen Ergänzungsband 2, Bonn, Verlag Mittler & Sohn GmbH, 2009, Seite 203 - 441

[3] Vincze Hajnalka: Az Európai Unió biztonság- és védelempolitikai dokumentumai II., 2004-2005, Charta Press Kft., Seiten 456-467

[4] Geoinformationssystem

[5] Europäisches Satellitennavigationssystem

[6] Digitales Radionetz

Zu alarmierende Bereitschaftssysteme

- Definierte Einheiten und Untereinheiten der Sicherheitsbehörde;
- Feuerwehr;
- Rettungsdienst;
- Ziviler Sicherheitsdienst (optional);
- Bereitschaften sonstiger Behörden, in kritischer Lage;
- Bereitschaftsdienste der Stadtwerksleistungen erbringenden Unternehmen.

SitCen-Schutz

Das SitCen ist innerhalb eines gegebenen Objekts als strategisches Sicherheitsgelände zu behandeln.

Elemente des komplexen Sicherheitsschutzes:

- Mechanischer Schutz
- Elektronischer Schutz
- Wachschutz
- Administrativer Schutz.

Der SitCen-Sicherheitsschutz ist eine komplexe Tätigkeit. Es gibt keine Komponenten, die gegenüber beliebigen anderen in den Vordergrund gerückt werden könnten.

Der SitCen-Sicherheitsplan ermöglicht den Schutz des SitCen-Managements, der Angestellten, ihrer Materialien und Informationen vor unbefugten Eindringlingen und anderen Kriminellen.

Außenschutz

Die Ausgestaltung eines Außenschutzes ist in dem Objekt, in dem das SitCen tätig ist, in vollem Umfang berechtigt. Die Anlage der Umzäunung bietet einen entsprechenden mechanischen Schutz gegen unbefugte Eindringlinge, weil sie sich nur mit ernsthaften Anstrengungen bzw. unter Einsatz verschiedener Hilfsmittel bewältigen lässt. Die Beleuchtung der Umzäunung sichert den Wachleuten die systematische Beobachtung zu.

Der elektronische Schutz der Umzäunungen besteht aus Bewegungsmeldern und einem Kamerasystem und funktioniert vollkommen automatisch. Bei einem Stromausfall besteht die Möglichkeit zur Beobachtung der Umzäunung im Infrarot-Betrieb des Kamerasystems. Zum Umzäunungsschutzsystem gehört eine vom Objektschutzdienst bestimmte Eingreiftruppe, die aus 2-3 Sicherheitsleuten besteht.

Parkmöglichkeiten

Geparkt werden darf in der unmittelbaren Umgebung des Objekts nur mit einem zum Objekt gehörenden Dienstwagen. Auf das Armaturenbrett der Fahrzeuge ist die ständige Eintrittsberechtigung des Fahrzeugs zu positionieren. Das dient in erster Linie einem Vorbeugen von Abhörversuchen und Terrorhandlungen.

Pflanzen

Dicht wachsende Sträucher und rankende Pflanzen müssen in unmittelbarer Nähe des Gebäudes kurz geschnitten werden, um die Möglichkeiten für unbefugte Eindringlinge zu verringern, sich im Dickicht tarnen zu können. Bäume sind im Umfeld des Gebäudes so anzupflanzen, dass keine Möglichkeit besteht, von den Bäumen über Fenster des Gebäudes oder andere Öffnungen einzudringen.

Blumenrabatten und Blumenkörbe in den Fenstern anzubringen ist verboten.

Diese Vorschriften muss der Objektschutzdienst regelmäßig kontrollieren.

Der SitCen-Werkschutz (Option)

Ein entsprechender Pfortendienst ist ein gewichtiger Präventionsfaktor. Der Pfortendienst besteht aus 2 Wächtern.

Aufstellungsort: Vorhalle am SitCen-Haupteingang
Dienstzeit: Laufend, mit 12-Stunden-Wechseln
Aufgabe:

- - Verrichten allgemeiner Wach- und Schutzaufgaben;
- - Überwachung des am SitCen-Eingang installierten Einlass-Systems;
- - Kontrolle der Berechtigungen der sich innerhalb der administrativen Zonen aufhaltenden Personen;
- - Kontrolle von Anlieferungen (z.B. Catering[7], Reinigungspersonal);
- - Kontrolle des verschlossenen Zustandes der Räumlichkeiten am Ende der Arbeitszeit;
- - Wahrnehmung weiterer Aufgaben aufgrund von Anweisungen.

Internes Schutzsystem

Basis des internen Schutzsystems ist eine komplexe Anwendung des mechanischen, elektronischen und humanen Wachschutzes.

