Tanka László, Endrődi István (szerk.)

A katasztrófavédelem informatikai rendszerei

Dialóg Campus

UNI KÖNYVEK

A katasztrófavédelem informatikai rendszerei

Tanka László, Endrődi István (szerk.)

A KATASZTRÓFAVÉDELEM INFORMATIKAI RENDSZEREI

Dialóg Campus Kiadó ❖ Budapest, 2016

Szerzők:
Endrődi István
His Imre
Horváth Ferenc
Horváth Krisztina
Tanka László
Turányi Zoltán

Szerkesztők:
Endrődi István
Tanka László

Szakmai lektor:
Négyesi Imre

© Dialóg Campus Kiadó, 2016
© Szerzők, 2016

A mű szerzői jogilag védett. Minden jog, így különösen a sokszorosítás, terjesztés és fordítás joga fenntartva. A mű a kiadó írásbeli hozzájárulása nélkül részeiben sem reprodukálható, elektronikus rendszerek felhasználásával nem dolgozható fel, azokban nem tárolható, azokkal nem sokszorosítható és nem terjeszthető.

Tartalomjegyzék

ELŐSZÓ 7

1. A KATASZTRÓFAVÉDELEM INFORMATIKAI RENDSZEREI 9

1.1. Bevezetés 9
1.2. Informatikai biztonság 9
1.2.1. Informatikai biztonság humán szempontból 9
1.2.2. Informatikai biztonsági politika 12
1.2.3. Informatikai biztonsági szabályzat (IBSZ) 13
1.3. Az informatikai biztonság megvalósulása 13
1.3.1. Informatikai üzemeltetési szabályzat 14
1.3.2. Vírusvédelmi szabályzat 14
1.3.3. Mentési és archiválási szabályzat 14
1.4. A felhasználói jogosultságkezelés szabályai 15
1.4.1. Informatikai objektumvédelmi szabályzat 15
1.4.2. Informatikai katasztrófaelhárítási terv 15
1.5. Hálózatüzemeltetés és rendszerfelügyelet 15
1.6. Integrált eszközök és hálózatok 16
1.7. Végpontvédelem 16
1.8. Informatikai hálózatok 16

2. A BM OKF SZAKRENDSZEREI 17

2.1. Iparibaleset-megelőzési információs rendszer 17
2.2. Safety program 17
2.3. A nukleáris baleset-elhárításhoz kapcsolódó rendszerek 18
2.4. A Nemzetközi Regionális Radiológiai Adatcsere Központ rendszer 18
2.5. Az Országos Nukleárisbaleset-elhárítási Rendszer 18
2.6. Az OSJER − országos radiológiai távmérő hálózat 19
2.7. EURDEP projekt 20
2.8. Forrás – SQL integrált pénzügyi rendszer 20
2.9. Zárt levelezőrendszer: katved.gov 21
2.10. A BM OKF intranet portálja 21
2.11. Syrius helyett RobotZsaru 22
2.12. Személyzeti Nyilvántartó Országos Rendszer (SZENYOR) 22
2.13. Honlap, közösségi média 22
2.14. Határidős Jelentések Tára 24
2.15. HUNOR/HUSZÁR riasztási rendszer 24

3. A KATASZTRÓFAVÉDELEM INFORMATIKAI FEJLESZTÉSEI 25

3.1. A katasztrófavédelem központi informatikai rendszereinek felépítése 25
3.1.1. Katasztrófavédelmi Adatszolgáltatási Program (KAP-ONLINE) 26
3.1.2. PAJZS 27
3.1.3. PAJZS MINI 30
3.1.4. Szolgálatösszesítő szoftver 31
3.1.5. HADAR 31
3.1.6. HELIOS 31
3.1.7. Szolgálati gépjárművek nyilvántartása 32

3.1.8. A veszélyes áruk szállításának kezelése 34
3.1.9. VÉSZ 35
3.1.10. TAVIHAR 36
3.1.11. Marathon Terra 36
3.2. Térinformatika 37
3.2.1. Térinformatika a katasztrófavédelemnél 38
3.2.2. Térinformatikai Katasztrófavédelmi Publikációk (TÉRKAPU) 39
4. A KATASZTRÓFAVÉDELEM TÁVKÖZLÉSI RENDSZEREI 41
4.1. Bevezetés 41
4.2. Katasztrófavédelmi Távbeszélő Rendszer 41
4.2.1. Vezetékes távközlés 41
4.2.2. GSM 44
4.3. A katasztrófavédelem és az EDR 44
4.4. Lakossági riasztás és tájékoztatás 46
4.4.1. Lakossági riasztó végpontok (motoros szirénák) 47
4.4.2. Az LTRR (Lakossági Tájékoztató és Riasztórendszer) 50
4.4.3. Viharjelző rendszerek 52
4.4.4. A MoLaRi (Monitoring és Lakossági Riasztórendszer) 53
4.5. A lakosság veszélyhelyzeti riasztását, tájékoztatását szolgáló egyéb eszközök, rendszerek, szolgáltatások 56
4.6. Mobil vezetési pontok 57
FELHASZNÁLT IRODALOM ÉS JOGFORRÁSOK 59

ELŐSZÓ

Jelen jegyzet a katasztrófavédelem informatikai szakterületéhez tartozó feladatok bemutatását foglalja magában. Egyedi módon a BM Országos Katasztrófavédelmi Főigazgatóságnál az informatikai szakterület a más szervezeteknél megszokottnál sokkal szélesebb palettával rendelkezik, s ez elsősorban a katasztrófavédelem alapfeladataiból, speciális rendeltetéséből fakad. A dokumentum, a BM OKF Informatikai Főosztály szervezeti felépítését követve, a rendszerfelügyeleti, fejlesztési és távközlési szakterületek anyagaira tagozódik.

Az informatikai szakterület a katasztrófavédelem valamennyi szervezeti egységének a munkáját támogatja, de elsősorban a szakmai szervezetek (tűzoltóság, polgári védelem, iparbiztonság) munkáját igyekszik hatékonyabbá, egyszerűbbé, gyorsabbá tenni. Ennek a célnak csak úgy lehet megfelelni, ha a kapcsolat folyamatos a szakmai szervezetek és az informatika között, a fejlesztések nem öncélúak, hanem valós szakmai igényeket szolgálnak ki. A rohamos technikai fejlődés megköveteli az állandó fejlesztést, de ez egy ördögi kör lehet, hiszen egy indokolatlan beszerzési spirált indíthat el (új hardver > új szoftver > még újabb hardver > még újabb szoftver…) Épp ezért szükséges úgynevezett mérföldköveket lerakni, s ezeket minden lépésnél szem előtt tartani úgy, hogy a fejlesztési irány mindig arra mutasson, még akkor is, ha például pénzügyi okokból csak kis lépésekben lehet haladni.

A fentiekből adódóan nagyon fontos, hogy az informatikai szakterület tisztában legyen a szakmai munkával, átlássa a folyamatokat. Ugyanakkor az is elengedhetetlen, hogy az informatika által kiszolgált szervezetek ismerjék a lehetőségeiket, a meglévő és fejlesztés alatt álló rendszereket. E jegyzet ebben próbálja segíteni az olvasókat.

A szerzők

1. A katasztrófavédelem informatikai rendszerei

1.1. Bevezetés

A BM Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: BM OKF) országos hatáskörrel rendelkező szervezet, Magyarország területén elszórtan elhelyezkedő alárendelt szervekkel, amelyek a kormányzati gerinchálózatot használva állnak kapcsolatban egymással, összesen mintegy 200 telephellyel, ezen keresztül zajlik az adat- és hangátvitel. A BM OKF önmaga, alárendelt szervei és engedélyezett külső szervezetek számára központi szolgáltatásokat biztosít, például elektronikus levelezés, központi vírusvédelem, ügyviteli rendszer, térinformatikai szolgáltatás és egyéb, a napi folyamatos munkavégzéshez, illetve a veszélyhelyzeti időszakban ellátott tevékenységekhez szükséges szolgáltatások. A központi szolgáltatások jellege és a törvényi háttér is megköveteli a különböző, működést szabályozó rendelkezések meglétét és alkalmazását, amelyek az informatikai biztonság alapjait képezik.[1]

A BM OKF vezetése kötelességének tekinti az informatikai rendszerek, valamint az azokban kezelt adatok bizalmasságának, hitelességének, sértetlenségének, funkcionalitásának és rendelkezésére állásának zárt, teljes körű és folytonos, valamint a kockázatokkal arányos védelmét, azaz az informatikai biztonság megteremtését, fenntartását, és erre minden munkatársát kötelezi.

Ennek érdekében a szükséges utasításokat, rendelkezéseket, valamint szabályzatokat kiadja és karbantartja, kiépíti és működteti a védelem adminisztratív, személyi biztonsági, technikai, fizikai, kommunikációs, ellenőrzési rendszerét, és ehhez biztosítja a szükséges anyagi, technikai, információs és emberi erőforrásokat.

A katasztrófavédelem különböző szakterületei és háttérintézményei, külső partnerei, illetve a hazai védekezésben részt vevő más szervezetek feladatainak támogatása érdekében különböző informatikai rendszereket használ.[2] Ezeket alapvetően három csoportra lehet osztani:

- operációs rendszerek, irodai alkalmazások;
- más gyártótól származó, illetve kötelezően előírt informatikai rendszerek, amelyek a rendészeti ágazaton belül egységesek;
- a katasztrófavédelemre jellemző speciális szakrendszerek.

A katasztrófavédelem informatikai szakterülete ezeket üzemelteti, felel elérhetőségükért és biztonságukért.

1.2. Informatikai biztonság

1.2.1. Informatikai biztonság humán szempontból

A felhasználó kényelme, ismerethiánya, gondatlansága sok esetben ellentétes az informatikai biztonsággal. Ezt nem tudják megoldani még a legmodernebb technikák sem, képzéssel, megelőzéssel, szabályozással lehet a kockázatot csökkenteni, valamint megfelelő technikai megoldásokkal, amelyekkel a felhasználó tevékenységeiből adódó biztonsági rések számát lehet csökkenteni. *A leggyengébb láncszem az ember!*

A biztonsági kockázatok többségét az emberi tényezők és a felhasználói szokások okozzák. Az IT-biztonsági szakemberek gyakran szembesülnek olyan problémákkal, amelyek biztonságtudatos gondolkodással

1 3/2016. (IV. 29.) BM OKF utasítás a BM Országos Katasztrófavédelmi Főigazgatóság Szervezeti és Működési Szabályzatának kiadásáról.
2 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról.

legtöbbször kiküszöbölhetők lennének. Egy kutatás szerint a vállalati felhasználók akár kétharmada is úgy gondolja, hogy megfelelően tájékozott az internetes veszélyforrásokkal kapcsolatban, illetve hogy vállalatánál megfelelően védett az aktuális biztonsági veszélyekkel szemben. Az említett tanulmány egyik következtetése, hogy a legnagyobb kockázatot a felhasználók hamis biztonságtudata jelenti. Három válaszadóból kettő vallotta azt, hogy teljes mértékben tudatában van a biztonsági szempontoknak, de a gyakorlatban tanúsított magatartása gyakran rácáfolt erre. A legtöbb probléma azoknál a felhasználóknál jelentkezik, akik számítógépüket nem csupán a vállalat ellenőrzött körülményei között használják, hanem laptopjukat hazavihetik, és azt családtagjaik magáncélokra is használják.

Sokan elismerik, hogy otthoni munkavégzéskor nem saját előfizetésű, biztonságos módon védett vezeték nélküli hálózatot használnak, hanem illegálisan, a környéken elérhető hálózatok egyikét. Mindennek az az oka, hogy a felhasználók megbíznak a nyitott wifirendszerek biztonságában. A leggyengébb láncszem elve alapján egy vállalatnál elegendő csupán néhány olyan felhasználó, aki nem tartja be a biztonsági kódexek alapkövét, és a gyanús e-mailek csatolmányait felelőtlenül megnyitva különböző káros programokkal fertőzi meg a hálózatot.

Magyarországon egyre több végfelhasználó használja az informatikai eszközök és szolgáltatások egyre szélesebb körét, így egyre többet találkoznak biztonsági problémákkal (vírusok, férgek, spam, phishing, malware stb.). Az IT-biztonsági problémák Magyarországra is ugyanúgy igazak, mint más európai országokra, hiszen az emberi tényezőben nincs számottevő eltérés. A védelmet a cégek hazánkban is rendszerint egy eszköz/szoftver kombinációjaként képzelik el, amely a konkrét támadást felismeri és megakadályozza, nem pedig úgy, mint egy tudatos tevékenységet, amellyel megelőzhető a konkrét támadás. Ezzel párhuzamosasan az alkalmazottak a céges informatikai eszközeikre úgy tekintenek, mint a nekik mint alkalmazottaknak járó szolgáltatásra, ezért nehezen fogadnak el bármilyen korlátozást.

A biztonsági kérdések a cégek méretével, a nyújtott vagy igénybe vett IT-szolgáltatások mennyiségével arányosan jelentkeznek. Míg a nagyvállalatok sok esetben tudatában vannak e veszélyforrásnak, és megfelelő módon védekeznek ellene, addig a cégméret csökkenésével – az IT-kérdések egyre kevésbé intézményesített jellegéből adódóan – mindinkább kitettek a fentiekben felsorolt biztonsági kockázatoknak. Mindazonáltal a valós veszély akkor jelentkezik, amikor a cégek az üzleti folyamataikat elektronikus útra terelik, így ezek elérhetővé válnak az egyébként is sebezhető hálózatokon keresztül. A vállalatoknál bekövetkező biztonsági események jelentős része belső eredetű, azaz a cégen belülről származó információ vagy tudás felhasználásával történik. A támadások rendszerint a legsebezhetőbb ponton következnek be, s ez nemcsak a technológia lehet, hanem az azt üzemeltető vagy használó ember is. A biztonsági kérdések megválaszolásakor fontos az eszköz és a felhasználó kapcsolata, hiszen egy védelmi eszköz nem ér semmit, ha azt rosszul használják vagy megkerülik.

Az üzemeltetők és a felhasználók számára meg kell mutatni, hogy milyen veszélyek leselkednek rájuk, milyen támadási formák veszélyeztetik őket, és hogy miként lehet ezek ellen védekezni. Fontos tudniuk, hogy a védekezésből milyen szerep hárul rájuk, azaz hogy ők személyesen mit tehetnek annak érdekében, hogy ne az ő tevékenységük jelentsen kockázatot, ne az a tevékenység legyen a leggyengébb láncszem.

A nem megfelelően megválasztott jelszavak megkönnyítik a számítógépekbe, rendszerekbe való illetéktelen bejutást. Jelszóbiztonsági házirend alkalmazásával megnehezíthető és meggátolható az esetleges illetéktelen hozzáférés. A biztonsági előírások, házirendek minden menedzselt számítógépen érvényesülnek, így lehetőség nyílik a központi szabályozásra.

A kalózszoftverek alkalmazása biztos út lehet egy rendszer összeomlásához, a gépen tárolt kényes adatok megszerzéséhez, így ez szintén valós veszélyforrást jelent. Rengeteg olyan program létezik, amely ugyan kísértetiesen hasonló megjelenésű, mint az eredeti, de annak egy kártékony kóddal fertőzött verziója, és feltelepítés után, akár a felhasználó tudta nélkül óriási károkat okozhat.

A felhasználók viselkedéséből származó veszélyek a leghatékonyabban úgy küszöbölhetők ki, ha a rendelkezésre álló modern technológiákkal a cégek a lehető legkisebbre csökkentik az ember – mint a leggyengébb láncszem – jelentette kockázati tényezőket. E megoldások lényege az, hogy a cég által definiált biztonsági követelményeknek való megfelelést folyamatosan ellenőrizni kell, azok betartását ki kell kényszeríteni. Például a jelszó beírása helyett vagy mellett a munkaállomás kártyaolvasójába be kell helyezni a belépőkártyát, amely az épületen belüli közlekedést is biztosítja, így, ha a felhasználó elhagyja munkahelyét, a kártyáját magával kell vinnie. A kártya eltávolítása az olvasóból azonnal lezárja a munkaállomást. A távmunkát végző alkalmazott munkaállomásának védelméről is gondoskodni kell (tűzfal, behatolásfigyelő, vírusvédelem stb. telepítésével),

és ajánlott, hogy bejelentkezni is csak akkor tudjon a céges védett hálózatba, ha az előírások szerint működik a kialakított védelem.

Meg kell erősíteni az informatika stratégiai szerepét. Ehhez a szakembereknek mindent el kell követniük, hogy a felhasználókkal szorosabb kapcsolatot kiépítve hathatósabb védelmet biztosítsanak a vállalat működését veszélyeztető támadásokkal szemben. Az informatikusok előtt álló nagy lehetőség és egyben feladat, hogy a korábbi támogató, reaktív szerepükön pozitív irányba változtassanak. A szakemberek feladata, hogy állandó párbeszédet folytassanak a felhasználókkal, olyan képzési programokat vezessenek be, amelyek alkalmazkodnak a felhasználói csoportok sajátosságaihoz, illetve hogy a leginkább bevált biztonsági gyakorlatokat a vállalati kultúra szerves részévé tegyék. Magyarországon sajnos általánosnak mondható, hogy a cégvezetők nem tartják cégükre nézve kockázatnak a kiberbűnözést. A cégek többsége úgy gondolja, túl kicsi ahhoz, hogy támadás célpontja legyen. Nos, kkv akkor lesz célpont, amikor nagyobb cég beszállítójává válik. A támadók azt vélelmezik (joggal), hogy nála gyengébb a védelem, amelyen keresztül a nagyobb cég adataihoz is hozzá lehet férni. *A mentalitáson kell változtatni!*

2016 februárjában jelent meg a Nemzeti Kibervédelmi Intézet (NKI) 2015. évi jelentése. Eszerint ötezer magyar weboldalt ért tavaly támadás, jellemzően a tartalom megváltoztatása („deface”), illetve túlterhelés formájában. Gyakoriak a zsaroló szándékú támadások, és az adatlopási kísérletek, például hazai banki ügyfelek ellen. Szerencsére ez utóbbiak még mindig primitívek, Google Translate-ből származó, alig érthető szövegűek, ezért a pénzintézetek azonnal ki tudnak adni figyelmeztetést – a gyakoriság miatt az ügyfelek nagy része már pontosan tudja, hogy a bank soha nem kér azonosítókat sem telefonon, sem e-mailben.

A sárga szalag

Mi az alapvető különbség a nemzetközi és a hazai hozzáállás között? A következő példa ezt mutatja be: Csőtörés történt. Külföldön kiássák a gödröt, megjavítják a csövet, és amíg be nem temetik a gödröt, addig körberakják olyan betontömbökkel, amelyek az autópályákon a sávokat elválasztják. Magyarországon odatesznek négy műanyag oszlopot, és körbekerítik a gödröt egy – jó esetben – élénk színű szalaggal. Külföldön akkor sem tud beleesni az ember, ha nagyon akar, mert nekiütközik a betontömbnek, itthon meg akár halálra is zúzhatja magát a mélyben. Melyik a szimpatikusabb? A hazai megoldás nagyságrendekkel olcsóbb…

A támadó

A laikusok úgy képzelik el a hackereket, hogy azok éjt nappallá téve a számítógép előtt gubbasztanak, és biztonsági réseket keresnek informatikai rendszereken, számítógépes hálózatokon. Viszonylag ritka alkalom, hogy a laikus közvélemény ilyen közel járjon a valósághoz: a hackerek tényleg éjt nappallá téve ott gubbasztanak a komputerük előtt, és hibák, sérülések, rések után kutatnak a kibertérben.

A kiberbűnöző, amikor támad, mindig a leggyengébb láncszemet, tehát általában az embert veszi célba. Támadás előtt passzív vagy aktív információszerzéssel összegyűjt minden, nyilvánosan elérhető információt a célpontról. Nagyon sokan önként és tömegével osztanak meg magukról fontos, személyes információkat a közösségi oldalakon. Nem ritka az olyan felhasználó, aki teljes részletességgel felteszi családja összes személyes adatát a Facebookra. Ezek az információk kincsesbányák például azok számára, akik belépési jelszavakat próbálgatnak (vagy arra kíváncsiak, mikor megy nyaralni a leendő áldozat). De akadnak, akiknél még ennyi fifikára sincs szükség. Egy felmérés szerint ugyanis az interneten fellelhető jelszavak egy százaléka a következő: 123456. Nagyon sok esetben telepítéskor a gyártók által megadott jelszót sem változtatják meg. Ilyen védelmen egy gyerek is könnyen túljut.

Vajon észrevettük már, hogy ha egy nő vagy egy férfi ugyanazt a keresőszót írja be a Google-ba, akkor néha ruhák és cipők, máskor versenyautók jönnek ki eredményül. A program ugyanis minden egyes lépésünket regisztrálja, és az így összegyűjtött információk alapján elkészíti a személyes érdeklődési körünknek megfelelő profilunkat, és a további kereséseink eredményeit ennek megfelelően állítja be, így ennek megfelelően szabadítja ránk az internetes reklámcégeket is. Az ingyenes e-mail-címekkel történt levélváltásokat is regisztrálja a rendszer, és ha én gyakran írok párizsi barátomnak, akkor nem kell csodálkoznom, ha elöntenek a franciaországi szállást és repülőjegyet hirdető reklámok. A Google eladja felhasználói profilunkat a hirdetők-

nek, de személyes adatainkat titokban tartja. A Facebook viszont mindent elad, a profilunkat, az érdeklődési körünket, a személyes adatainkkal együtt. A Yahoonak van az egyik legnagyobb adatbázisa az emberek internetezési szokásairól. Annak ellenére, hogy manapság már kevesen használják, mégis dollármilliárdokat ér az adatbázisa miatt.