Mechanischer Schutz:

Türen und Tore (mit Ausnahme des Haupteingangs) im Erdgeschoss sind so auszugestalten, dass sie nur von innen geöffnet werden können. Fenster im Erdgeschoss dürfen über keine Öffnungstechnik verfügen. In sicherheitstechnisch sensiblen Räumlichkeiten sind Sicherheitsfenster (vom Typ A1) zu installieren.

Elektronischer Schutz:

Die Alarmsignale der zur Installation gelangenden elektronischen Schutzanlagen gelangen in die Zentrale des Objektschutzdienstes, wo sie mit dem integrierten Überwachungssystem zusammenfließen. Bei Alarm unterrichten die Mitarbeiter der Zentrale des Objektschutzdienstes die Eingreiftruppe des Objektschutzdienstes und den SitCen-Pfortendienst.

Die elektronischen Schutzsysteme sind mit einem Notstromaggregat für einen 72-Stunden-Betrieb auszustatten.

A) Einbruchsmelder:

Im Erdgeschoss sind alle Räumlichkeiten mit passiven Infrabewegungsmeldern zu versehen, die über nach außen öffnende Türen- und Fensteröffnungen (Türen, Tore, Belüftungsschächte usw.) verfügen. Deren Installation hat in Kenntnis der zu erwartenden Einbruchsrichtung unter Berücksichtigung ihrer charakteristischen Sensibilitätscharakteristik an optimierten Stellen zu erfolgen.

Die eingesetzten passiven Infrabewegungsmelder müssen über Sabotageschutz, die Möglichkeit der Sperrung der Rückmeldungs-LED, duale PIR-Batterien, Wärmekompensation und mindestens RF-Schutz der Größe 10 V/m verfügen und auf der Frequenz 1 MHz funktionieren.

[7] Bereitstellung von Speisen und Getränken, Gastgewerbe

Türen und Fenster im Erdgeschoss müssen mit Öffnungssensoren ausgestattet werden. Die Türen zur sensiblen Sicherheitszone innerhalb des Gebäudes sind mit einer zum Einlass-System gehörenden Lesevorrichtung auszustatten. Diese Vorrichtung funktioniert bei einem unbefugten Eindringen als Alarmanlage.

B) Videokameras:

Videokameras sind anzubringen im Erdgeschoss bei den mit Öffnungssensoren ausgestatteten Türen und Fenstern, auf den Fluren, am Eingang zu den Räumlichkeiten mit sensiblem Sicherheitsschutz sowie am Haupteingang. Das Videosystem muss Echtzeitbilder an die Zentrale des Objektschutzdienstes weiterleiten bzw. im automatischen Modus betrieben werden. Das heißt, dass sofort eine Aufnahme vom Alarmort gestartet und der Ort sowie die Art des Alarms graphisch für die Mitarbeiter der Zentrale des Objektschutzdienstes dargestellt werden, wenn ein Alarm von den Einbruchssensoren gemeldet wird. Der betreffende Mitarbeiter informiert den Objektschutzdienst über den entsprechenden Fall.

Einlass-System

Das SitCen-Einlasssystem ist eng mit dem Objekteinlasssystem verknüpft. Es muss eine allgemeine Regelung für das gesamte Objekt ausgearbeitet werden, die um eine spezielle Ordnung zu ergänzen ist, welche ausschließlich für das SitCen und das Datenverarbeitungszentrum[8] gilt.

Innerhalb des Objektes unterscheiden wir 4 Eintrittskategorien:

- Mitarbeiter des SitCen und des Datenverarbeitungszentrums;
- zu anderen Organen gehörende Personen;
- vor Ort tätige Mitarbeiter externer Unternehmen;
- Besucher.

Die in die ersten drei Kategorien fallenden Personen erhalten ständige Einlassgenehmigungen, die Besucher der vierten Kategorie Karten mit der Aufschrift „VISITOR"[9].

Personen mit ständiger Einlassgenehmigung können durch das Terminal an der Tür in der SitCen-Vorhalle in die Sicherheitszone eintreten.

Besucher können durch das Haupttor auf das Objektgelände gelangen. Der Besucher zeigt dem Pförtner, der Dienst am Haupttor leistet, seine Absicht an, einen Besuch im SitCen zu machen. Daraufhin ruft der Pförtner den SitCen-Leiter an und fragt, ob der Besucher empfangen werden kann und wer diesen begleiten wird. Nach erfolgter Genehmigung wird mit der vor Ort installierten Vorrichtung zur Herstellung von Besucherkarten eine Karte mit der Aufschrift „VISITOR" angefertigt, während der Pförtner und/oder der Sicherheitsmann gleichzeitig kontrolliert, ob der Besucher korrekte Angaben zur Erstellung der Karte gemacht hat. Nach sichtbarem Anbringen der Karte darf der Besucher in Begleitung einer im SitCen Dienst leistenden Person auf das SitCen-Gelände eintreten, nachdem eine Kontrolle durch den Pfortendienst geschehen ist.

Gruppenbesuche auf dem Gelände des SitCen und des Datenverarbeitungszentrums sind nur mit Genehmigung des Leiters der betreffenden Organisationseinheit möglich.

Beim Betreten und Verlassen des Geländes ist der Pfortendienst verpflichtet, das Handgepäck zu kontrollieren.

---

[8] Serverraum

[9] Besucher

Objektschutz

Die Beförderung von Materialien, Dokumenten und elektronischen Tonträgern nach draußen darf ausschließlich mit Sondergenehmigung durch den Leiter der betreffenden Organisationseinheit erfolgen.

Die Eingreiftruppe des Objektschutzdienstes und der Pfortendienst sind zu alarmieren, wenn Personen wahrgenommen werden, die sich verdächtig verhalten, bzw. wenn verdächtig erscheinende Gegenstände entdeckt werden.

Schlüsselordnung und Schließaufgaben

Die Schlüsselordnung und die Schließaufgaben sind organisch mit dem Schließsystem des Objektschutzes verbunden.

Verwaltung

Es ist entscheidend, dass das Objekt über eine entsprechende Verwaltung verfügt. Dem Facility Management[10] sind die Namenslisten und Daten der durch den SitCen-Leiter zur Ausübung von Verwaltungsaufgaben benannten Personen zu übergeben, die erst nach erfolgter Kontrolle eine ständige Einlassgenehmigung in das Gebäude erhalten können.

Die Mitarbeiter der Verwaltung dürfen die sensiblen Sicherheitszonen nur während der Arbeitszeit und zu Wartungszwecken (z.B. Reinigung, Fehlerbehebung) unter Aufsicht der dort ihren Dienst leistenden Personen aufsuchen.

Außerhalb der Arbeitszeit dürfen sie nur in Anwesenheit des Sicherheitsmannes in Räumlichkeiten mit sensiblem Sicherheitsschutz eintreten, wofür eine Genehmigung der SitCen-Mitarbeiter erforderlich ist. Über dieses Ereignis ist ein Protokoll aufzunehmen, in welchem der Name der die Zone betretenden Personen, der Grund für den Zutritt, die Zeitdauer des Aufenthaltes in der Zone bzw. Name und Position der dies genehmigenden Person aufzuführen sind.

Zum Schutz des Datenverarbeitungszentrums sind die oben genannten Maßnahmen wegen der weitreichenden und strategischen Rolle des SitCen zu ergänzen.

Schutz des Datenverarbeitungszentrums[11]:

- Die Tür ist mit einem elektronischen Öffnungssensor und einer mit dem Einlasssystem verknüpften Lesekarte zu versehen;
- Innerhalb des Raums sind mehrere passive Infrabewegungsmelder und mehrere Videokameras zu installieren. Die Videokameras sind so zu installieren, dass die Identität der eintretenden Person in jedem Fall festgestellt werden kann;
- Automatische Feuermelde- und automatische Gaslöschanlage;
- Möglichkeit zum Stromabschalten;
- Bei Stromabschaltungen darf das Notstromaggregat den Strom nicht wieder zuschalten;
- Systematische Datenrettung;
- Durch den Raum und in dessen Nähe dürfen keine Infrastrukturkabel verlegt werden;
- „Blitzschutz", Tieferdung;
- Installation einer Faraday-Zelle gegen Ausstrahlung.

[10] Organisationseinheit oder Firma zur Verwaltung und Bewirtschaftung von Gebäuden
[11] Serverraum

Schutz des Tresorraums:

- Die Tür zum Tresorraum ist durch eine Stahlplatte zu verstärken und mit einem an vier Punkten schließenden Sicherheitsschloss mit Kreuzband und bohrsicherem Zylinderschloss zu versehen;
- Die Tür ist mit einem elektronischen Öffnungssensor und einer mit dem Einlasssystem verknüpften Lesekarte zu versehen;
- Innerhalb des Raums sind mehrere passive Infrabewegungsmelder und mehrere Videokameras zu installieren. Die Videokamera ist so zu installieren, dass die Identität der eintretenden Person in jedem Fall festgestellt werden kann;
- Automatische Feuermelde- und automatische Gaslöschanlage.