„Legyünk óvatosak! Ne hagyjuk a pénztárcánkat az autó tetején, mert még a végén valaki elviszi…”

Annak elkerülésére, hogy egy hálózatba kötött, bejelentkezett számítógépen keresztül – amelyet a felhasználó magára hagyott – illetéktelen ne férhessen hozzá az adatokhoz, amelyeket megsemmisíthet, meghamisíthat, a BM OKF az informatikai eszközein inaktivitási időkorlátot vezetett be, amelynek letelte után a rendszer az eszközt lezárja, és az csak érvényes felhasználói név és jelszó birtokában oldható fel újbóli munkavégzés céljából.

Az Informatikai Biztonsági Szabályzat alapján az OKF informatikai rendszerében nem lehet használni olyan szoftvereket, amelyek nem jogtiszta forrásból származnak, illetve nem lettek előtte tesztelve. A nem megfelelő szoftverek telepítésének elkerülése céljából házirend alkalmazásával a számítógépet kezelő felhasználó csak „felhasználói” jogosultsággal rendelkezik a gép fölött, így meggátolható a nem biztonságos program bekerülése a rendszerbe. A telepítéshez rendszergazda együttműködése szükséges.

Fontos, hogy egy operációs rendszer biztonsági, illetve az egyéb telepített szoftverek frissítései mindig naprakész állapotban legyenek. A kritikus frissítések mindig azután kerülnek kiadásra, miután valamilyen biztonsági rés már ismertté vált, vagy már történt támadás a biztonsági rés használatával. Ezért a BM OKF központi telephelyén üzemeltetett, frissítések kezelésére használt szerver az alkalmazott szoftverek biztonsági javításainak terítését központilag valósítja meg, így el lehet kerülni a különböző verziókból adódó sérülékenységet.

A körlevelek mintájára úgynevezett lánclevelek, kéretlen levelek keringenek az interneten, amelyek soha nem egy bajba jutott ember megsegítésére, hanem a felhasználók postafiókjának megtöltésére, az informatikai rendszer blokkolására szolgálnak. Az ilyen típusú levelezés a „spam” kategóriájába tartozik. A spamek szűrésére a BM OKF hivatalos levelezőrendszere felkészült, a szűrő adatbázisának frissítése folyamatosan történik. Egy emelt szintű, úgynevezett rendszergazdai jogosultságokkal használt számítógép komoly sérülékenységet hordoz magában, éppen ezért a BM OKF esetében ilyen jogosultság csak az IT-területen dolgozó üzemeltetőknek adható azzal a megkötéssel, hogy alkalmazni kell a „legszűkebb jogosultság” elvét. Ennek értelmében csak és kizárólag az adott probléma megoldásáig, valamint csak arra a területre adható emelt szintű jogosultság az üzemeltető informatikus részére, amelyre az feltétlenül szükséges a feladatának ellátásához.

1.2.2. Informatikai biztonsági politika

Az IT-biztonsági politika, amelyet a biztonságért felelős személyeknek egyben iránymutatásként is kell kezelniük, amikor az információbiztonsággal kapcsolatos döntéseiket meghozzák, felső szinten definiálja a vezetői szintű elvárásokat az információbiztonság területén. A BM Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: BM OKF) informatikai biztonsági politikája egy iránymutatás, a hivatásos katasztrófavédelmi szervektől elvárt, az informatikai biztonsághoz való viszonyulás, amely az érvényesítés alapelveit fogalmazza meg egységes szemlélettel és a szervezet egészére vonatkozóan.[3] Az informatikai biztonsági politika célja a BM OKF informatikai rendszerei által kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésére állásának biztosítása, ezen belül különösen a következők:

- az irányelvek meghatározása az informatikai biztonsági feladatok összehangolt, tervszerű végrehajtásának biztosítása érdekében;
- az informatikai biztonsággal kapcsolatos felelősségi körök elkülönítése az informatikai rendszereket működtető BM OKF Informatikai Főosztály (a továbbiakban: IFO), az alárendelt szervek informatikai üzemeltetéssel kapcsolatos egységei esetében, valamint az együttműködés módjának rögzítése;

3 45/2014. számú BM OKF főigazgatói intézkedés a BM Országos Katasztrófavédelmi Főigazgatóság Informatikai Biztonság Politikájának, továbbá annak megvalósítását célzó Informatikai Biztonsági Szabályzatának kiadásáról.

- útmutatás az érintett vezetőknek az informatikai biztonságot érintő döntések meghozatalához;
- egységes információtechnológiai biztonsági követelmények meghatározása, ideértve a külső szereplőkkel szembeni elvárásokat is;
- az informatikai biztonsággal kapcsolatos jogszabályi kötelezettségeknek és ajánlásoknak való megfelelés minél teljesebb körű biztosítása;
- olyan, egységes elveken nyugvó, a nemzetközi és hazai szabványokhoz, ajánlásokhoz igazodó előírások betartatása, amelyek bizalmat teremtenek az informatikai rendszer biztonságát illetően.

1.2.3. Informatikai biztonsági szabályzat (IBSZ)

Az informatikai biztonsági szabályzat célja, hogy meghatározza az IT-biztonsággal kapcsolatos feladatokat és felelősségeket, megteremtse a számonkérhetőség alapjait. Az IT-biztonsági szabályzatban meghatározott biztonsági intézkedések részletes végrehajtási utasításait, eljárásait kapcsolódó dokumentumok, mint például üzemeltetési és felhasználói kézikönyvek tartalmazzák.

A BM OKF informatikai biztonsági szabályzat kiadásának célja, hogy a hivatásos katasztrófavédelmi szervek részére egységes és általános értelmezést adjon az informatikai rendszerekben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása érdekében követendő irányelvekre.[4] Az irányelvek figyelembevételével, a hatályos jogszabályok alapján meghatározható az informatikai rendszerek biztonsági osztályba sorolása. Kidolgozhatóak a konkrét, rendszerszintű informatikai biztonsági szabályozások, amelyek az adott rendszer teljes életciklusában meghatározzák a szabványos biztonsági funkciók tervezéséhez, megvalósításához, üzemeltetéséhez és megszüntetéséhez szükséges alapelveket és követelményeket.[5]

Legfontosabb jogszabályok:

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról;
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról;
- 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének tartalmáról;
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

A felhasználóknak és az informatikai dolgozóknak az e-learning-alapú távoktatást – az IBSZ kiadását – követően számonkérés formájában kell tanúbizonyságot tenniük a szükséges szakmai ismeretek eredményes elsajátításáról. A vizsga akkor tekinthető sikeresnek, ha a vizsgázó a kérdések 70 százalékára helyes választ adott.

1.3. Az informatikai biztonság megvalósulása

Az alapvető és szakmaspecifikus IT-biztonsági előírások megvalósítása a BM OKF esetében alárendelt, konkrét előírások, szabályzatok útján történik meg. Az informatikai biztonság szabályozási rendszerének egyik alapvető eszköze a biztonsággal kapcsolatos szerepkörök szétválasztása a felelős tevékenységek és az ellenőrzésükhöz szükséges jogosultságok összeférhetetlen alkalmazásának megakadályozása érdekében.[6]

4 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének tartalmáról.

5 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról.

6 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

1.3.1. Informatikai üzemeltetési szabályzat

Az informatikai üzemeltetési szabályzat (a továbbiakban: IÜSZ) megalkotásának célja a BM OKF és a hivatásos katasztrófavédelmi szervek informatikai rendszereinek – a kitűzött szolgáltatási szintnek megfelelő – biztonságos és áttekinthető működtetése. Az IÜSZ a szükséges üzemeltetői, felhasználói, vezetői teendők és felelősségi körök meghatározásával biztosítja:

- az informatikai rendszerek folyamatos és rendeltetésszerű működését,
- a szakmai feladatok ellátásához szükséges informatikai szolgáltatások rendelkezésre állását,
- a BM OKF gazdálkodási szabályzatában és informatikai biztonsági szabályzatában, valamint a BM OKF informatikai, informatikai biztonsági és távközlési szakstratégiájában rögzített elvek és előírások teljesülését,
- az információk és adatok hitelességét és jellegüktől függő bizalmas kezelését.

1.3.2. Vírusvédelmi szabályzat

A vírusvédelmi szabályzat (a továbbiakban: VSZ) célja, hogy egységes keretbe foglalja a BM OKF és a hivatásos katasztrófavédelmi szervek számítógépes vírusvédelmére vonatkozó előírásokat, figyelembe véve a BM OKF informatikai biztonsági szabályzatában meghatározott, vírusvédelemmel kapcsolatos felelősségi köröket és feladatokat.

1.3.3. Mentési és archiválási szabályzat

A mentési és archiválási szabályzat kialakításának célja, hogy a szabályzatban meghatározott adatokat tartalmazó alkalmazások mentését, a mentések visszaállítását és a mentések sikerességét megfelelő rendszertervek elkészítésével segítsük elő.

Mentési rendszerterv kialakítása

Minden, a szabályzat által meghatározott adatokat tartalmazó alkalmazásra ki kell alakítani egy önálló mentési eljárást a következő szempontok figyelembevételével:

- az informatikai rendszer sajátosságai:
  - a mentendő adatok mennyisége,
  - a mentendő adatok növekedési üteme,
  - a hálózat átlagos és maximális sebessége;
- mentési frekvencia (a mentések sűrűsége);
- mentendő munkakönyvtár vagy eszközkonfiguráció;
- a rendszeres mentéseket indító script(ek) vagy programok helye és neve, illetve ennek sikeres vagy sikertelen naplózási helye;
- a mentési eljárás tartalma:
  - mentőeszközök fajtája, típusa, mennyisége, elhelyezése,
  - a mentésért felelősök neve,
  - terv készítése a mentett adat visszaállítására, amely pontosan és részletesen tartalmazza az elvégzendő feladatokat, a hozzájuk kapcsolódó eszközök elérhetőségével együtt,
  - a mentett adat visszaállíthatóságának ellenőrzése.

1.4. A felhasználói jogosultságkezelés szabályai

A felhasználói jogosultságkezelés szabályainak célja, hogy meghatározzák a BM OKF informatikai biztonsági szabályzatában előírt jogosultságkezelési keretrendszer feladatait, elősegítve ezzel a hozzáférések és jogosultságok létrehozását, naplózását, folyamatos ellenőrzését és megszüntetését.

1.4.1. Informatikai objektumvédelmi szabályzat

A szabályzat tartalmazza a védett objektum elhelyezkedését, kapcsolattartóját, IBSZ szerinti biztonsági és védelmi besorolását, az objektum maximálisan megengedett kiesési idejét, az érintett hardvereszközöket, a védelem megvalósítását, az ellenőrzés menetét, a belépésre jogosultak listáját, a kulcsdoboz számát és helyét, valamint a katasztrófaelhárítási tervet.

1.4.2. Informatikai katasztrófaelhárítási terv

Az informatikai katasztrófaelhárítási terv alapvető célja, hogy megvédje a BM OKF-et azoktól a váratlan hatásoktól, amelyek a folyamatos működést és/vagy az informatikai rendszerek funkcionalitását veszélyeztetik. Ennek legfontosabb eleme a rendkívüli helyzetekre történő felkészülés. A tervezésnek az a célja, hogy minimalizálja a kockázatokat és az üzemelési stabilitást egy olyan szinten biztosítsa, amely a károkhoz mérten optimális költségekkel és gyorsan teszi lehetővé az eredeti állapot helyreállítását.

1.5. Hálózatüzemeltetés és rendszerfelügyelet

Kormányzati szándék nyomán a *Nemzeti Hálózatfejlesztési Projekt* (NHP) során, az államigazgatási intézmények esetében megkezdődött egy egységes infrastruktúrán alapuló informatikai rendszerre történő csatlakozás. A BM OKF 2011 végéig az *Elektronikus Kormányzati Gerinchálózat*hoz csatlakozott, majd az addig 22 végpontból álló országos hálózat (főigazgatóság, megyei katasztrófavédelmi igazgatóságok, Katasztrófavédelmi Oktatási Központ) lényeges bővítésen és átalakításon ment keresztül. Az NHP kapcsán létrejött *Nemzeti Távközlési Gerinchálózat* (NTG) használatával a katasztrófavédelem országos hálózata egy nagyobb (4-ről 50 Mbit/s-ra növelt) sávszélességű és nagyobb (22-ről több mint 200-ra emelt) végpontszámú informatikai rendszerré fejlődött. Az informatikai összeköttetéseket a szolgáltató (NISZ Zrt.) biztosítja az MVM gerinchálózatán.

A BM elvárásai alapján a végponti eszközöket nem a szolgáltatónak, hanem magának a szervezetnek kell felügyelnie. A kiépített hálózati infrastruktúra önmagában nem sokat ér, ha annak monitorozása nem történik meg, ezért egy egységes rendszerfelügyeleti alkalmazást vezetett be a katasztrófavédelem. A kialakított felügyeleti rendszer segítségével immáron nemcsak a hálózati csatlakozások, hanem az egyéb informatikai szolgáltatásokat nyújtó rendszerek (összesen több mint 700 host: hálózati eszközök, kiszolgálók, hangrögzítő berendezések, IP-s telefonközpontok) felügyeletét is ellátja az IT-ügyelet. A rendszer a nap 24 órájában, redundáns módon végzi a szolgáltatások működőképességének vizsgálatát, és a szakterület részére azonnali riasztást, valamint ütemezett módon kimutatást küld a statisztikákról. A feladata egyszerűen megfogalmazva az, hogy a beállított szolgáltatásokat ellenőrizze, eközben az adott szolgáltatás vizsgálni kívánt jellemzőjét számszerűsítse, és a kapott értéket a megadott szintekhez viszonyítva tisztázza a szolgáltatás aktuális állapotát.

Az alkalmazott rendszer azonnal értesíti az illetékes szakembereket a rendszerben keletkezett hibákról, így hamarabb megkezdhető a probléma elhárítása, csökkentve az esemény reagálási idejét, s ez nagyban hozzájárul a katasztrófavédelem informatikai rendszerének megbízható működéséhez.

1.6. Integrált eszközök és hálózatok

A BM OKF korábban is több más intézménnyel tartott fenn közvetlen adatkapcsolatot, és a szakmai igények nem csökkentek eddig. Jelenleg tíz intézménnyel tartunk fenn adatkapcsolatot a VPN-technológia felhasználásával (pl.: ESR-112, NKE, a régi ÁAK – új nevén Magyar Közút Nonprofit Zrt., MoLaRi, Vodafone, MÁV, a vízügy kapcsán a NEKI stb.).

A megnövekedett végpontszám és az újonnan kialakított adatkapcsolatok új irányba terelték az informatikai biztonság kérdését. A BM OKF szervezetébe integrálódott intézmények hatására megnőtt az informatikai biztonság kockázata. A korábbi tűzoltósági informatikai hálózatokat az újonnan kialakított országos informatikai hálózatba kellett kapcsolni. Emiatt bővült a hálózati biztonság alapkövének számító tűzfalszolgáltatás, a központi vírusvédelem, a hálózati adatkommunikáció védelme.

1.7. Végpontvédelem

Az alkalmazott informatikai biztonsági rendszerek önmagukban nem képesek megfelelő védelmet garantálni naprakész vírusvédelmi, illetve végpontvédelmi megoldás alkalmazása nélkül. Központi beszerzéssel a BM OKF-nél és alárendelt szerveinél bevezettek egy vírusvédelmi megoldást, amely védelmet nyújt a kártékony kódok ellen az asztali és hordozható gépek, illetve a kiszolgálók számára is. A központi szolgáltatásként üzemeltetett vírusvédelmi rendszer a szervezet tartományába tartozó összes számítógép részére biztosítja a naprakész állapothoz szükséges információk elérhetőségét.

1.8. Informatikai hálózatok

A BM OKF központi telephelyén kiépítettek és üzembe helyeztek egy, a teljes épületet lefedő vezeték nélküli informatikai hálózatot, amelynek segítségével a nyílt internet érhető el az épületben szolgálatot teljesítők és a külsős vendégek számára is. Bár az említett megoldás segítségével a belső, érzékeny hálózat nem érhető el, a megfelelő védelmi szint biztosítása érdekében erős titkosítást vezettek be. A BM OKF központjában virtuális hálózatok működnek, amelyek leszűkítik a hálózat használatát. Külön virtuális hálózatok állnak rendelkezésre a különböző felhasználási területek működéséhez.

2. A BM OKF szakrendszerei

2.1. Iparibaleset-megelőzési információs rendszer

A veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 2/2001. (I. 17.) Korm. rendelet értelmében a hatóság a veszélyes létesítményekről, a végrehajtott feladatairól, valamint a kapott információkról nyilvántartást vezet. A baleset-megelőzési információs rendszer kialakításának célja azon információk feldolgozása volt, amelyek a felügyeleti, kárelhárítási és kárfelszámolási feladatok végrehajtása során szükségesek.

Az információs rendszer adatbázistartalma:

- értékelések, elemzések: tartalmazzák a veszélyes anyagokra vonatkozó adatbázisokat (Hommel, Vakond, VESVE-katalógusok), valamint a gyors értékelés megvalósítását biztosító terjedési modelleket (ALOHA, AMAR);
- jogszabályok: elsősorban a felügyeleti feladatok ellátását segítik a területet érintő tűz- és környezetvédelmi nemzetközi szabályzók (pl.: Seveso II. irányelv, katasztrófatörvény és más hazai kapcsolódó jogszabályok);
- nemzetközi rendszerek: a Seveso II. irányelvből adódó adatszolgáltatási feladatok végrehajtása az EU illetékes bizottságának hatósága által kiadott szoftverekkel történik (SPIRS, MARS, DSDMS);
- térképi modellezés szoftverrel (pl. ArcView, ArcExplorer): ezzel tartják nyilván a veszélyes üzemekkel, illetve azok környezetével kapcsolatos információkat – feltöltése a biztonsági dokumentációk alapján történik (az EOV vetületben működtetett ArcView és a nemzetközi adatbázisok közötti kompatibilitást scriptek biztosítják);
- adatkezelés, kommunikáció: a kapcsolattartáshoz szükséges információk feltalálási helye (riasztás, név és címjegyzékek stb.), valamint a rendszerkarbantartási feladatok kezelésének megoldására szolgáló modul.

2.2. Safety program

A Seveso II. irányelv és a helsinki egyezmény 2002. január 7-én lépett hatályba Magyarországon. Az egyezményben foglaltak koordinálására a BM Országos Katasztrófavédelmi Főigazgatóságán az Ipari Baleset-megelőzési Nemzeti Központot jelölték ki. A részes felek kapcsolattartó pontjaikon keresztül biztosítják az információcserét, az értesítést és a segítségnyújtást.

A nemzetközi joganyagokban szereplő, felsorolt feladatok hazai végrehajtása csak egy jól kiépített ipari baleset-megelőzési és -elhárítási informatikai rendszer kialakításával lehetséges. A rendszernek tárolnia kell várhatóan közel 500 veszélyes üzem, raktár, telep biztonsági jelentéseinek összes adatát, kockázatelemzési eredményét, a veszélyességi övezet határait különféle mérgező anyagok, hőmérséklet, túlnyomás esetén, az egyéni és társadalmi kockázati rádiuszokat, a súlyos baleset esetére készített belső és külső védelmi terveket. Meg kell tudnia határozni – rövid idő (10 perc) alatt – a bekövetkező baleset káros következményeinek hatásait, a terjedési irányt és területet – határon túlra is – az aktuális meteorológiai értékek figyelembevételével. E kockázatszámítás végrehajtásához nyújt segítséget a Safety program.

2.3. A nukleáris baleset-elhárításhoz kapcsolódó rendszerek

A veszélyhelyzetek elhárításával kapcsolatos eddigi tapasztalatok szerint a megelőzés egységes rendszerének megteremtése az egész világon nagymértékben felértékelődött az elmúlt időszakban. A megelőzést, a védekezést és a következmények felszámolását a különféle döntéstámogató, országos és nemzetközi szintű folyamatos információ- és adatcsere, valamint a védekezési rendszerek összehangolásával lehet biztosítani.

A szennyezőanyagok légköri kibocsátása kapcsán, nukleáris események, veszélyhelyzetek esetében fontos szempont, hogy a légköri terjedésszámítási eredmények továbbfeldolgozhatóak és beépíthetők legyenek az ilyen esetekben rendkívül felelősségteljes döntések meghozatalát segítő alkalmazásokba, amelyek leginkább szolgálják a lakosság védelmét és az állampolgárok biztonságát. Ezt az elvárást nagymértékben kielégíti az Európai Unió által, az EU Phare program keretében a BM OKF-re telepített, jelenleg a magyarországi megvalósítás (honosítás) fázisában lévő RODOS, illetve a Nemzetközi Regionális Radiológiai Adatcsere Központ (prototípusrendszer, a továbbiakban röviden: PDX – Prototype Data eXchange system) rendszerek.