Ausarbeitung der für den Betrieb notwendigen Anweisungen, Ordnungen und Prozesse

Die global oder auf regionalem Gebiet eintretenden Ereignisse haben die durch die betreffenden Organisationen benannten Personen oder die das Ereignis wahrnehmenden Personen unverzüglich an den Leiter (Kommandanten) der strukturell betroffenen Organisation zu melden, wobei außerhalb der Arbeitszeit und an arbeitsfreien Tagen das SitCen-Personal – in Abhängigkeit vom Charakter des Ereignisses – der Berichts-, Melde- und Alarmpflicht nachkommt.

Als außerordentliches Ereignis ist anzusehen

- jedes im Gebiet der Region eintretende Ereignis, das eine die Sicherheit der Republik Ungarn gefährdende Handlung darstellt;
- Ereignisse, die den laufenden Betrieb des Landes behindern und deren Auswirkungen (auf Landesebene) bedeutend sind;
- Ereignisse, die mit beträchtlichen Umweltschäden einhergehen (Wasser-, Luft-, Bodenverschmutzung usw.);
- Naturkatastrophen, die das komplette Landesterritorium oder einen erheblichen Teil davon gefährden (Vis major);
- Explosionen und Brände größeren Ausmaßes;
- Betriebsunfälle, Unfälle mit Luft-, Bahn- oder Straßenfahrzeugen sowie einstürzende Gebäude mit tödlichem Ausgang oder zahlreichen (mehr als 10) Verletzten;
- Epidemieartige Erkrankungen, gesundheitsschädigende Umstände für Menschenmassen (Lebensmittel-, Gasvergiftungen usw.).

Tätigkeitsordnung bei Eintreten eines außerordentlichen Ereignisses

Sollte jemand Vorabinformationen über das erwartete Eintreffen eines außerordentlichen Ereignisses besitzen, ist er verpflichtet, diese zwecks Einleitung der erforderlichen vorbeugenden Maßnahmen unverzüglich dem SitCen-Leiter zur Verfügung zu stellen.

Die wichtigsten Maßnahmen:

- Alarm, Warnung der gefährdeten Personen, Alarm für bestimmte Personen und/oder Organisationen;
- Organisation der Lebensrettungsaktion, Unterrichtung der medizinischen Dienste, Organisation der Ersten Hilfe, Aufbau eines mobilen Krankenhauses;
- Stromabschaltung der betroffenen Stromnetze und Objekte;
- Schließen der Gas- und Kraftstoffleitungen;
- Bereitstellung der zur Schadensbehebung notwendigen Fachleute, Arbeitskräfte und Techniken sowie von Materialien zur Schadenslinderung;
- Organisation der Aufrechterhaltung der Ordnung;
- Rettung materieller Güter;
- Untersuchung des Ortes des außerordentlichen Ereignisses, Klärung der Personalverhältnisse, Schadenserhebung;
- Untersuchung des Ereignisses durch die zuständigen Behörden und Wiederherstellung der ursprünglichen Situation.

Schlussfolgerungen:

Die Region und das Land als Ganzes, sowie die Gelände der strategischen Objekte und Einrichtungen bzw. die rechtzeitig erkannten, potenziellen Gefahrenquellen sind laufend zu kontrollieren. Für derartige Aufgaben ist eine schnell einsetzbare, verantwortlich handelnde Einheit von Seiten der betreffenden Sicherheitsorgane zu bestimmen.

Es sind Informationen über die eingeleiteten Sicherheitsmaßnahmen, über einen besonderen Schutz verlangende Veranstaltungen sowie über den allgemeinen Geländeschutz auszugeben.

ZUSAMMENFASSUNG

Wir haben in unserer Studie den Aufbau, die Funktionen, den Betrieb und die Aufgaben einer Lageanalysezentrale dargestellt, die in der Lage ist, den Anforderungen des XXI. Jahrhunderts zu entsprechen.

Betrieben durch einen belegten und eigenen Algorithmus entspricht die SitCen so den Herausforderungen.

Literaturverzeichnis

[1] Bundesakademie für Sicherheitspolitik: Sicherheitspolitik in neuen Dimensionen, Ergänzungsband 2, Bonn, Verlag Mittler & Sohn GmbH, 2009

[2] Vincze Hajnalka: Az Európai Unió biztonság- és védelempolitikai dokumentumai II., 2004-2005, Charta Press Kft.

[3] János PATAKI – Péter SULÁNYI : Personenschutz, Abhandlung, Militär-Ingenieur, Budapest, 2011