2.4. A Nemzetközi Regionális Radiológiai Adatcsere Központ rendszer

A PDX-rendszer lehetővé teszi a részt vevő országok radiológiai és meteorológiai monitoring-, környezeti fix laboratóriumi rendszerének, továbbá a területén működő atomerőművek adatainak elérését normál, illetve veszélyhelyzeti időszakban a Közép-Európai (magyarországi) és a Kelet-Európai (oroszországi) regionális PDX-központokon át. Az adatok elérése ISDN2-adatvonalon keresztül, nemzetközileg egységes EURDEP (EURropean Data Exchange Platform) formátumban történik. Az EURDEP-formátumú adatok kezelése, rendszerezése Oracle adatbázis-kezelő rendszer segítségével történik. Az adatokat az alkalmazói szoftver segítségével a felhasználó által kiválasztható különböző szempontok szerint lehet rendszerezni, megjeleníteni grafikus, táblázatos, diagramos, szöveges formában.

Ez az információ és adatcsere folyamatosan frissülő információkat, adatbázist biztosít a tagországok számára az európai térség országainak radiológiai, meteorológiai, levegő-, talaj- és vízszennyezettségének aktuális helyzetéről. A PDX adatait a RODOS rendszer közvetve fel tudja használni a több országon átnyúló nukleáris események hatásainak vizsgálatához, értékeléséhez. A RODOS rendszer (grafikus, táblázatos, diagramos és szöveges) eredményfájljai a PDX-rendszer segítségével könnyen, gyorsan eljuttathatók a nemzetközi regionális alközpontokon keresztül az egyes érintett tagországok nemzeti alközpontjaiba. A különböző helyzetekben kiválasztott adatok szükség esetén könnyedén beilleszthetők a rendszer által biztosított, nemzetközileg elfogadott szabvány szerinti EMERCON-formátumú táviratokba, és megküldhetők az érintett országok számára. A beérkező adatok megléte lehetővé teszi a mérési eredményekben jelentkező trendek figyelemmel kísérését, értékelését. A PDX-rendszer hazai és nemzetközi adatbázisokból épül fel, amelyek jelenleg a következők:

- Az AMAR-rendszer (Országos Automatikus Radiológiai Mérő és Adatgyűjtő Rendszer) mérési adatai a nukleáris szakterület alhálózatán keresztül.
- Az Országos Sugárbiológiai és Sugáregészségügyi Kutató Intézet (OSSKI) által szolgáltatott Országos Környezeti Sugárzásfigyelő és Ellenőrző Rendszer (OKSER) mérési adatai – amely tartalmazza az egészségügyi radiológiai mérő és adatgyűjtő hálózat (ERMAH), a hatósági környezeti sugárfigyelő és ellenőrző rendszer (HAKSER) és az FM-mérőhálózatok és laboratóriumok mérési adatait – ISDN2-adatvonalon.
- A KFKI AEKI környezeti radiológiai mérőrendszerének mérési adatai ISDN2-adatvonalon.
- Az OMSZ Paks és Budapest 100 km-es körzetében lévő meteorológiai távmérőállomásainak mérési adatai ISDN2-adatvonalon.

2.5. Az Országos Nukleárisbaleset-elhárítási Rendszer

Az Országos Nukleárisbaleset-elhárítási Rendszer üzemeltetése és a nukleáris veszélyhelyzet elleni védekezés tervezése, irányítása, valamint a végrehajtásának összehangolása kormányszintű feladat, amelyért a felelősség a belügyminisztériumot terheli. A megfelelő intézkedések meghozatalához kiépítettek egy kormányzati és önkormányzati döntéshozatali rendszert, amelyet kormányzati szinten a Kormányzati Koordinációs Bizottság

(KKB), a Nukleárisbaleset-elhárítási Védekezési Munkabizottság, területi szinten a megyei és helyi védelmi bizottságok, önkormányzatok és polgármesterek alkotnak. A kormányszintű feladatellátást, a nukleáris veszélyhelyzetre való felkészülés, a megelőzés és a végrehajtás koordinációját a Kormányzati Koordinációs Bizottság végzi (KKB).

A nukleáris rendellenességek, balesetek, veszélyhelyzetek a katasztrófák egyik típusát jelentik, így a katasztrófavédelmi feladatok közé tartoznak. A katasztrófavédelem megvalósításában fontos szerepe van a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóságának (BM OKF). A nukleáris tevékenységek közül a legjelentősebb veszélyforrást a hazai és a határon túli atomreaktorok üzemeltetése, továbbá a kiégett fűtőelemek, a hasadványtermékek, a radioaktív anyagok szállítása, a nukleáris és radioaktív hulladékok tárolása és a nukleáris űrobjektumok működtetése jelenti.

Nukleáris veszélyhelyzet esetén a döntéshozók részére a szakmailag megalapozott döntés-előkészítési tevékenységet a BM OKF Operatív Törzse végzi a Nukleárisbaleset-elhárítási Védekezési Munkabizottság működésének megkezdéséig. A szakmailag megalapozott döntések érdekében a szükséges adatokat és információkat a döntéshozók számára a BM OKF-en működő, a KKB Veszélyhelyzeti Központ részét képező Nukleáris Baleseti Információs és Értékelő Központ (NBIÉK), valamint a Nukleárisbaleset-elhárítási Védekezési Munkabizottság OAH CERTA-ban működő szakértői részlege szolgáltatja.

Az országos nukleárisbaleset-elhárítási rendszer a jogszabályok alapján kidolgozott különböző szintű feladatait az országos baleset-elhárítási tervek szerint végzi. Normál időszakban az országos sugárzási helyzet felmérését az ONER részét képező Országos Sugárfigyelő, Jelző és Ellenőrző Rendszer, az OSJER végzi, amelynek vezető eleme az NBIÉK. Az OSJER fontos részét képezi az országos radiológiai távmérő hálózat, amelynek mérési adataira épül az ország korai riasztási rendszere. Nukleáris veszélyhelyzetben az ONER szervezetei részlegesen vagy teljes egészében aktivizálódnak, a veszélyhelyzet felmérését az OSJER végzi, s ehhez az Országos Környezeti Sugárfigyelő és Ellenőrző Rendszer (OKSER) szolgáltat adatokat.

2.6. Az OSJER − országos radiológiai távmérő hálózat

Régóta tudjuk, hogy nap mint nap együtt élünk az ionizáló sugárzással. A természetes háttérsugárzás eredete kettős: egyrészt a Napból és a világűrből érkező kozmikus sugárzás, másrészt a környezetből érkező talajsugárzás okozza. Ennek köszönhető, hogy a háttérsugárzás térben és időben folyamatosan változik, jelentősen függ a talajszerkezettől, az időjárástól, a naptevékenységtől és egyéb kozmikus jelenségektől. A modern ember az ionizáló sugárzás használatával hozzájárult a természetes háttérsugárzás kismértékű megváltoztatásához. Ez a változás azonban esetenként – például a csernobili reaktorbaleset során, az atomerőmű környezetében – olyan jelentős lehet, hogy az emberek egészségét is befolyásolja. Ennek megakadályozása érdekében a háttérsugárzás változását folyamatosan nyomon kell követni.

A Magyar Köztársaság területén a háttérsugárzás mérését 1993 óta az Országos Sugárfigyelő, Jelző és Ellenőrző Rendszer részét képező országos radiológiai távmérő hálózat mérőállomásai végzik. A távmérő hálózat a honvédelmi, belügyi ágazati rendszerekből, az Országos Meteorológiai Szolgálat és a Paksi Atomerőmű Rt. összesen 77 db mérőállomásából áll jelenleg.

A rendszer a helyi meteorológiai adatok mellett a környezeti gamma-dózisteljesítmény értékeit méri. A gamma-dózisteljesítményt BIT típusú proporcionális szonda méri. A mérési adatokból tízperces dózisteljesítmény-átlagok állnak rendelkezésre, amelyek növekedési mértéke, illetve jelzési és riasztási határérték-túllépése fontos információt jelenthet a szakemberek számára. A háttérsugárzás mértéke (a dózisteljesítmény) a Magyar Köztársaság területén 60–180 nSv/óra között változik. Amennyiben a háttérsugárzás valamelyik mérőállomáson meghaladja a riasztási szintet – 500 nSv/óra –, az állomás riasztási jelet küld a központba, amelyet kivizsgálnak. Szükség szerint sugárvédelmi mobil mérőautó segítségével helyszíni izotópspecifikus méréseket is végeznek, továbbá levegő-, talaj- és vízmintát is elemeznek. Ezek alapján – illetve szükség esetén fix laboratóriumi mérésekkel – meg lehet határozni, hogy milyen izotópok felelősek a háttérsugárzás mértékének növekedéséért.

Az összegyűjtött adatok az Országos Sugárfigyelő, Jelző és Ellenőrző Rendszer központjaként is működő BM OKF Nukleáris Baleseti Információs és Értékelő Központba érkeznek be. Az adatokat a központ folyamatosan értékeli, ellenőrzi és eltárolja, illetve a többi ágazat felé továbbítja. A 24 órás ügyeleti rendben működő VK Ügyeleti Szolgálat a rendszer állapotát és a sugárzási adatokat egy, az adatbázishoz folyamatosan kapcso-

lódó grafikus megjelenítő felületen folyamatosan figyeli. A mérési adatokból napi, heti és havi rendszerességgel készülnek háttérsugárzási jelentések, amelyek mind a szakmai szervek, mind a lakosság felé nyilvánosak.

2.7. EURDEP projekt

A European Radiological Data Exchange Platform (EURDEP) az Európai Unió legtöbb országából valós idejű sugárzási adatok fogadására, illetve feldolgozására és megjelenítésére képes. A projekt a 2000/473/EURATOM szerződés elfogadása után kezdődött. Irányítója az olaszországi Isprában található EU Joint Research Centre (Központi Kutató Intézet). Az Európai Unió országai mellett számos nem EU-tag szolgáltat folyamatosan adatot a központnak. A megegyezés értelmében az elküldött adatok a többi adatküldő ország részére publikusok.

Az adatküldés normál időszakban napi rendszerességgel történik, de egy esetleges nukleáris baleset esetén az országok óránkénti adatküldésre váltanak át, ekkor válik ténylegesen online rendszerré. A mérési adatokat szabványformátumban (2002-ig az EURDEP 1.31, majd 2003-tól az EURDEP 2.0) továbbítják FTP- vagy e-mail-kapcsolaton keresztül, illetve a többi ország adatainak a letöltése is ezen az úton történik.

A projekt saját weboldalán a felhasználók interaktív térképen megjeleníthetik az aktuális sugárzási helyzetet, illetve adatbázis-formátumban lekérdezhetik az aktuális és historikus adatokat. A rendszer online működését éves gyakorisággal a JRC egy radiológiai adatküldési gyakorlat keretében ellenőrzi. Az EURDEP projekt keretében a BM OKF NBIÉK a radiológiai távmérő hálózat összes mérőállomásának az adatát átkonvertálja a megfelelő formátumba, és a kért rendszerességgel megküldi Isprába.

Szorosan összefügg az EURDEP projekttel az EASY-PROTEO projekt, amelynek kapcsolati pontját szintén az NBIÉK látja el. A projekt keretében éves gyakorisággal a Magyar Köztársaság területén mért összes hatósági és egyéb radiológiai adatot megküldenek a JRC-nek. A projektben az NBIÉK mellett adatszolgáltatóként részt vesz az Országos Környezeti Sugárellenőrző Rendszer központjaként működő OKK OSSKI. Az EURDEP-hez hasonlóan az adatküldő országok az összes többi ország adatához hozzáférnek. A projektben elsősorban az EU tagállamai vesznek részt.

2.8. Forrás – SQL integrált pénzügyi rendszer

A *Forrás* ügyviteli rendszermodulokból – alrendszerekből – álló, SQL-adatbázisra épülő integrált ügyviteli és bonyolítási rendszer. A rendszerben lévő modulok egymásra építkeznek, számuk tetszőlegesen bővíthető. Egy adott gazdálkodó szervezet adminisztrációja alapvetően két jól elkülöníthető részre osztható. Az egyik a felhasználó tevékenységeinek bonyolítása, amely alapvetően a cég/intézmény tevékenységi körétől, speciális feladataitól függ. Az adminisztráció másik része az ügyviteli elszámolások köre. Az elmúlt több mint húsz évben a Forrásnak nagyon sok sztenderd és speciális – tevékenységfüggő – modulja készült el, amelyekbe beépültek annak a több száz ügyfélnek az igényei, ötletei, tapasztalatai, akik a Forrást használják. A szoftver nyitottsága révén szinte tetszőleges struktúrájú más rendszerekkel integrálható. Felhasználói igény esetén lehetőség van akár a meglévő modulok funkcionális továbbfejlesztésére, akár új Forrás-modulok kifejlesztésére.

A Forrás további jellemzői:

- moduláris felépítés,
- ügyvitelileg zárt rendszer,
- egyszeres adatfeldolgozás,
- szabad paraméterezhetőség,
- széles funkcionalitás,
- többszintű jogosultsági rendszer,
- saját vezetői információs rendszer,
- több devizanem egyidejű kezelése,
- a felhasználó által definiálható, egyszerűen szerkeszthető lekérdezések, adatvisszanyerés,
- tetszőleges számú vállalati adatbázis kezelése,
- beépített eszköztár adatimportálásra, -exportálásra,
- saját bevezetési módszertan.

A Forrás ügyviteli rendszer illeszkedik a felhasználók munkaszervezési és információs igényeihez, olyan általános keretet biztosít, amelyet a felhasználó egyedi igény szerint tölthet ki konkrét tartalommal. A fejlesztőbázis, valamint a több mint két évtizedes értékesítési és ügyféltámogatási tapasztalat biztos hátteret, hosszú távú támogatottságot biztosít a rendszer felhasználói részére.

A Forrás az alábbi alrendszerekből áll:

- Pénzügyi-számviteli alrendszer:
  - pénzügyi modul,
  - főkönyvi modul,
  - kötelezettségvállalási modul,
  - k11,
  - külföldi kiküldetési modul,
  - határozatok pénzügyi bonyolítása modul,
  - határozatok pénzügyi analitikája modul.
- Készlet-eszköz alrendszer:
  - készletnyilvántartási modul,
  - készletkönyvelési modul
  - tárgyi eszköz modul,
  - érték nélküli készletek modul,
  - vonalkódos eszközleltár modul.

A BM OKF és területi szerveinek, háttérintézményeinek teljes pénzügyi nyilvántartását (főkönyvi, készlet- és tárgyieszköz-nyilvántartási modul) használja az OKF. A Forrás SQL-feladatait jelenleg a Magyar Államkincstárnál működő terminál szerverpark szolgálja ki. A hozzáférés a BM OKF és alárendelt szerveinek jogosult személyi állománya felé biztosított.

2.9. Zárt levelezőrendszer: katved.gov

A levelezőrendszer a BM OKF és területi szervei részére nyújt biztonságos, zártkörű szolgáltatást. A levelek és a naptár elérésére lehetőség van biztonságosan, az interneten keresztül is, valamint a belső hálózaton, önálló levelezőalkalmazással, valamint mobil eszközökkel is. Jelenleg közel 4000 postafiókot kezel a rendszer, minden felhasználó tárterülete szabályozott, ezért az archiválásnak kiemelt jelentősége van. A naptárak egymással megoszthatók, illetve ún. időpontfoglalással lehet támogatni a csoportmunkát. A központi szerveknél dolgozóknak egyéni, a funkcionális, területi szerveknél dolgozóknak funkcionális e-mail-címet állítanak be (piroska.toth@katved.gov.hu, illetve bacs.titkarsag@katved.gov.hu). Igény alapján felhasználói csoportok is címezhetők egy e-mail-címmel, de lehetőség van saját csoportok kialakítására is.

2.10. A BM OKF intranet portálja

Az intranet portál egy tartalmi és jogosultsági hierarchia szerint gyorsan elérhető, adatbázis-megjelenítést (szerkesztést) és a felhasználók hierarchikus azonosítását ellátó rendszer, szigorú hozzáférési adminisztrációval. Egységes felhasználói felület létrehozásával megoldja a különféle információforrásokból származó adattartalmak egy képernyőn való megjelenítését, a belső hírek előállítását és terjesztését, lehetőséget teremt a biztonságos távmunkára, ösztönzi a dolgozók közötti információcserét. Az OKF intranet portáljának előnye, hogy a szervezet belső hálózatának logikájára épít, s külső, idegen személyek részére egyáltalán nem vagy csak korlátozottan elérhető. Az intranet portál a könnyen és gyorsan kereshető információtárolást helyezi fókuszba. Tekintve, hogy a portálon nemcsak publikus információk jelennek meg, ezért kiemelten fontos feladata, hogy a tárolt adatokhoz csak jogosultsággal rendelkező személyek férjenek hozzá.

Az információs technológiák fokozatos elterjedtsége ma már lehetővé teszi, hogy a gyakorlatban is új, elektronikus oktatási formákat és módszereket vezessünk be. A lehetőségek egyike az e-learning, vagyis az internetes oktatás, az internetalapú oktatás. Ez az új, korszerű kommunikációs technológiát előtérbe helyező tanítási-tanulási folyamat, amely nagyobb részben internetes eszközökön keresztül, webes technikákkal zajlik, és átviteli közegként az internetet vagy az intranet hálózatokat használja.

2.11. Syrius helyett RobotZsaru

2010-ben megvalósult a 2009-ben indított EKOP-1.A.1 projekt, amelynek eredményeként bevezették az elektronikus ügyintézést a BM OKF-nél és alárendelt szerveinél. Az ügyek kezelése áttekinthető, monitorozható, az ügyintézői teljesítmény mérhető. Egyszerűsödött a vezetői munka, a vezetői terhelés csökkent, egyrészt az egyes operatív folyamatokban való részvétel módjának rugalmasabbá tételével, másrészt a vezetői beszámolókészítés támogatásával. Lehetővé vált a dokumentumok hatékonyabb kezelése, az ügykezelés támogatása, csökkent a papíralapú munkavégzés. A rendszerben megtalálható információk biztonságos, információbiztonsági szempontból kielégítő kezelése megoldódott.

Kormányzati döntés értelmében az államigazgatási intézmények részére bevezették a Kormányzati Érkeztető Rendszert (KÉR), amely nagyban segíti a papírmentes iroda mint cél elérését, mivel képes digitálisan aláírt dokumentumok küldésére és fogadására. A katasztrófavédelemnél 2015. január 1-től bevezették a korábbi Syrius helyett a RobotZsaru Neo ügyviteli rendszert, amely teljeskörűen támogatja a KÉR használatát.

2.12. Személyzeti Nyilvántartó Országos Rendszer (SZENYOR)

A rendvédelem területén népszerű szoftver már évek óta a SZENYOR for Windows rendszer, amely kifejezetten a közigazgatás számára fejlesztett humánerőforrás-gazdálkodási rendszer. A magyar közigazgatási szerveknél előforduló majdnem minden jogviszonyt lefed:

- kormánytisztviselő,
- köztisztviselő,
- közalkalmazott,
- hivatásos állomány,
- munkavállalók.

A rendszer az állomány személyzeti és munkaügyi adatait kezeli, okmányok kiállítására és egyéb dokumentumok, statisztikák előállítására is alkalmas. Számos helyen az ügyviteli folyamatokat is ezen keresztül bonyolítják. A rendszer természetesen követi a jogszabályi változásokat, és támogatja a közigazgatás által megkövetelt eltérő működési feltételeket. Ezt a rendszert használja jelenleg a Belügyminisztérium és az alárendelt szervezetek tekintélyes része, valamint a katasztrófavédelem szervei is.

Feladata az alkalmazottak személyzeti jellegű adatainak nyilvántartása, szervezési, tervezési feladatok végrehajtása. Ehhez a főigazgatóságon üzemeltetett terminálszerver áll rendelkezésre. A szerverhez való hozzáférés a BM OKF Személyzeti és Oktatási Főosztályának és alárendelt szerveinek személyi állománya felé biztosított. A tárolt adatokat adatbázisba szervezve tartják nyilván és elemzik.

2.13. Honlap, közösségi média

A katasztrófavédelem központi honlapja a http://katasztrofavedelem.hu oldalon érhető el. Elsősorban Internet Explorer böngészőre optimalizálták, de minden kereső alatt működik. A megyei honlapokat a központi oldal aloldalaiként hozták létre, a linkek pedig a megye nevével utalnak az oldalra (pl.: http://baranya.katasztrofavedelem.hu). Az oldalak felépítése hasonló, néhány tartalmi elem a központi oldalról szinkronizálódik. A hírek, az eseménytérkép és szezonban a viharjelző információk folyamatosan frissülnek. A honlap üzemeltetését külső cég végzi, külső szerverparkban, így a honlapot érintő bármely támadás esetén a BM OKF szakrendszerei biztonságban vannak.

1. kép: A BM OKF honlapjának képe (forrás: BM OKF)

A BM OKF a kommunikációs palettájának bővítéséhez a közösségi média lehetőségeit is kihasználja, és önálló Facebook-oldalt üzemeltet. Az oldalon megjelenő információkat, híreket a kommunikációs szolgálat frissíti.

2. kép: A BM OKF Facebook-oldalának képe (forrás: BM OKF)

2.14. Határidős Jelentések Tára

Az alkalmazás alapvető célja az időszakos HJT-jelentések központosított, elektronikus adatszolgáltatásának biztosítása. Segítségével az adatszolgáltatás és adatkarbantartás naprakésszé válik, és a kimutatások mindig az aktuális állapotot adják vissza. A modul segítségével határozzák meg, hogy melyik EDR-készülék melyik szerbe lett telepítve. A szer és az EDR kapcsolódása a szer rendszámának megadásával történik. Segítségével válik elérhetővé a döntéstámogatási térképen a szerek mozgása.

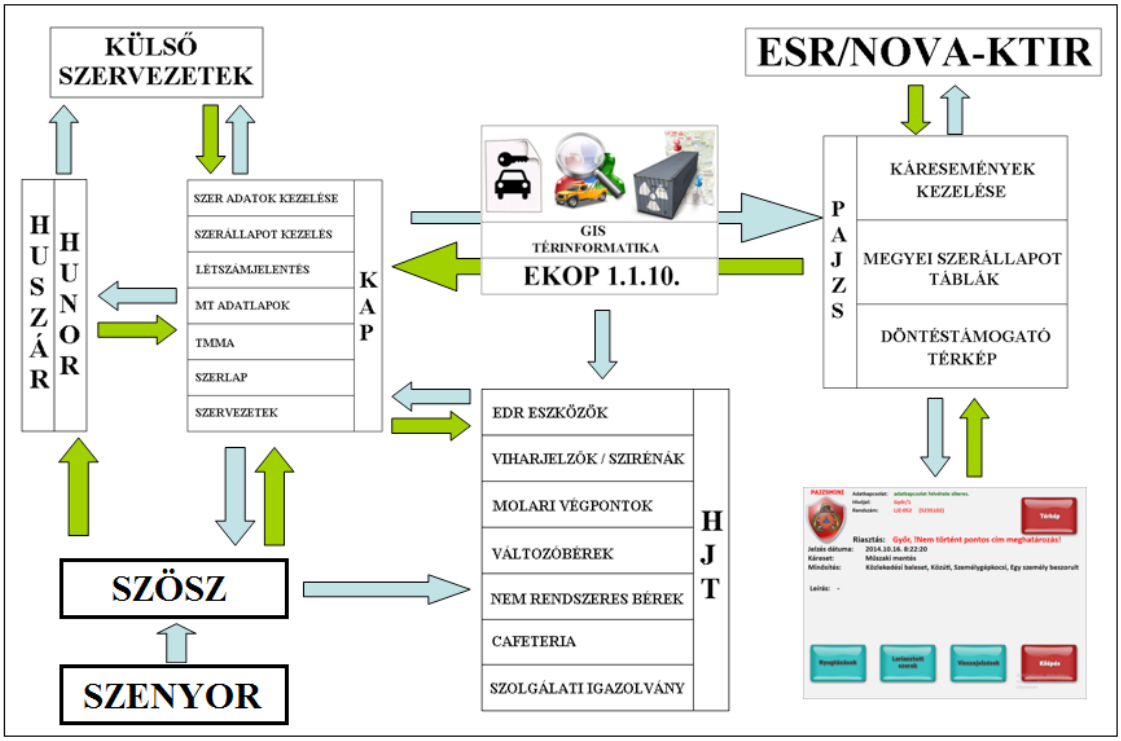
2.15. HUNOR/HUSZÁR riasztási rendszer

Az alkalmazás célja egy olyan rendszer biztosítása, amely lehetővé teszi a magyar nehéz (HUNOR), valamint közepes (HUSZÁR) kategóriájú városi kutató-mentő csapatok riasztását. A rendszer segítségével a riasztás pillanatában a területi szervek ügyeletei értesítést kapnak a riasztható személyek adatairól, elérhetőségeiről. Az alkalmazás következő lépcsője egy SMS-szerver üzembe helyezése, amelynek segítségével az érintettek értesítést kapnak szolgálati telefonjukra a riasztás szövegével és utasításaival.

3. A katasztrófavédelem informatikai fejlesztései

3.1. A katasztrófavédelem központi informatikai rendszereinek felépítése

A katasztrófavédelem működéséhez elengedhetetlen feltétel egy megfelelő informatikai és térinformatikai háttér, amely biztosítja a helyi, területi és országos szintű online adatokat, valamint folyamatosan segíti a megyei katasztrófavédelmi igazgatóság döntéstámogatási munkáját.[7]



1. ábra: A katasztrófavédelem központi informatikai rendszereinek felépítése (forrás: BM OKF)

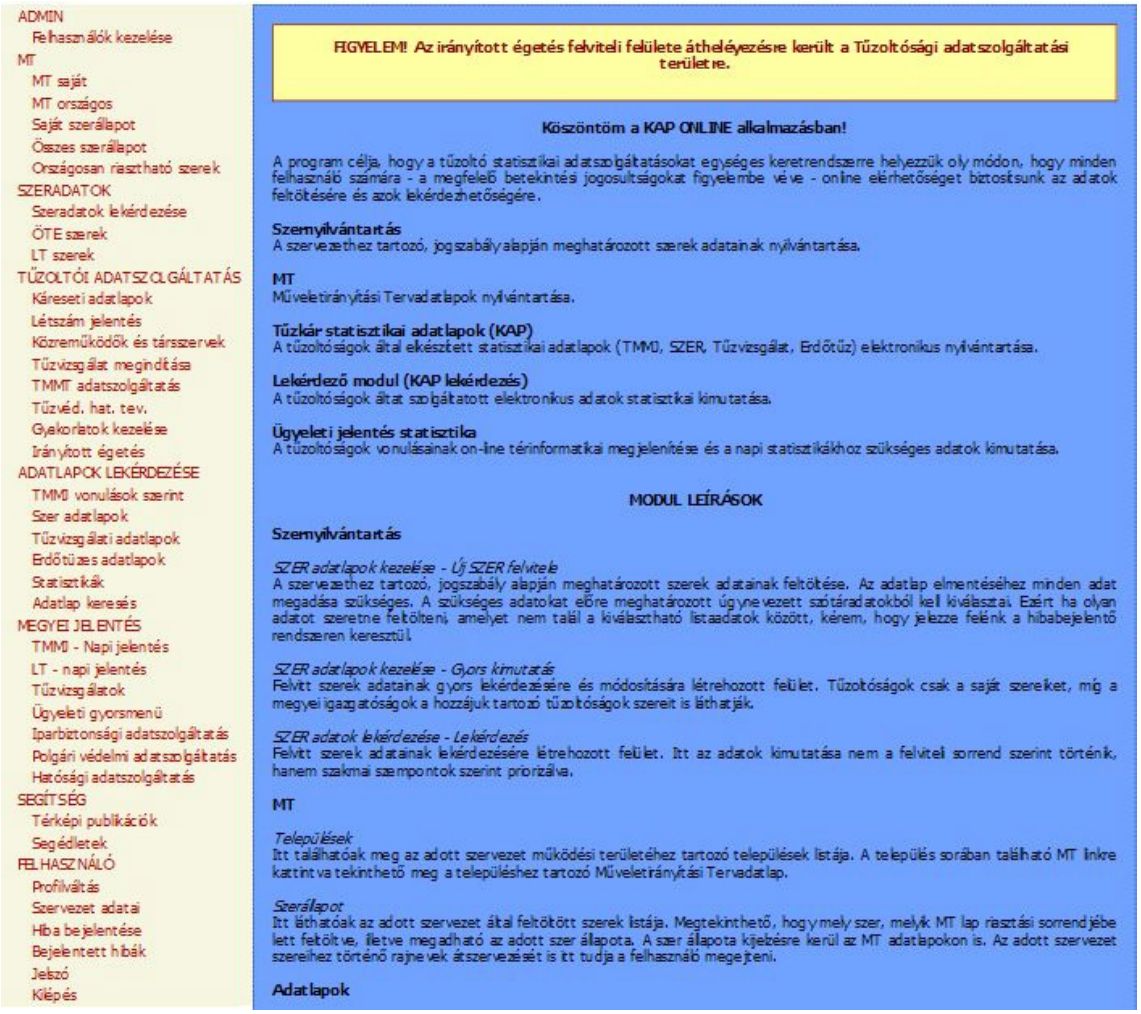
7 Endrődi István (2015): *Polgári védelmi szakismeret 1.* Egyetemi jegyzet, Budapest, NKE.

3.1.1. Katasztrófavédelmi Adatszolgáltatási Program (KAP-ONLINE)

A szakmai terület számára kialakított központi rendszer alapja egy statisztikai rendszer (online KAP), amelynek elsődleges feladata az országos, területi és helyi szervektől való adatbekérés és adatkinyerés. A rendszer célja, hogy az adatbevitel ott történjen, ahol az adat keletkezik, és – a hozzáférés függvényében – minden hierarchiaszinten ugyanazt az adatot kapjuk vissza.

Az alkalmazás legfőbb moduljai:

- *Szeradatok kezelése:* Az adott szervezethez tartozó, jogszabályban meghatározott szerek nyilvántartása. A nyilvántartás – a szer típusának megfelelően – a mindennapi munkához szükséges szakmai és műszaki adatokat tartalmazza.
- *Szerállapot-kezelés:* A modul segítségével a vizsgált szervezet szereinek státuszáról kaphatunk információt.
- *Létszámjelentés:* A létszámjelentés segítségével kimutathatóvá válik az egyes szerekre beosztott személyek száma. A hivatásos és önkormányzati tűzoltóságok minden létszámváltozás esetén, de minimum naponta egy alkalommal (szolgálatváltás után) elkészítik a jelentést, amelyet a megyei ügyelet ellenőriz és hagy jóvá.
- *MT-adatlapok:* A településekhez tartozó műveletirányító terv a tűzesetek eloltására, a műszaki mentést igénylő események felszámolására és a katasztrófák elleni védekezésre irányuló terv. Az MT-adatlapok adatait a hivatásos tűzoltóságok tartják karban a megyei igazgatóságok jóváhagyásával. Minden MT-adatlap tartalmazza a riasztási sorrendet, amely a településre tervezhető szerek számát adja meg az egyes riasztási fokozatok figyelembevételével. Az MT-adatlapok másik fontos része az MT-térkép, amely a tűzoltási és műszaki mentési szempontból fontos objektumokat (pl. tűzcsapokat, vízlelőhelyeket, víztározókat, tűzeseti és műszaki mentési tervvel, TMMT-vel rendelkező létesítményeket, tanyákat stb.) tartalmazza.
- *TMMJ és szerlap:* Minden tűzoltói vagy műszaki mentési beavatkozás után a tűzoltóság feladata, hogy szakmai szempontok alapján adatokat szolgáltasson az adott káreseménnyel kapcsolatban. Az adatszolgáltatás két legfontosabb része a káresemény statisztikai adatait tartalmazó tűzeseti és műszaki mentési jelentés (TMMJ), valamint a káreseményre riasztott szerek vonulási adatlapja (szerlap). Káresemény lezárásakor a rendszer automatikusan megindítja a TMMJ- és szerlapadatlapokat az online KAP felületén.



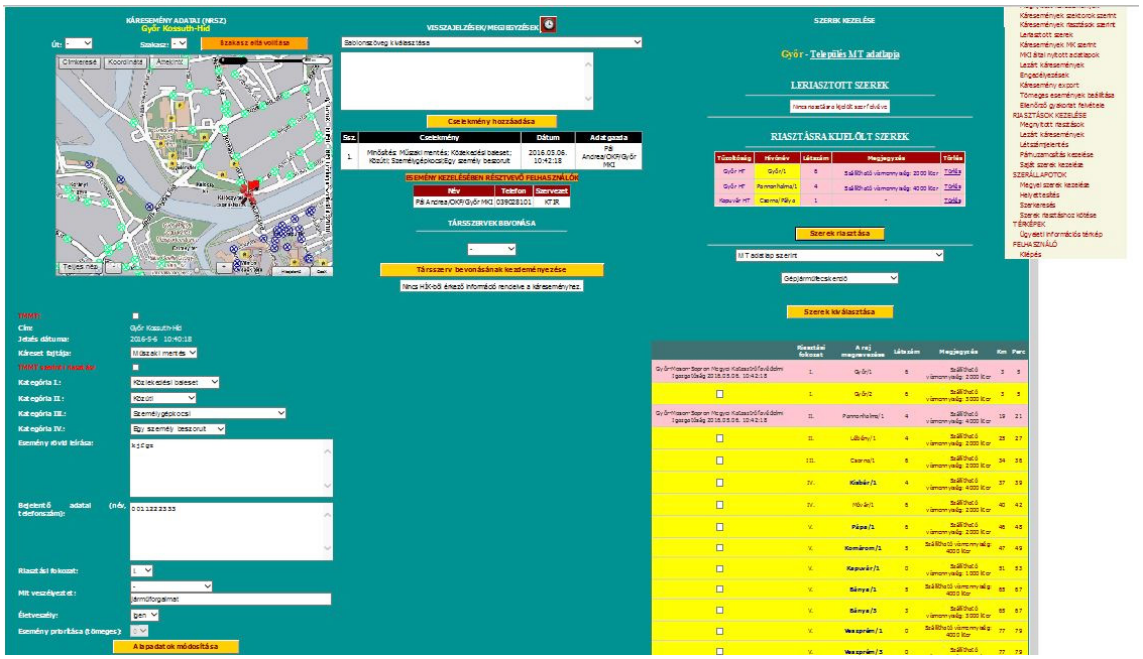
3. kép: Szerlap (forrás: BM OKF)

Térképek letöltése, szelvények megjelenítése

A tűzoltóságok számára a térképek letöltését jelen KAP modul biztosítja. A település *Keresés településre* listából történő kiválasztását követően a térkép ránagyít a településre, majd megjeleníti a nagyítás méretarányában az 1:10 000 EOV-szelvényhálózatot. A térképen a megfelelő helyre történő kattintással megnyitható az adott szelvény, amennyiben a számítógépen telepítve van Adobe Acrobat Reader program. A szelvény mentése is e programban történik a saját gépre.

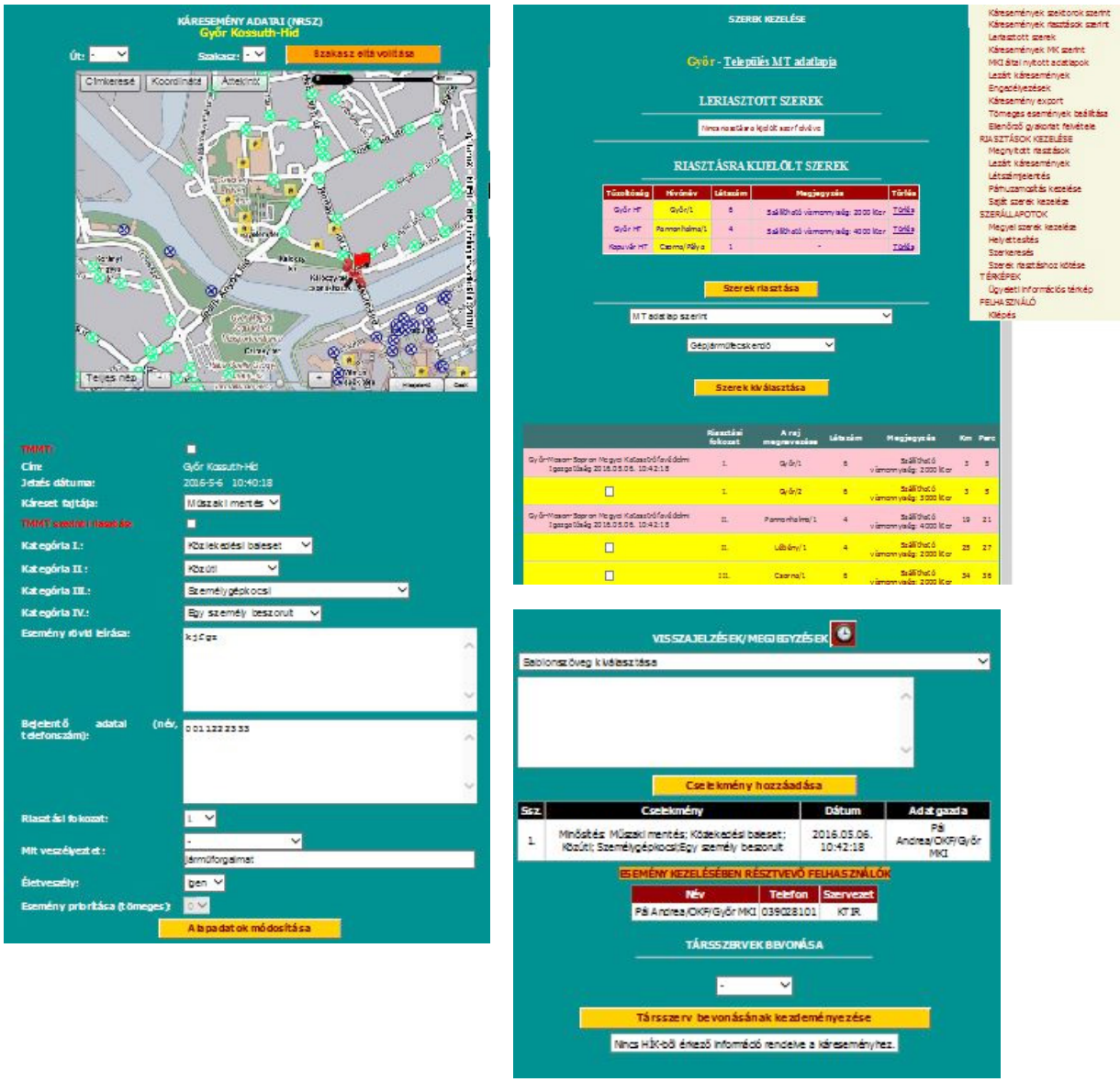
3.1.2. PAJZS

A katasztrófavédelmi szerveknél 2012 áprilisától fokozatosan bevezetett műveletirányítási rendszer személyi, elhelyezési feltételei mellett fontos elem az informatikai támogatás megteremtése. Az ügyeletek egyre több adattal és információval dolgoznak, amelyeknek a nap 24 órájában rendelkezésre kell állniuk ahhoz, hogy a szükséges erőket, eszközöket másodpercek alatt a helyszínre lehessen irányítani. E téren a BM OKF-en komoly fejlesztési háttérmunka folyt, amelynek eredményeként rendszerbe állt a PAJZS program.



4. kép: A PAJZS program munkalapja 1. (forrás: BM OKF)

A PAJZS, a térinformatikával támogatott központi informatikai rendszer rendelkezik azzal a káresemény-kezelési és riasztási modullal, amellyel a tűzoltógépjárműveket a káreseményekhez lehet rendelni, továbbá megyei szintű szerátcsoportosítási modullal, amely az erő- és eszközgazdálkodást szolgálja. Ezek mellett elkészült a térképes modul (DÖMI), amely megjeleníti az ország összes településének tűzoltási és műszaki mentési szempontból legfontosabb adatait – működési és illetékességi területek, megközelíthetőség stb. –, és automatikusan javaslatot tesz a riasztási sorrendre.



5. kép: A PAJZS program munkalapja 2. (forrás: BM OKF)

2014. december végén elindult a PAJZS éles működése a Fővárosi Katasztrófavédelmi Igazgatóság Műveletirányítási Ügyeletén. Így már az ország teljes területén a PAJZS rendszert alkalmazzák a bevetésirányításban. A főváros csatlakozásával nélkülözhetetlen feladatként jelentkezett a fővárosi tűzoltóságokon az automatika kiépítése.

Az automatika kiépítése

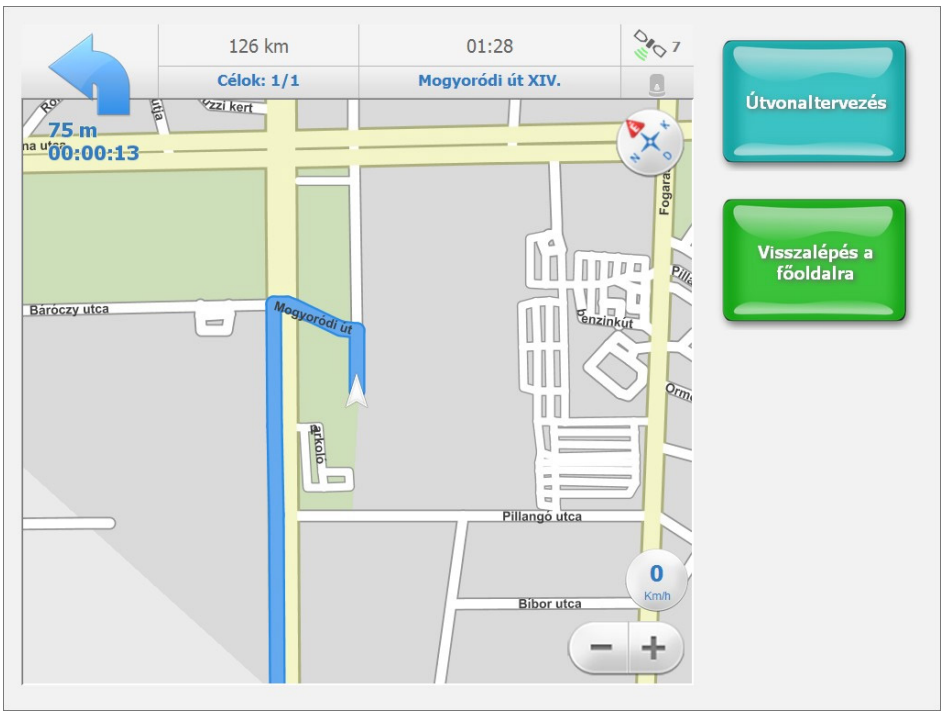
A riasztásfogadás automatikus folyamat. Ha egy állomáshely – parancsnokság vagy őrs – számára riasztási üzenet érkezik, akkor általánosságban a következő folyamatokat kell a lenti sorrendben elindítani:

- riasztási lap nyomtatása,
- figyelmeztető üzenet,
- riasztóvilágítás vezérlése,
- hangbemondás,
- közlekedési lámpa vezérlése,
- szertárkapu vezérlése.

3.1.3. PAJZS MINI

A PAJZS bevetésirányítást támogató rendszer mobil alkalmazása, a gépjármű fedélzeti egységén futtatható PAJZS MINI alkalmazás. Átadásával a műveletirányítók és a beavatkozó állomány olyan térinformatikával támogatott megoldást használhatnak, amely az adatok online szolgáltatásával lehetővé teszi az állomáshelyén kívül tartózkodó szer közvetlen riasztását, a szer indulásának nyugtázását, a kiérkezés, valamint a visszafordulás pontos idejének megadását, valamint a GPS-alapú navigáció segítségével a vonulás ideje is lényegesen lerövidül. Az alkalmazást 2015 júliusáig országosan minden vonulós gépjárműre teljeskörűen telepítették.

6. kép: A PAJZS MINI látványképe (forrás: BM OKF)



7. kép: A PAJZS MINI program munkalapja (forrás: BM OKF)

3.1.4. Szolgálatösszesítő szoftver

A 2013-ban bevezetett országos szintű szolgálat-összeállítási rendszer online módon képes kezelni mind a hivatali, mind a váltásos munkarendben dolgozó állomány beosztási rendjét és annak tervezését. Az alkalmazás a napi létszámról, a távollétekről, a túlszolgálatról és a pótlékjelentésekről szóló naprakész, pontos kimutatások, a gazdasági szakterület munkáját segíti, míg a szerekre, gépjárművekre beosztott létszámadatok a katasztrófavédelem riasztási és döntéstámogatási rendszerét szolgálja. Az alkalmazás bevezetésével kiváltották az elektronikus HJT-felületen a nem rendszeres kifizetésre vonatkozó adatszolgáltatást.

Az alkalmazás két fő pillére a személyügyi nyilvántartó rendszer (SZENYOR) és a Katasztrófavédelmi Adatszolgáltatási Program (KAP). Mivel a szolgálatszervezés kihat a katasztrófavédelem döntéstámogatási rendszereire (PAJZS, DÖMI), valamint pénzügyi adatokat biztosít a gazdasági terület felé (bérszámfejtés), szabályzóban szükséges rögzíteni a hiteles adatszolgáltatásra, az adatok karbantartására és visszaellenőrzésére vonatkozó szabályokat.

3.1.5. HADAR

A KAP részeként működő Hatósági Adatszolgáltatási Rendszer kezeli a katasztrófavédelmi hatósági feladatokhoz köthető ügyfelek, kötött létesítmények, szemlék, ellenőrzések, hatósági eljárások információit. A szoftver országosan valamennyi hatósági szakterület igényét kiszolgálja, az alkalmazásba épített térinformatikai modul segítségével a feltöltött objektumok (pl. tűzoltási és műszaki mentési tervvel rendelkező létesítmények) adatai információt biztosítanak a döntéstámogatási rendszer (PAJZS) számára.

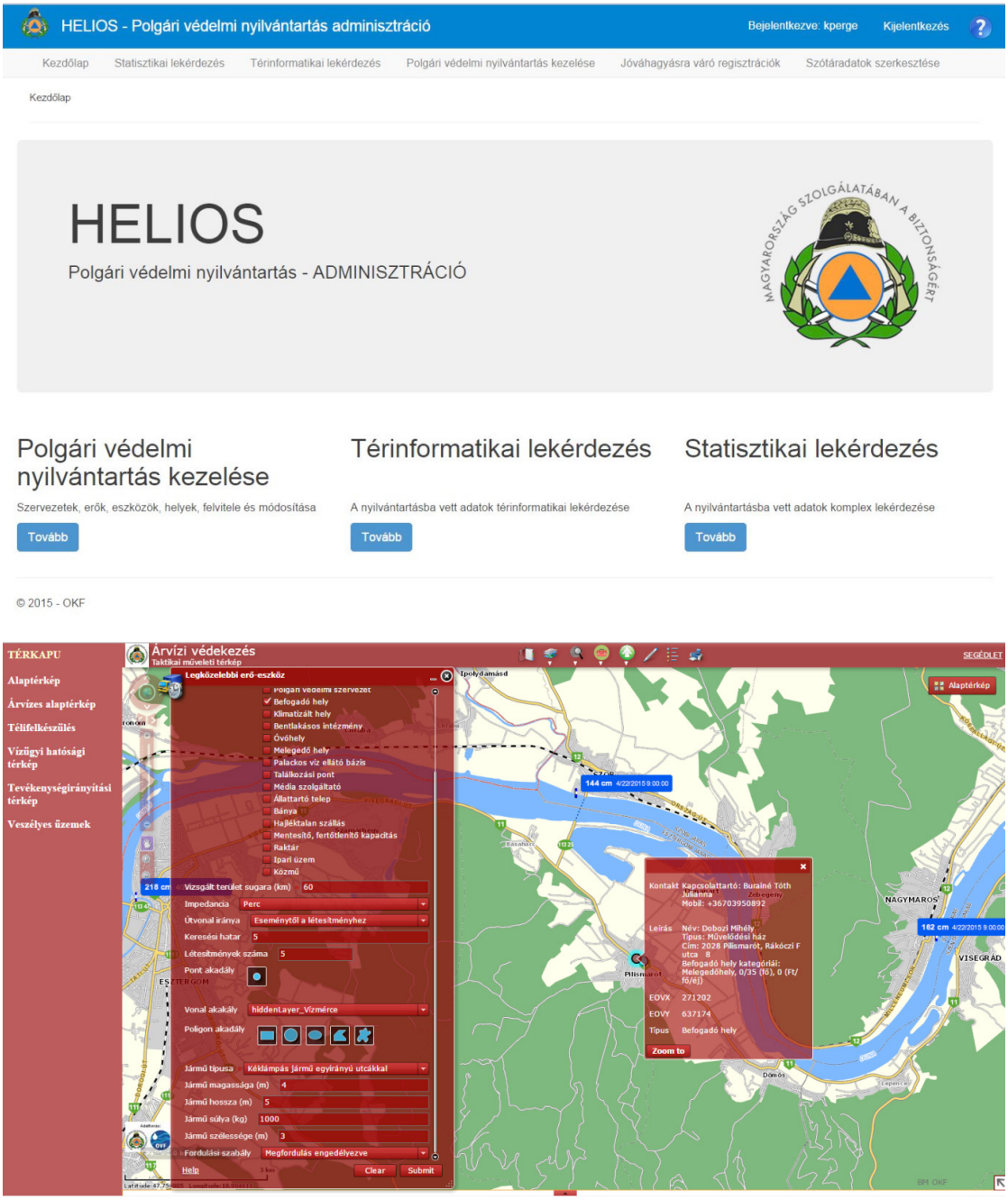
3.1.6. HELIOS

A HELIOS a polgári védelmi szakterület számára kialakított webes környezetben működő alkalmazás, a hivatásos katasztrófavédelmi szervezetnél bevezetett és központilag biztosított rendszer. A fejlesztés alapvető célja, hogy a katasztrófavédelem polgári védelmi szakterülete által megfogalmazott igényeknek megfelelően olyan térinformatikával támogatott alkalmazást biztosítson, amelynek segítségével nyilvános internetes felületen (regisztrációt és megfelelő hitelesítést követően) a katasztrófák elleni védekezésben részt vevő szervezetek riaszthatósági adatai feltölthetők, elérhetők, elemezhetők és térképen valós időben megjeleníthetők. A feltöltött információk (személyek, illetve elérhetőségeik, bevethető eszközeik stb.) alapján létrehozott nyilvántartás és a menedzselését biztosító alkalmazás a riasztandó erők pillanatnyi lehetőségeinek számbavételével és elemzésével, a riasztás technikai támogatásával a vezetői döntéshozatal hatékony támogatását biztosítja.

A rendszer a következő szervezetek és a hozzájuk köthető személyek, erők, eszközök adatait dolgozza fel:

- katasztrófavédelmi szervezetek;
- önkéntes tűzoltóságok;
- polgári védelmi szervezetek (munkahelyi, települési, területi, központi);
- önkéntes mentőszervezetek;
- segítséget nyújtó civil szervezetek;
- szakértők.

A nyilvántartás a felsorolt szervezetekkel és személyekkel kapcsolatos naprakész adatokat tartalmazza. Szem előtt kell tartani, hogy az információt ott töltsék fel, ahol keletkezik, és az adatok lekérdezhetősége ott jelenjen meg, ahol azokat a legnagyobb hatékonysággal lehet igénybe venni. Az adatok jogosultságszintű feltöltését és lekérdezését biztosítja a szoftver a katasztrófavédelem országos, területi és helyi szintű szervezeti egységeinél. A BM OKF Országos Polgári Védelmi Főfelügyelősége határozza meg az adatbázissal szemben elvárt részletes adattartalmat és a jogosultsági szinteket. Az adatfeltöltés az egyes érintett szervezetek feladata a webes felületen keresztül.



8. kép: A HELIOS munkalap képe (forrás: BM OKF)

3.1.7. Szolgálati gépjárművek nyilvántartása

A szolgálati gépjárművek kezelése alrendszer feladata a jelenleg hagyományos, papíralapú vagy táblázatos riportok elektronikus, egy komplex alkalmazáson belül történő kezelése, a hibabejelentések, az üzemképességre és málhafelszerelésre vagy a szer adott állapotára vonatkozó adatok dinamikus kezelhetősége, exportálhatósága, amelyet jogosultságtól függően használnak a katasztrófavédelem különböző szintjein. A katasztrófavédelem gépjárműparkjának és üzemállapotának nyilvántartása fontos információt nyújt a vonulások szempontjából, hogy az adott időpillanatban a gépjármű igénybe vehető-e vagy sem.

A szolgálati gépjárművek kezelése alrendszernek szükséges biztosítania a járműalapadatok (a forgalmi engedélyben szereplő adatok) nyilvántartását és az adatok rögzítéséhez, kezeléséhez szükséges funkciókat, továbbá a rendszerben nyilvántartható mindazon információkat, amelyek a járművek felhasználhatóságáról adnak tájékoztatást (képességre, felszereltségre, rendelkezésre állásra vonatkozó adatok stb.).

A felhasználóknak lehetőségük van az üzemeltetési napló digitális formában való feltölthetőségére, kezelésére, az adatok strukturált megjelenítésére, exportálhatóságára és nyomtathatóságára. Automatizált figyelmeztető és jelző megoldások követik az időszakos szervizek automatikus jelzését, ütemezését, elvégzésének idejét vagy a következő szerviz idejét. A rendszer támogatást ad a karbantartási adatok rögzítésére.

Az alrendszerben az arra jogosult felhasználóknak lehetőségük van:

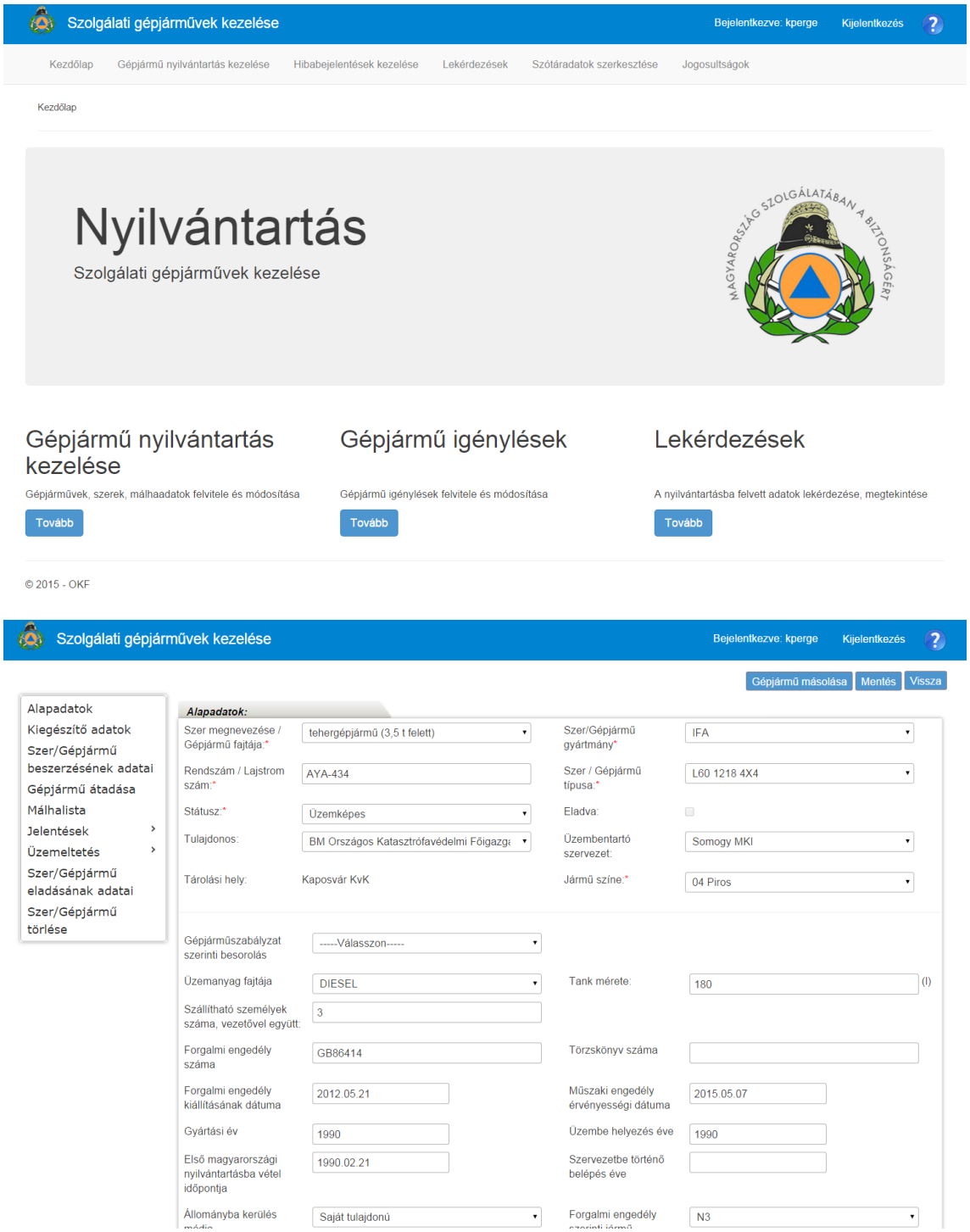
- a havi záró kilométeróra-állás rögzítésére;
- a menetlevéltömb számának rögzítésére göngyölítetten;
- a tankolások adminisztrálására (mennyiség, dátum, számlaszám vagy napi jegyzék száma);
- a MOL által küldött számlaadatok adminisztrálására (a tankolás időpontja, mennyisége, értéke stb.);
- az adott évre vonatkozó kilométerkeret rögzítésére;
- a kilométerhez kötött szervizciklus rögzítésére és követésére;
- a gépjárműtörzslap elektronikus változatának rögzítésére;
- a teljesítmény és költségráfordítási gyűjtőlap elektronikus változatának adminisztrálására;
- a felvitt anyagok alapján az üzemeltetési költség rögzítésére: térítési költség és kedvezményes térítés (amortizáció és javítás nélkül) költsége két fülön;
- az üzemképtelen járművek adatainak részletes nyilvántartására, adminisztrálására.

A baleseti nyilvántartást rögzítő és támogató modul segítségével nyilvántarthatók a gépjárművekhez kapcsolódó baleseti adatok:

- a járműre vonatkozó adatok;
- az üzemeltetőre vonatkozó adatok;
- a gépjárművezetőre vonatkozó adatok;
- a balesetre vonatkozó adatok.

Az alrendszer az arra jogosult felhasználóknak lehetőséget biztosít egyszerű és összetett riportok, lekérdezések készítésére (pl. járművenként, kategóriánként, szolgálati helyenként stb.), időintervallum megadásával az alábbiakra:

- kilométerfutás;
- üzemanyag-felhasználás;
- az üzemanyag értéke a NAV üzemanyag-árszámításával;
- a javítások, technikai kiszolgálások száma;
- javításra fordított költségek (ki javította, mennyibe került a javítás, anyag- és munkadíjköltség);
- átlagfogyasztás;
- a baleseti nyilvántartási riport elektronikus változata;
- a HEROS hibabejelentő riport elektronikus változata;
- a riportok nyomtatóbarát verziójának és exportjának elektronikus változata;
- a rendszerben keletkezett adatok dinamikus exportálása.

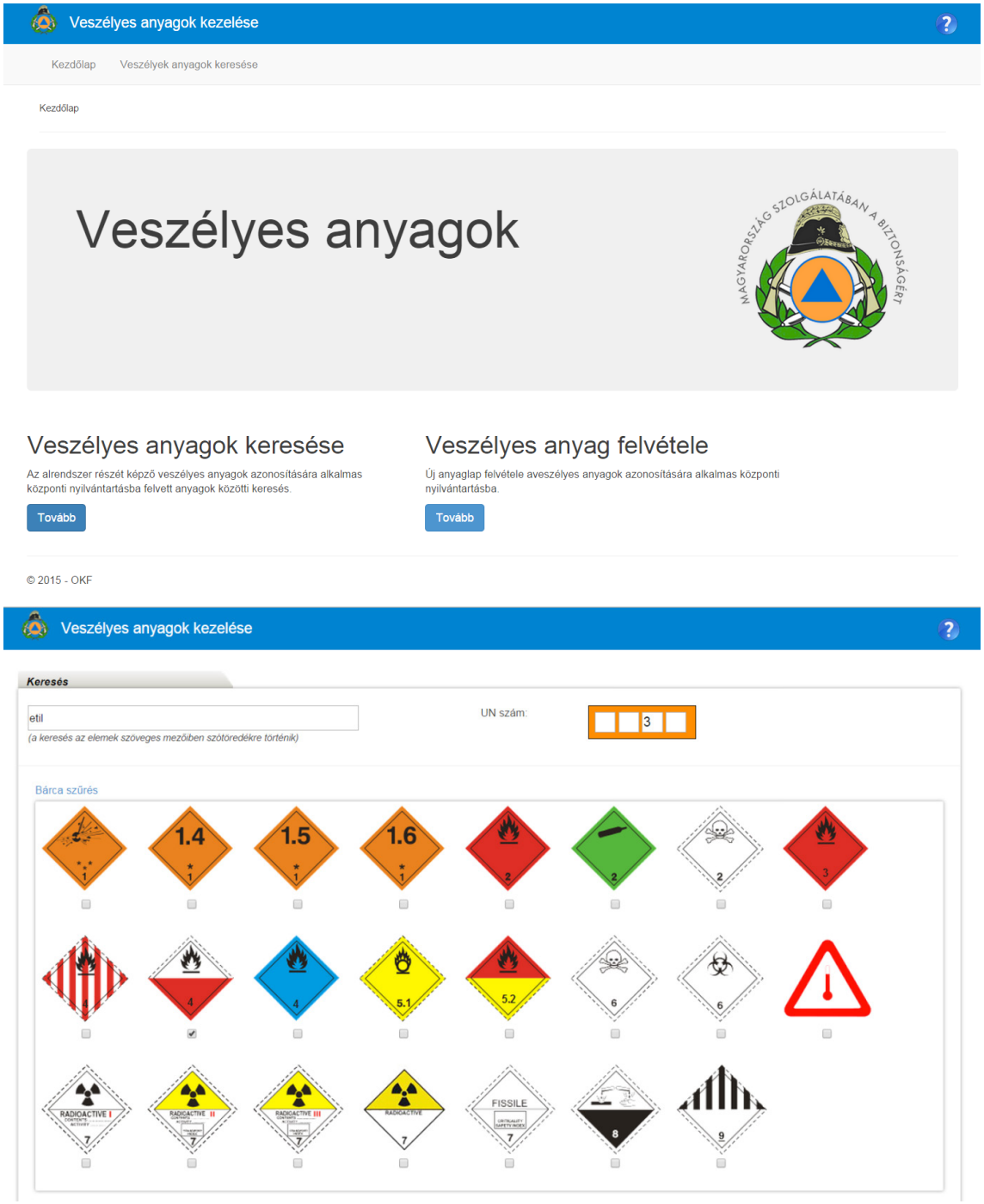


9. kép: Szolgálati gépjárművek nyilvántartási lapja (forrás: BM OKF)

3.1.8. A veszélyes áruk szállításának kezelése

A rendszer feladata, hogy az Országos Katasztrófavédelmi Főigazgatóság belső felhasználói köréhez tartozó felhasználók elérhessék a publikus felületeken regisztrált, veszélyes áruk vasúti szállításával összefüggő adatokat, továbbá olvasási és szerkesztési lehetőséget biztosítson a veszélyes anyagok központi nyilvántartásához. Ez két jogosultsági szint elkülönítésével valósul meg az alkalmazáson belül: admin (teljes hozzáférés, beleértve a regisztrációk kezelését, a szótáradatok szerkesztését stb.), illetve publikus. A veszélyes áruk vasúti szállításával kapcsolatos nyilvántartás mellett mobil és asztali környezetben egyaránt elérhető veszélyes-

anyag-kereső is a rendszer része, amellyel nemcsak anyagjellemezőkre, hanem piktogramokra is kereshetünk. A veszélyes anyagokkal összefüggő balesetek minél gyorsabb felszámolása érdekében az asztali környezetben terjedésmodellező is elérhető.



10. kép: A veszélyes anyagokat nyilvántartó program lapja (forrás: BM OKF)

3.1.9. VÉSZ

Okostelefonokra és táblagépekre készített országosan bárki által ingyenesen elérhető alkalmazást a BM OKF. A 21. század elvárásainak megfelelő veszélyhelyzeti tájékoztató rendszer a Rádiós Segélyhívó és Infokommunikációs Országos Egyesülettel és a Microsoft Magyarország Kft.-vel közös fejlesztés révén valósult meg. Az alkalmazás célja a lakosság azonnali, naprakész, célzott tájékoztatása. A rendszer segítségével az okostele-

fonnal rendelkezők azonnal tájékozódhatnak a lakóhelyük, az úti céljuk által érintett területek, figyelt útvonalak, megyék vagy akár az egész ország aktuális helyzetéről, a kiadott figyelmeztető és riasztási jelzésekről. Az információkat a katasztrófavédelem sajtóügyeletese teszi ki a rendszerre. Az ingyenesen letölthető alkalmazás az Android, iOS, Windows Phone 8 és Windows 8.x operációs rendszerek mellett Windows Phone 7-en is elérhető, teljesen díjmentesen.

11. kép: Lakossági tájékoztató eszközök (forrás: BM OKF)

3.1.10. TAVIHAR

A BM OKF szintén okostelefonokra és táblagépekre készített, országosan bárki által ingyenesen elérhető alkalmazása a TAVIHAR. Az alkalmazás célja a viharjelzők aktuális állapotának mutatása, illetve riasztási fokozat változása esetén értesítés küldése. Valamennyi jelentősebb tavunk (Balaton, Velencei-tó, Fertő tó, Tisza-tó) viharjelző állomásának állapota megtekinthető az alkalmazásban, és különféle szűréssel tetszőlegesen testre szabható. Az információk automatikusan kerülnek fel a rendszerbe a viharjelző rendszerből. Az ingyenesen letölthető alkalmazás az Android, iOS, Windows Phone 8 és Windows 8.x operációs rendszerek mellett Windows Phone 7-en is elérhető, teljesen díjmentesen.

3.1.11. Marathon Terra

MARATHON terra

A Marathon Terra a katasztrófavédelem felügyelete alatt működő, védelmi igazgatási célú infokommunikációs rendszer. A története egészen 2002-ig nyúlik vissza, amikor a Belügyminisztérium Helyzetelemző-értékelő Központjának létrejöttét követően felmerült az igény a hazai védelmi igazgatásban egy sokszereplős kommunikációs rendszer kifejlesztésére. A fejlesztés során kiemelt cél volt, hogy a BM és alárendelt intézményeinek regisztrált védelmi munkatársai között a meglévő levelezőrendszerektől független, megbízható, méret- és fájltípus-korlátozás nélküli informatikai összeköttetés jöjjön létre.

A teljes rendszer megalkotásával és a szoftver elkészítésével a Belügyminisztérium programozóját, Rácz Zoltán szoftverfejlesztő mérnököt bízták meg, aki 2003-ban elkészítette a Marathon rendszer első verzióját, amelynek körülbelül 50 felhasználója volt. Mivel a rendszer több gyakorlaton és „éles helyzetben" is bebizonyította használhatóságát, ezért a BM vezetői a rendszer továbbfejlesztése és bővítése mellett döntöttek.

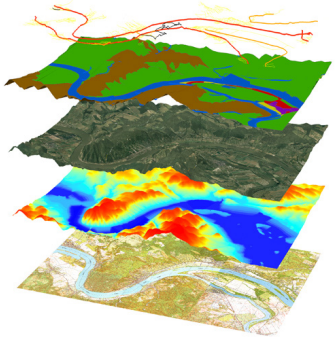
2007-ben elkészült a rendszer újabb verziója, a Marathon Terra. Ez az alkalmazás, amellett hogy megbízható adatkapcsolatot biztosít a felhasználói között, már rendelkezik „közösségi funkciókkal" is. Létre lehet hozni benne szakmai fórumokat, ahol a felhasználók különféle témakörökben oszthatják meg egymással a tapasztalataikat. A rendszer megbízhatóságát tükrözi, hogy ez lett Magyarországon a veszélyhelyzet-kezelés fő informatikai kommunikációs eszköze.

Jelenleg a Marathon Terra több mint 1200 felhasználóval rendelkezik. Felhasználói között megtalálhatóak a katasztrófavédelmi szervek mellett többek között a megyei és helyi védelmi bizottságok, büntetés-végrehajtási intézetek, az ÁNTSZ szervei, a Magyar Közút Nonprofit Zrt., a vízügyi szervek, a népegészségügyi szakigazgatási szervek, a kiemelt fontossággal bíró rádiók és televíziók, valamint egyre több, a védelmi igazgatás rendszerében tevékenykedő civil szervezet is bekapcsolódik a rendszerbe. A rendszer legnagyobb előnye az, hogy a komplex védelmi igazgatási rendszert képes kiszolgálni a kormányzati döntések előkészítéséért felelős központi szintű törzsektől (pl.: a Katasztrófavédelmi Koordinációs Tárcaközi Bizottság Nemzeti Veszélyhelyzet-kezelési Központja) a helyi végrehajtást koordináló műveletirányítási (pl.: katasztrófavédelmi kirendeltségek, járási védelmi bizottságok) szakterületekig.

A felhasználási köre rendkívül sokrétű, a BM OKF és az NMHH közötti megállapodás alapján a televíziók számára ezen a kommunikációs csatornán jutnak el az adatok a nézők felé, az OMSZ meteorológiai riasztásait e rendszeren továbbítják a védelmi igazgatásban részt vevő szervezeteknek, valamint a Marathon Terra az országos baleset-elhárítási intézkedési terv alapján a nukleárisbaleset-elhárításhoz kapcsolódó események kezelésének elsődleges kommunikációs eszköze is. A rendszer a védelmi szféra által megfogalmazott szakmai igényeknek megfelelően folyamatos fejlesztés alatt áll. A fejlesztések legfontosabb jövőbeli célja, hogy a rendszer minden informatikai platformon elérhető legyen, ennek megfelelően készül az Android-alapú, mobiltelefonokon futó kliensprogram, amelynek segítségével akár irodán kívül – okostelefonokon, táblagépeken – is elolvashatóak lehetnek az üzenetek.

3.2. Térinformatika

A térinformatika (angolul *geographical information system* vagy *geoinformatics,* röviden GIS) a térbeli adatok gyűjtésére, tárolására, adatbázisba szervezésére, elemzésére és térképi megjelenítésére szolgáló eljárások összefoglaló megnevezése. A földrajztudomány és a számítástechnika határterületeinek egymásba olvadásával kialakult módszertan lehetővé teszi a térben zajló folyamatok modellezését – így hatékony és korszerű eszközként használható szinte bármilyen környezeti, társadalmi, illetve gazdasági vonatkozású döntés során.



Térbeli adattípusok:

- Raszteres állományok (például műholdas távérzékeléssel előállított digitális űrfelvételek), alapegysége: pixel.
- Vektoros állományok (például terepi bejárás során GPS-készülékkel rögzített poligon), a térbeli objektumokat geometriai szempontból az alábbi három elemmel írhatjuk le: pont, vonal, poligon.

Leíró (attribútum-) adattípusok:

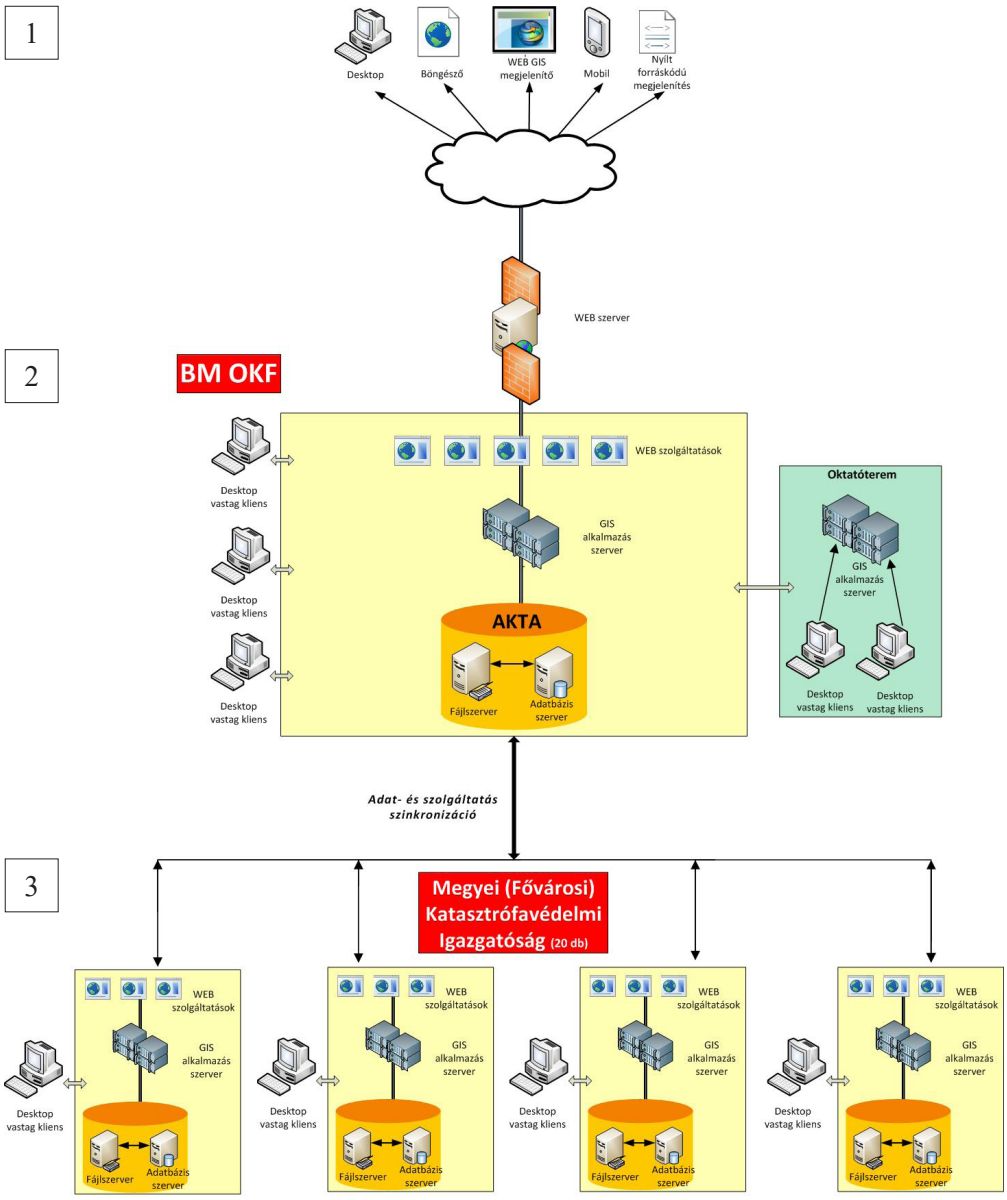
- Attribútum, szakadat (például a terepi bejárás során GPS-készülékkel rögzített poligon neve).
- Rétegek (fedvények): a digitális térképek rétegekből állnak, ezeket a fedvényeket úgy kell elképzelnünk, mintha egymásra tett átlátszó fóliák lennének, amelyeket ki-be kapcsolhatunk. Mindegyik fóliára az adott térkép egy-egy elemét rajzoljuk: tűzcsapok, vízrajz, domborzat, települések, úthálózat, veszélyes ipari létesítmények, űrfelvétel stb. Az ideális megjelenítési sorrend: poligon, majd vonal, végül pont, így nem takarják ki egymást.

A térinformatika működése szempontjából kritikus, hogy az adatainkat strukturáltan, logikai szempontból is összetartozó módon, adatbázisban tároljuk. A térképekkel, légi és műholdfelvételekkel együtt a tematikus adatgyűjtemények is fontos részei a térinformatikai rendszereknek. Ezen adatbázisok nélkül nem tudnánk különböző típusú elemzéseket végezni a térképeken, holott ez a térinformatika lényege.

A térinformatika legfontosabb végterméke a térkép, de lehetnek 3D-modellek, légi felvételek alapján készített ortofotók vagy az eredeti adatbázisok elemzéséből alkotott új adatbázisok is. Ezeket a végeredményeket vagy a képernyőn, vagy nyomtatott formában jeleníthetjük meg. A digitális megjelenítés egyre elterjedtebb formája a térinformatikai webes alkalmazás, azaz az interneten keresztül elérhető interaktív térképek.

3.2.1. Térinformatika a katasztrófavédelemnél

A katasztrófavédelemnél a térinformatika egy olyan szolgáltatást nyújt speciális tematikus megjelenítés és elemzések segítségével, amely elsősorban a döntések előkészítését, a tervezést és a beavatkozó erők munkáját támogatja. Ennek része a tűzoltó-parancsnokságok diszlokációs tervezése, az informatikai (adatszolgáltatási) rendszerek térképi moduljainak térképi támogatása, a célirányos elemzések elvégzése katasztrófa- vagy veszélyhelyzet esetén.



2. ábra: Az országos térinformatikai rendszer felépítése (forrás: BM OKF)

A térinformatikai rendszer felépítése

1. Végfelhasználói szint (vékony kliens):
   - szakterületek, a katasztrófavédelem állománya,
   - irodai számítógépek (webböngésző),
   - GIS-szolgáltatások.
2. Központi szint (BM OKF):
   - három térinformatikai rendszeradminisztrátor, egy fejlesztő,
   - két szerver – négy desktop,
   - GIS-adatbázisok, GIS-szolgáltatások.
3. Megyei (fővárosi) szint:
   - egy térinformatikai rendszeradminisztrátor,
   - egy szerver – egy desktop,
   - GIS-adatbázis, GIS-szolgáltatások.

3.2.2. Térinformatikai Katasztrófavédelmi Publikációk (TÉRKAPU)

A TÉRKAPU segítségével a katasztrófavédelem térinformatikai adatvagyonának a térinformatikában nem járatos, átlagos számítástechnikai ismeretekkel rendelkezőkkel való megosztása is biztosított. Az alábbi képességek egy webes böngészőből, egyszerű, gyorsan megtanulható felhasználói felületen, gyors adateléréssel érhetők el, irodai számítógépen, professzionális szoftver használata nélkül:

- előre definiált, használatra kész tematikus térképek közül való választás, a rendelkezésre álló térképi rétegekből saját térképi tartalom összeállítása, igény esetén nyomtatása,
- földrajzi adatok közötti keresés és a rendelkezésre álló térképi információk alapján egy adott terület jellemzőiről gyors, pontos áttekintés,
- új térképi, rajzos és szöveges elemek felvitele a térképre, azok megtekintése és a szerkesztésre megnyitott adatok valós idejű kezelése,
- előre meghatározott térképi elemzések, leválogatások grafikus és szöveges eredményeinek kezelése,
- változatos adatlekérdezések végrehajtása (pontokhoz rendelt szöveges adatok, koordináták, két pont közti távolságmérés, területmérés, hatászóna-definiálás, úthálózati alapú tervezés stb.),
- adatoknak a címadatok geokódolásával történő megjelenítése és térbeli összefüggések láttatása,
- térinformatikai szolgáltatások (pl. webes szerkesztés, hálózatelemzés, az útvonal és a szolgáltatási terület meghatározása), valamint előre definiált modellezési, statisztikai és egyéb térbeli elemzési eszközök használata.

A szakembereknek olyan professzionális alkalmazást biztosítunk, amelyben több mint száz eszköz áll rendelkezésre térbeli elemzések végrehajtására, megoldott az adatok dinamikus kezelése, és lehetőség van a térinformatikai feladatok (folyamatok) modellezésre, automatizálására. A fejlett szerkesztőeszközök egyszerűbbé teszik az adatbevitelt, megjelenítést és karbantartást.

A térinformatikai rendszer teljes eszköztárat kínál ahhoz, hogy a felhasználó adatait hatékonyan menedzselje, más IT-rendszerekkel integrálja, összetett elemzéseket végezzen, modellezzen, az eredményeket pedig professzionális térképeken jelenítse meg. A kialakított adatbázis-struktúra lehetővé teszi a közvetlen kommunikációt a BM OKF más, térinformatikával támogatott rendszereivel (pl. online KAP, DÖMI stb.), így lehetőség van a valós idejű adatok megjelenítésére is.

A térképi adatok és szolgáltatások biztonságos (webes) megosztásával széles körben lehet szervezeten belülre és kívülre publikálni. A rendszer informatikai háttere lehetővé teszi a nagyszámú felhasználó általi egyidejű használatot, illetve a védett adathozzáférést is. A szakterületi alkalmazások között megjelenik a téli felkészülést, árvízi védekezést támogató funkció, de a térinformatika az éles helyzetek mellett gyakorlatok és eseményidőszakon kívüli megelőzési feladatok támogatására is működtet alkalmazásokat. Ez utóbbi kategóriába tartoznak a diszlokációs elemzések, hatósági feladatok támogatása.

4. A katasztrófavédelem távközlési rendszerei

4.1. Bevezetés

A BM OKF Informatikai Főosztálya a megyei katasztrófavédelmi igazgatóságok (a továbbiakban: MKI) informatikai osztályaival, a katasztrófavédelem szakmai területeivel, valamint több civil szervezettel szorosan együttműködve működteti a lakosság biztonságérzetét növelő távközlési rendszereit. Az üzemeltetett távközlési rendszerek egy részét még a hivatásos katasztrófavédelmi szerv 2000-ben történt megalakulását megelőzően, más részüket az elmúlt másfél évtized során alakították ki.

Jelen jegyzet a teljesség igénye nélkül, rövid történeti áttekintéssel ismerteti az alábbi rendszereket:

- A Katasztrófavédelmi Távbeszélő Rendszer a katasztrófavédelmi szervek számára biztosít egy önálló, zárt célú távbeszélő hálózatot, GSM.
- A hivatásos katasztrófavédelmi szervek jelenleg használatos rádiótávközlő rendszere a TETRA technológián alapuló EDR.
- A BM OKF IFO napjainkban négy jól elkülöníthető lakossági riasztó- és riasztó-tájékoztató rendszert üzemeltet:
  - mechanikus és elektronikus szirénák,
  - a Pakson és 30 km-es körzetében telepített Lakossági Tájékoztató és Riasztórendszer (a továbbiakban: LTRR),
  - viharjelző rendszerek,
  - Monitoring és Lakossági Riasztórendszer (MoLaRi).
- Mobil vezetési pontok.

4.2. Katasztrófavédelmi Távbeszélő Rendszer

4.2.1. Vezetékes távközlés

2000 előtt a katasztrófavédelem elődszervezetei (Tűzoltóság Országos Parancsnoksága, Polgári Védelem Országos Parancsnoksága) részére a BM zárt célú távközlő hálózatát üzemeltető szervezetek biztosítottak távbeszélő végpontokat, főként bérelt vonali, valamint BM-tulajdonú, analóg vezetékes kapcsolatokon alapuló hálózaton. A BM OKF, valamint az MKI-k 2000-ben történő megalakításakor a főigazgatóság központi telephelyén üzembe helyeztek egy Siemens HiCom 300-as telefonközpontot, amely a rendelkezésre álló mellékekkel kiszolgálta a főigazgatóság személyi állományát. A megyei igazgatóságok különféle telefonközpontjai (Panasonic, Alcatel, Siemens, Bosch) a megyei rendőr-főkapitányságok telefonközpontjairól kaptak hat számjegyű (körzetszám + hívószám) mellékeket.

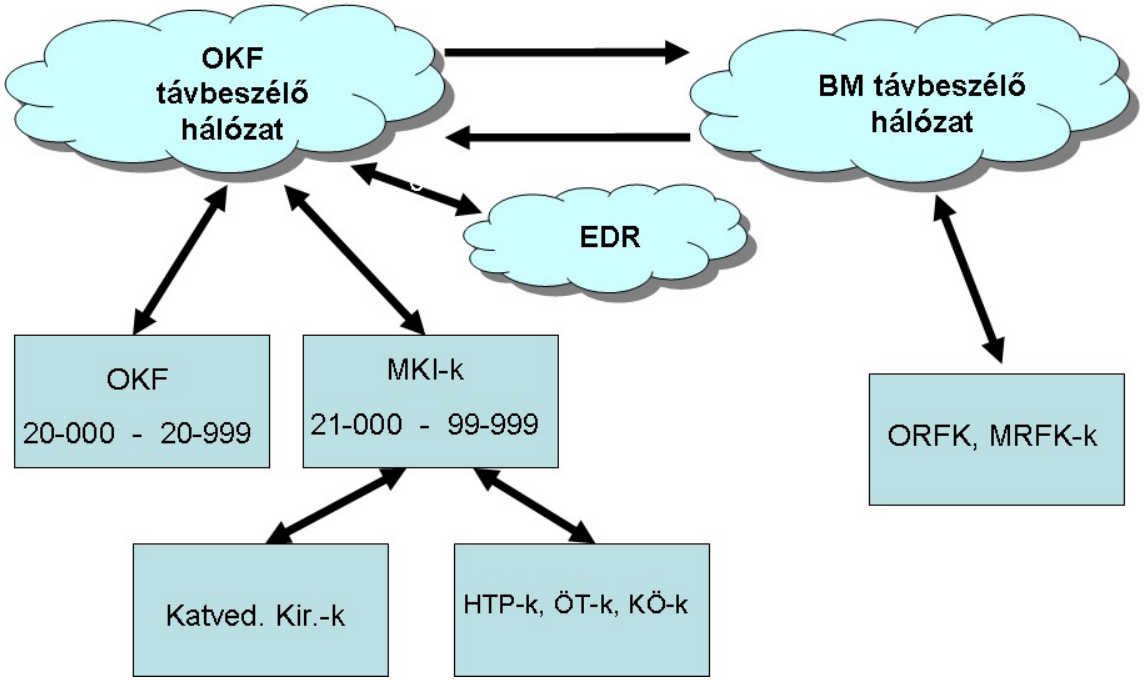
A katasztrófavédelem 2007-ben csatlakozott az Egységes Kormányzati Gerinchálózathoz. A gerinchálózat – mint átviteli út –, valamint az akkor beszerzett HiPath 4000-es telefonközpont már képes volt a megyei telephelyek részére is biztosítani az akkor már meglévő 2000 hívószámot tartalmazó tartományból országosan több igazgatóságon, kirendeltségen távbeszélő végpontokat. Ez a két darab, 1000 hívószámból álló számmező még a BM zárt célú távközlő hálózatának szerves részét képezte, ugyanis a BM és az Országos Rendőr-főkapitányság főközpontjai biztosították a hívások pontos irányítását. A csatlakozási projekt részeként korszerű Siemens

3550-es alközpontokat szereztek be az igazgatósági telephelyekre. A fejlesztés eredményeként a hivatásos katasztrófavédelmi szervek már körzetszám tárcsázása nélkül tudtak egymással telefonon beszélni. A hálózaton belüli hívások díjmentesek, a hálózaton kívüli hívások díjkötelesek. Belső szabályozó rendelkezik az egyes felhasználók által felhasználható keretekről, az elszámolás egy tarifaszámláló rendszer segítségével történik.

2012-től, az új katasztrófavédelmi törvény elfogadását követően az addigi önkormányzati tűzoltóságok állami kezelésbe, a megyei katasztrófavédelmi igazgatóságok irányítása alá kerültek. A telephelyek jelentős mértékben megnövekedett száma (kb. 200 db) és a több mint 10 000 főre duzzadt létszám megkövetelte egy új távközlési rendszer kialakítását.[8] A BM OKF Informatikai Főosztálya 2011-ben megkezdte a hálózat bővítésének tervezését, az együttműködő partnerekkel történő egyeztetéseket.

A sikeres tervezést és a minden irányba kiterjedő egyeztetéseket követően 2011 végén megkezdődött az egységes Katasztrófavédelmi Távközlési Rendszer kialakítása. A BM zárt célú távközlési hálózatát üzemeltető Nemzeti Infokommunikációs Szolgáltató Zrt.-vel (a továbbiakban: NISZ) folytatott tárgyalások eredményeként a megyei rendőrségi telefonalközpontok átprogramozásával egyidejűleg a BM OKF egy önálló, saját, ötjegyű számmezőből álló zárt célú távközlő hálózatot hozott létre.

A folyamat eredményeként a BM OKF kezelésében lévő főközpont, valamint a Nemzeti Távközlési Gerinchálózat (a továbbiakban: NTG) elemeiként működő telefonalközpontok látják el a kapcsolattartást a főigazgatóság, a megyei igazgatóságok és a külső publikus hálózat irányába. A BM OKF-en és a Fővárosi Katasztrófavédelmi Igazgatóság (a továbbiakban: FKI) budapesti telephelyén Siemens Hipath 4000, a megyei igazgatóságokon (Pest megye kivételével) Siemens Hipath 3800, a hozzájuk tartozó katasztrófavédelmi kirendeltségeken pedig Hipath 3550 telefonalközpontok üzemelnek. Az így kialakított rendszer egy főközponttal, több mint ötven alközponttal közel 10 000 távbeszélő végpont működtetésére képes.



3. ábra: A katasztrófavédelem távbeszélő hálózata (forrás: BM OKF)

A megyékben lévő más kirendeltségeken, illetve tűzoltó-parancsnokságokon országosan mintegy 1100 db IP-telefonkészüléket helyeztek el, amelyek az NTG-re kapcsolódva, az egységes katasztrófavédelmi távközlő hálózat végső elemeiként működnek, a megyei igazgatóságok Hipath 3800-as telefonalközpontjainak belső mellékeiként.

A rekonstrukció során egy, az új szervezeti struktúrához igazodó, a többi hálózattól független, öt számjegyű, megyénként ezer mellékből álló, tipizált, ún. katasztrófavédelmi távbeszélő rendszert alakítottak ki. Ez a gyakorlatban annyit jelent, hogy a szervezetekhez, azokon belül pedig a beosztásokhoz kapcsolódó szám-

8 66/2014. BM OKF főigazgatói intézkedés a hivatásos katasztrófavédelmi szervek informatikai szakterületének Gazdálkodási Szabályzatáról szóló 6/2013. számú BM OKF főigazgatói intézkedés módosításáról.

kiosztás történt meg. A hívószám első két számjegye a megyét azonosítja, az utolsó három pedig a szervezeti egységet és a felhasználó beosztását. Előnye, hogy minden azonos beosztású személy azonos végződésű hívószámmal elérhető. Az új szervezeti struktúrához igazodva megkülönböztethetők egymástól az igazgatósági, kirendeltségi és parancsnoksági szintek. A katasztrófavédelem hálózatából történő kitelefonálás és behívás előhívókkal (prefixekkel) valósul meg.

A 2011. évi CXXVIII. törvény (a továbbiakban: Katved. tv.) hatálybalépése előtt a beérkező 105-ös lakossági segélyhívásokat a hivatásos önkormányzati tűzoltóságok (a továbbiakban: HÖT) ügyeleti szolgálata fogadta, sok esetben hangrögzítés nélkül. Ez a szisztéma megfelelt az 1990 előtti rendszernek. Ekkor még csak egy, majd később egyre több távközlési szolgáltató lett Magyarországon. Az önkormányzati tűzoltóságok saját hatáskörben egyeztettek a szolgáltatóval az érintett településekről érkező segélyhívások irányításával kapcsolatban.

A távközlési piac megváltozása miatt azonban az ország területén egyre több, napjainkra mintegy száz szolgáltató biztosítja az ügyfelei részére a segélyhívások lehetőségét. A korábbiakban, a működési terület esetleges megváltozásánál vagy egy alközponti hibánál minden tűzoltóság saját hatáskörben intézte a segélyhívások átirányítását a szolgáltató felé. Tovább bonyolította a helyzetet, hogy a HÖT-ök számos különböző gyártótól származó alközponttal rendelkeztek, sok esetben karbantartási szerződés nélkül. 2012-től a BM OKF Informatikai Főosztályának irányításával, a Nemzeti Média és Hírközlési Hatóság (a továbbiakban: NMHH) szoros együttműködésével, a távközlési szolgáltatók felé történő hatósági feladatszabással megreformálták a 105-ös segélyhívószám fogadását.

Az NMHH elrendelte a szolgáltatók felé, hogy megyénként egy-egy előre meghatározott formátumban adják át a 105-ös segélyhívásokat a Magyar Telekom részére. A BM OKF felkérte a Magyar Telekom cégcsoportot, hogy a közel száz távközlési szolgáltató által működtetett lakossági és vállalati előfizetésekről kezdeményezett 105-ös segélyhívásokat a katasztrófavédelem által megadott alközpontok felé irányítsa. A folyamat eredményeként megvalósult a 105-ös segélyhívások centralizálása. Jelenleg az ország lakossága, amennyiben a 105-öt tárcsázza, biztosan a legközelebbi irányító hatáskörrel rendelkező katasztrófavédelmi szerv felé tesz bejelentést. A távközlési rendszer átalakításával egyidejűleg a megyei igazgatóságokon kialakították a műveletirányítási központokat. A segélyhívások fogadása a megyei telefonalközpontokba bekötött ISDN2-vonalakon valósul meg, amelyekből négy-négy darab található igazgatóságonként. A mellékek rendszerkészülékei lehetővé teszik a segélyhívást bejelentő személy, a társszervek vagy a helyi közműszolgáltatók gyors elérését, valamint a műveletirányítási központban lévő személyek egymás közötti hívásátadását is.

Nagyobb időjárási anomáliák, természeti vagy ipari katasztrófák esetén akár több száz százalékkal megnőhet az egyidejű lakossági bejelentések száma, ugyanakkor a hívásokat fogadó műveletirányítók száma korlátozott. Annak érdekében, hogy a bejövő hívások mielőbb a felelős döntést meghozó katasztrófavédelmi dolgozóhoz kerülhessenek, a kialakított távbeszélő rendszer finomhangolására volt szükség. A központok programozását végző beszállítóval és a műveletirányítást végző szervezeti egységekkel egyeztetve, az alközpontok meglévő tudását kihasználva újabb országos átprogramozás történt. A folyamat során azokat a segélyhívásokat, amelyeket a megyei központokban már nem tudnak fogadni, automatikusan a megyében lévő nagyobb tűzoltó-parancsnokságokra irányítják. Ezzel a bejelentő, a rendelkezésre álló személyi és technikai kapacitásokat maximálisan kihasználva, a lehető legrövidebb időn belül „élő hanghoz" jut.

A műveletirányítási központba befutó segélyhívások rögzítése érdekében megyénként beszereztek egy-egy darab digitális hangrögzítő berendezést. A hangrögzítők által felvett hanganyagot az OKF-en, központilag archiválják, így egy esetleges vizsgálat kapcsán biztosítja a hanganyagok hosszú idejű visszakereshetőségét.

Az Egységes Segélyhívó Rendszer (ESR – 112) korszerűsítésével Magyarországon is az európai színvonalnak megfelelő, korszerű rendszer kezdte meg működését. A nemzeti (104, 105, 107) és az európai (112) segélyhívó számokra érkező lakossági hívásokat a rendszer teljes üzembe helyezését követően két, egyenként több mint százfős operátori munkahellyel rendelkező, úgynevezett hívásfogadó központban (HIK) veszik fel. A HIK operátora a segélyhívó kikérdezésével egy időben számítógépes felületen kitölt egy adatlapot, amelyet a beavatkozó mentő-, rendőr- vagy katasztrófavédelmi műveletirányításhoz továbbítanak. A segítséget nyújtó szervezet az adatlapon lévő információk alapján riasztja a megfelelő erőket, eszközöket.

A 105-ös segélyhívásokat 2016 első negyedévének végétől a teljes országot érintően a HIK-ek fogadják. A katasztrófavédelem műveletirányító ügyeletei átköltöztek a rendőrségi telephelyeken kialakított húsz darab tevékenység-irányítási központba (TIK). A TIK-ekben egy légtérben foglalnak helyet a rendőr és a tűzoltó ügyeletesek, így könnyebbé vált az együttműködés, és nőtt a költséghatékonyság.

4.2.2. GSM

A katasztrófavédelem vezeték nélküli távközlése (GSM) mindenkor igazodik a Belügyminisztérium mint szakirányító szerv által meghatározott keretszerződéshez. Ennek keretében határozzák meg azt a távközlési szolgáltatót, amelynek szolgáltatásait a katasztrófavédelem igénybe veszi. Ezt a keretszerződést általában kétévente vizsgálják felül, és ez magában hordozza az esetleges szolgáltatóváltást. Ez, bár rengeteg adminisztrációval jár, nem okoz problémát a felhasználóknak, mert ún. számhordozás történik, tehát mindenkinek megmarad az évek óta ismert, eredeti hívószáma. Jelenleg a magyar államigazgatás a Vodafone szolgáltatásait használja. A hivatali előfizetések igényjogosultság szerinti kategóriákba soroltak, és ennek keretében történik az elszámolás, kerettúllépés esetén az esetleges túlhasználat kiszámlázása. A keretfelhasználás ellenőrzése negyedévenként történik.

4.3. A katasztrófavédelem és az EDR

A 2000-es évek közepén kormányzati igényként jelent meg, hogy a rendvédelmi szervek egy egységes technológián alapuló, a szoros együttműködést lehetővé tevő, új rádiórendszert alkalmazzanak. A magyar állam 2005-ben közbeszerzési pályázatot indított a készenléti szervek kommunikációját biztosító digitális rádiórendszer kiépítésére és üzemeltetésére. A TETRA *(Terrestrial Trunked Radio)* nemzetközi szabványon alapuló rádiórendszert 2007. január végén adták át. A felépült Egységes Digitális Rádiótávközlő Rendszer (a továbbiakban: EDR) a GSM-rendszerhez hasonlóan szintén a második generációs európai mobilszabványcsalád része. A rendszer négy kapcsolóközponttal, 381 diszpécser-munkaállomással (a továbbiakban: DWS), napjainkra közel 300 bázisállomással 42 ezer rádióterminál kiszolgálására képes.

Az egyes felhasználói szervezetek az EDR-rendszer használatában egy közös infrastruktúrán osztoznak, azonban minden szervezet képes a saját hálózati struktúráját szabadon, a többiektől függetlenül kialakítani és használni. Látszólag úgy viselkedik, mintha saját magánhálózata lenne, és nem egy mindenki által használt közös hálózaton kommunikálna. Ezt a tulajdonságot nevezzük virtuális magánhálózatnak, azaz VPN-nek. Minden egyes VPN a szervezeti struktúrának és alkalmazásnak megfelelően, hierarchikusan épül fel. Jelenleg az EDR-ben 14 – azonos jogokkal bíró – VPN-t alakítottak ki (pl.: rendészeti, katasztrófavédelmi, mentős stb.).

A digitális kommunikáció előnyei az analóggal szemben:

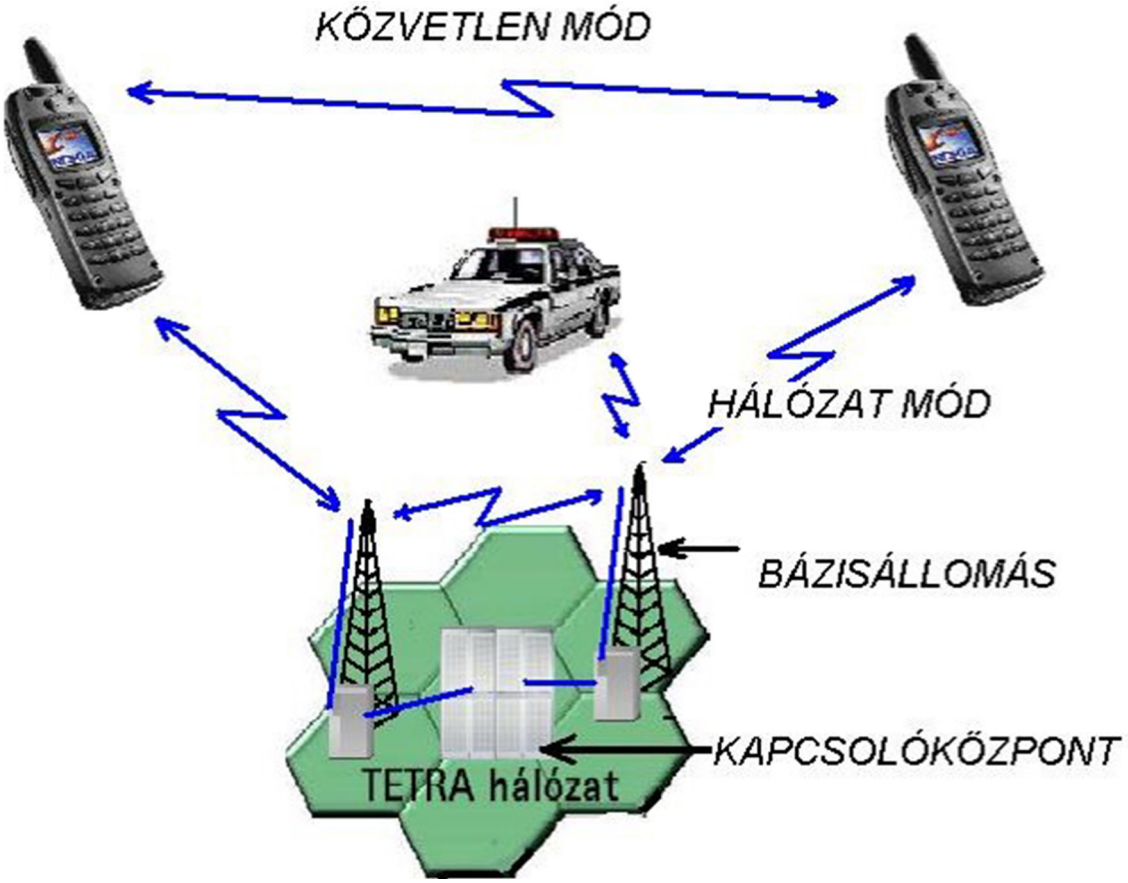
- szélesebb frekvenciaátvitel (a teljes hangfrekvenciás sáv átfogása),
- jobb jel-zaj viszony,
- nagyobb dinamikatartomány,
- nincs jeltorzulás.

Az információátvitel biztonságát mind a beszéd, mind az adatátvitel esetén háromszintű rejtjelezési eljárás védi, amely gyakorlatilag lehetetlenné teszi az információk illetéktelen lehallgatását. A jogosultságvizsgálat és a szigorú hozzáférés-ellenőrzés mechanizmusai garantálják, hogy csak az arra jogosult személyek férhessenek hozzá a hálózathoz. A rendszer által alkalmazott csatornakiosztás ma az egyik leghatékonyabb megoldásnak tekinthető (25 kHz/4 csatorna), másrészt a trönkölési technika segítségével minden csatornához minden felhasználó hozzáfér. A rendszer fő működési módja a csoportkommunikáció, amely tipikusan egy diszpécser és a hozzá tartozó csoport tagjai közötti kapcsolattartást szolgálja, amely által mindenki közvetlenül nyomon követheti a történéseket. A segélykérő hívások minden esetben prioritást élveznek, szükség esetén akár más, meglévő összeköttetés megszakítása árán is felépülnek.

A különböző adattovábbítási szolgáltatások természetesen a digitális szolgáltatási mód adottságait kihasználva (az analóg rádiózáshoz képest) más, egyértelmű funkciókiterjesztést jelentenek.

Alapvetően két kommunikációs üzemmódot különböztetünk meg az EDR-rendszerben:

- Hálózati üzemmód (TMO): normál működési mód. Ebben a módban a felhasználó a TETRA-rendszer által szabályozottan az összes szolgáltatáshoz hozzáfér.
- Közvetlen üzemmód (DMO): lehetővé teszi a tagállomások (terminálok) számára, hogy szimplex üzemmódban, minden infrastruktúra nélkül kommunikáljanak. Ez a képesség kiemelt fontosságú, mert olyan területeken teszi lehetővé a kommunikációt, amelyeket az infrastruktúra nem fed le (alagutak, hegyvidék, nagyobb kiterjedésű lakatlan területek stb.).



4. ábra: EDR-üzemmódok (forrás: BM OKF)

Az adattovábbítási szolgáltatások közül az alábbiak emelhetők ki:

- adatüzenet továbbítása (pl. SDS), ahol a felhasználó által bevitt rövid üzenetek küldhetőek a hálózaton belül;
- státuszüzenetek, előre definiált vagy egyénileg szerkeszthető szöveges üzenetek, amelyek a felhasználó állapotáról tájékoztatnak (pl.: intézkedem, mentést hajtok végre, súlyos sérültet látok el, utasítást várok stb.);
- csomagkapcsolt adatátvitel, ahol a hagyományos csomagkapcsolt üzenetküldési módon a lehető leghatékonyabb erőforrás-felhasználással történik az adatforgalmazás.

Az EDR-rendszer legnagyobb felhasználója a rendőrség. A BRFK az elsők között kezdte meg az EDR-rendszerre történő átállást. A készenléti szervezeteknek nem egyszerűen a kommunikációja lett fejlettebb a rádiótechnológia használatával, de a mindennapi feladataikat is hatékonyabban végzik, valamint további fontos felhasználói előnye a rádiótechnológiának a műveletirányítás lehetősége. A katasztrófavédelem napjainkban már több mint 8000 eszközzel használja hálózatot. A megyei igazgatóságokon lévő DWS-ek teszik lehetővé a megyei menedzserek számára a rádiók gyors beillesztését a rendszerbe, a rádiók jogosultságainak azonnali megváltoztatását. A hálózati és rádiós beállításoktól függően így országos használatú beszédcsoportok is létezhetnek.

Az 52-es katasztrófavédelmi EDR VPN-használatát természetesen szigorú szabályok alakítják. Ez országos szinten főigazgatói intézkedésben (általános VPN-használati szabályzat), területi és helyi szinten pedig különös VPN-használati szabályzat formájában nyilvánul meg.[9] A rádiórendszer használatában az informatikai főosztály által megfogalmazott rádióforgalmi alapelvek érvényesülnek. Az alapelvek kialakításánál a hivatásos tűzoltók korábbi gyakorlatát érvényesítették, a rádiós infrastruktúra minél észszerűbb és hatékonyabb felhasználásával. Külön csoportokat alakítottak ki a káresemények helyszíni kommunikációjának biztosítására, a különböző szintű ügyeletek közötti, valamint a társszervekkel történő együttműködésre. Az így kialakított, or-

9 53/2015. BM OKF főigazgatói intézkedés a BM Országos Katasztrófavédelmi Főigazgatóság, mint EDR VPN gazda szervezetnek az egységes digitális rádiótávközlő rendszer 52-es virtuális magánhálózat üzemeltetésének és használatának általános VPN szabályairól.

ságosan több mint ezer katasztrófavédelmi beszédcsoportot beprogramozták az összes, 52-es VPN-t használó rádióterminálba, azonban a diszpécserek az adott helyzetben módosíthatják a felhasználók jogosultságát az általános VPN-használati szabályzatban foglaltaknak megfelelően. A rádióterminálok esetleges elvesztése esetén a diszpécser a készüléket haladéktalanul kitiltja a rendszerből, így megelőzve az illetéktelen használatot.

A rádióterminálok beszerzésénél, a közbeszerzés szabályait maradéktalanul betartva, az Informatikai Főosztály törekedett az egységes eszközpark megtartására. Ennek ellenére a Fővárosi Katasztrófavédelmi Igazgatóságon EADS típusú, míg a megyei igazgatóságokon, illetve a főigazgatóságon Sepura kézi és mobil (járműbe szerelt), valamint Motorola kézi és stabil (asztali) rádiók működnek. Az elmúlt két évben az önkéntes tűzoltó egyesületek részére kiírt pályázatoknak köszönhetően már egyre több önkéntes tűzoltó is használhatja a rendszert. A rádiók első használatát megelőzi a szolgáltató által egy úgynevezett *K kulcs* betöltése a rádióba. Ezen hitelesítés nélkül a terminál nem használhatja a hálózatot. A kulcs betöltését követően az igazgatóságok szakemberei a hatályos szabályzókban foglaltaknak megfelelően felprogramozzák a rádiókat, majd a diszpécser-munkaállomásokon beállítják a jogosultságokat.

A hivatásos katasztrófavédelmi szervek műveletirányítási feladatait, valamint az igazgatóságok EDR-menedzseri feladatait ellátó személyek számára a BM OKF egy teszt- és vizsgakabinetet üzemeltet. A kabinetben elhelyezett hálózatban lévő szimulátori feladatokat ellátó számítógépeken teszt- és vizsgaszoftver üzemel. A Katasztrófavédelmi Oktatási Központ kezelésében lévő teremben a fluktuáció függvényében évente több négynapos tanfolyamot rendeznek, ahol az Informatikai Főosztály EDR-menedzsereinek vezetésével vizsga zajlik. Az objektív, számítógépes alkalmazással működő vizsga sikeres letételét követően a diákok bizonyítványt kapnak, amelynek birtokában elláthatnak bizonyos szolgálati feladatokat.

Az 52-es katasztrófavédelmi EDR VPN-központ diszpécseri feladatait a Rádiós Segélyhívó és Infokommunikációs Országos Egyesület (RSOE) végzi. A központi diszpécser révén az év 365 napján, a nap 24 órájában mindenre kiterjedő segítség áll a felhasználók rendelkezésére, valamint biztosítja a hiteles kapcsolattartást a szolgáltató ügyfélszolgálata, valamint hálózatfelügyelete felé. Az esetleges katasztrófahelyzetek, kiemelt országos események megnövekedett felhasználói igényeinek biztosítására a szolgáltató több mobil EDR-bázisállomást tart készenlétben. A mobil bázisállomások kirendelésére – szerződésben meghatározott esetekben és díjazásért – az Informatikai Főosztálynak van lehetősége.

4.4. Lakossági riasztás és tájékoztatás

A történelem során mindig fontos volt a veszély közeledtének, a kialakult veszélyhelyzetnek és a fenyegetés elmúltának valamilyen (egyeztetett) formában történő jelzése. Ahhoz, hogy a jelzés vételét követően az emberek valóban azt tegyék, ami az adott helyzetnek megfelelő magatartási forma, egyrészt mindenkinek ismernie kell a jelzéseket, másrészt olyan műszaki módszereket kell alkalmazni, amelyek (lehetőség szerint) minden körülmények között hitelesen alkalmazhatók riasztási jelzés leadására.

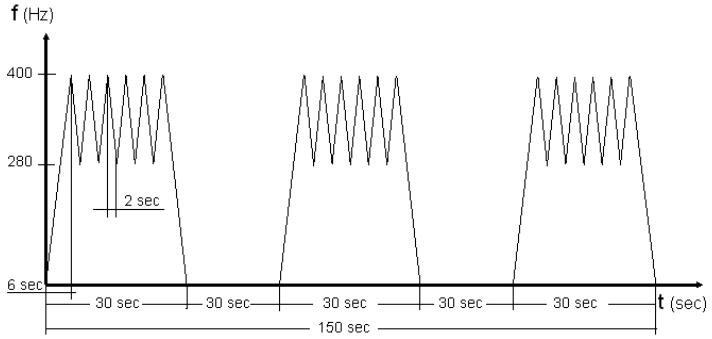
A magyar állam és a hivatásos katasztrófavédelmi szervek egyik alapvető feladata, hogy a lakosság élet- és vagyonbiztonságát veszélyeztető helyzetben – vagy még inkább a helyzet kialakulása előtt – a lakosságot a lehető legrövidebb időn belül tájékoztassa a problémákról, a követendő magatartási formákról (pl.: kimenekítés, kitelepítés, elzárkóztatás). Ez a helyzet lehet szinte pontszerű kiterjedésű, több települést érintő, de akár országos is. A vészhelyzet oka lehet meteorológiai, természeti, épített emberi környezeti katasztrófa vagy annak lehetősége. Az okokat és az érintett területet/lakosságot figyelembe véve a katasztrófavédelem nagyon sokféle riasztó és riasztó-tájékoztató rendszert üzemeltet.

A lakosság riasztását és tájékoztatását a hivatásos katasztrófavédelmi szervek több szakterülete koordinálja. A szakterületi koordináció alapján az alábbi két folyamat azonosítható:

1. A *polgári védelmi szakterület* az elektronikus médiumokkal megkötött szerződések, együttműködési megállapodások alapján az országos és helyi rádió- és televíziócsatornákon keresztül tájékoztatja a lakosságot. Jelen tananyag nem tartalmazza a polgári védelmi szakterület ez irányú feladatait, tevékenységét.
2. A *BM OKF informatikai szakterülete* a lakosság tájékoztatását a fentieken túli, a következőkben részletezett rendszerekkel biztosítja.

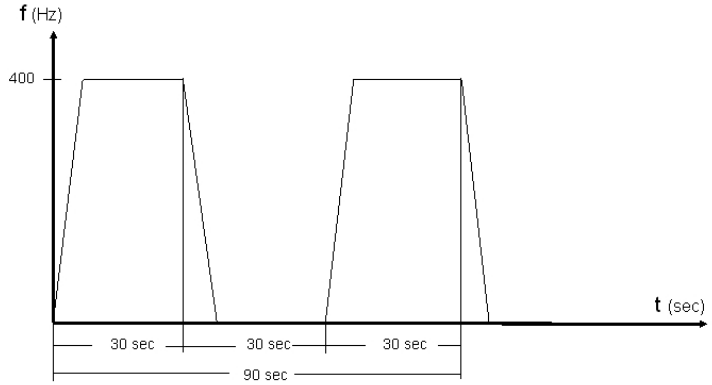
4.4.1. Lakossági riasztó végpontok (motoros szirénák)

Magyarországon a lakosság riasztására szolgáló eszközöket (motoros szirénákat) nagy mennyiségben a II. világháborút megelőző, illetve az azt követő években telepítették. Akkoriban az általános elvárás az eszközökkel szemben a magas rendelkezésre állás, az alacsony karbantartás igény, az egyszerű (tömeg-) gyártás lehetősége volt. A korszakra jellemző, hogy az ország veszélyeztetettsége jellemzően háborús természetű volt (légi fenyegetettség). A légi veszélyeztetettségnél alkalmazandó magatartási formához elegendő volt a sziréna (hangjelzés: légiriadó elrendelése, riadó elmúlt jelzés).



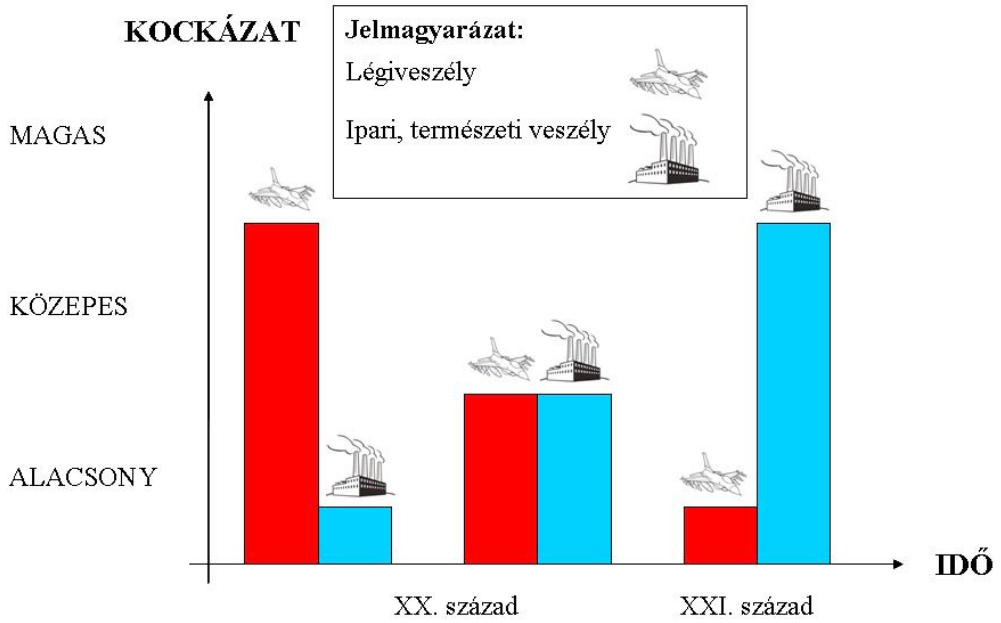
5. ábra: Légiriadó elrendelése (forrás: BM OKF)

A légiriasztás jele a polgári védelem riasztási rendszerén: háromszor egymás után megismételt, 30 másodpercig tartó, váltakozó (280 Hz és 400 Hz közötti) hangmagasságú szirénahang, a jelzések között 30 másodperces szünetekkel.



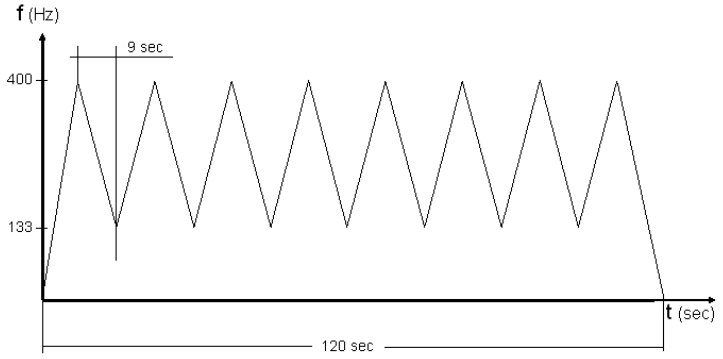
6. ábra: Riadó elmúlt jelzés (forrás: BM OKF)

A riadó elmúlt jelzés: kétszer egymás után megismételt, 30 másodpercig tartó, egyenletes hangmagasságú (400 Hz) szirénahang, a jelzések között 30 másodperces szünettel. A riadó elmúlt jelzés a légiriadó, valamint a katasztrófariadó elmúlt jelzés feloldására is vonatkozik. Légiriadó esetén a lakosoknak védett helyre (óvóhely) kellett vonulni, és a rádió- vagy tévéadáson keresztül kaptak információt a helyzetről. A (vegy)ipari tevékenység folyamatos fejlődése (nagyobb mennyiségű vegyi anyagok gyártása, tárolása, szállítmányozása), a klímaváltozás hatásainak érvényesülése (pl. villámárvizek) miatt egyre inkább áthelyeződött a hangsúly a háborús fenyegetettségről a természeti (ipari) katasztrófákra.



7. ábra: A kockázatok változása (forrás: BM OKF)

A ’80-as évektől egyre inkább szükségessé vált megteremteni annak lehetőségét, hogy a veszélyes üzemek környezetét figyelmeztetni tudják egy esetleges katasztrófaveszélyre. A lehetséges alternatívák közül az a költséghatékony megoldás született, amelynek keretében a meglévő (csak légiriasztásra és feloldásra alkalmas) szirénavégpontokat „katasztrófaveszély-jelzés” leadására tették alkalmassá.



8. ábra: Katasztrófariadó elrendelése (forrás: BM OKF)

Katasztrófariadó jelzése: 120 másodpercig tartó, *váltakozó (133 és 400 Hz közötti)* hangmagasságú, folyamatos szirénahang.

9. ábra: Próbajelzés (forrás: BM OKF)

A próba során alkalmazott jelalak első részében 6 másodperces időtartamban 400 Hz-ig felfutó jelzést adnak le, majd a jel lefutása következik. Ezzel a fejlesztéssel a lakosoknak két (egymástól eltérő) magatartási formát elrendelő jelzést kellett (fel)ismerniük. Az így kialakított jelzéseken túlmenően további igény volt az eszközök minél gyorsabb vezérelhetősége (ezáltal a riasztási jelzések minél korábbi leadása). A motoros szirénavégpontokat jellemzően manuálisan lehet vezérelni (egy személy egy végponton tud jelzést leadni). Több megoldás is napvilágot látott mint központi vezérlés (pl.: telefonvonalakon történő vezérlés), amelyek közül a leghatékonyabbnak az erősáramú hálózaton történő vezérlés bizonyult. A központi vezérlést nem országos szinten alakították ki, jellemzően szigetszerűen működött, például egy-egy nagyobb üzem (pl.: atomerőmű) körzetében.

Idővel ezek a fejlesztések sem tudták biztosítani azt, hogy a motoros szirénavégpontok a kor követelményeinek megfeleljenek. A légi riasztással ellentétben katasztrófaveszély esetén nem lehet egyértelműen meghatározni egyetlen olyan magatartási formát, amelyet követve a lakosok testi épsége biztosítható lenne. Lehetnek olyan esetek, amikor az elzárkóztatás elegendő, előfordulnak azonban olyan esetek is, amikor az adott területen élőket ki kell menekíteni, és biztonságos helyre kell szállítani.

11. kép: Motoros sziréna (forrás: BM OKF)

A riasztórendszerrel szemben újabb követelményként jelentkezett az „élőbeszédes” tájékoztatás szükségessége. A 21. század elején elérkezett az az idő, amikor a motoros szirénavégpontok – a több évtizedes (mintegy félszáz éves) szolgálat után – már nem tudták biztosítani az elvárt védelmi szintet.

A motoros szirénák tulajdonságai:

- alkalmas a jogszabályban megfogalmazott riasztási jelzések leadására;
- tájékoztatásra nem alkalmas, nem is tehető alkalmassá;
- azonnali riasztásra alkalmassá tehető;
- karbantartás igénye alacsony, egyszerű javítani;
- az eszközök erősáramú hálózati kimaradás esetén üzemképtelenné válnak (szünetmentesítésük nem megoldható).

12. kép: Modern lakossági riasztó-tájékoztató eszköz (forrás: BM OKF)

4.4.2. Az LTRR (Lakossági Tájékoztató és Riasztórendszer)

A hivatásos katasztrófavédelmi szervezet megalakulását követően, vagyis 2000. január 1. után, szinte azonnali feladatként jelentkezett, hogy a paksi atomerőmű környezetében élő lakosságot a lehető legrövidebb időn belül tájékoztassák egy esetleges üzemi meghibásodás esetén. Az elsődleges kockázati tényezők azonosítása után megfogalmazódott, hogy az erőmű 30 km-es környezetében élő lakosság részére egy elektronikus szirénarendszert kell kiépíteni. A kiépített rendszer 227+1 szirénavégpontból, két stabil (Tolna MKI és Paks védett vezetési pont), valamint egy hordozható vezérlőközpontból áll.

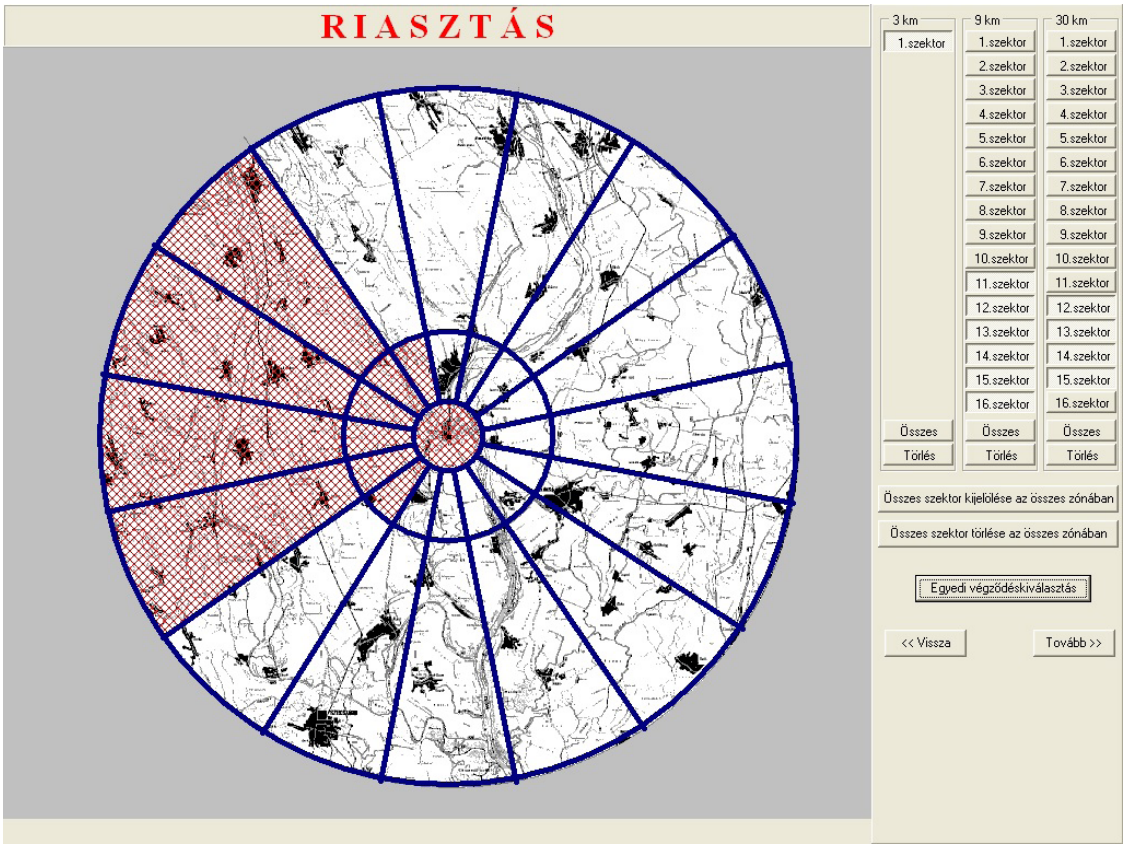
Az LTRR alapvető funkciói:

- *Előre definiált szignálok kiadása:* légiriadó, veszély elmúlt, katasztrófariadó, morgatópróba. A szignálok indíthatóak központról, illetve egyedileg, minden letelepített végződés kezelőfelületéről.
- *Előre tárolt:* központi oldalon „rögzített” közlemények kiadása.
- *Élőbeszéd sugárzása:* a kialakított központokban lévő vezérlő számítógépről élőbeszédes közlemény indítható. Ez a funkció elérhető minden letelepített végződésről az egység kezelőfelületén lévő mikrofonról.
- *„Csendes teszt” funkció:* központi oldalról van lehetőség a végződések tényleges működését szimuláló funkcióvizsgálatra. A csendes teszt ellenőrzi a központtól a hangszórók membránjáig a rendszer összes elemét (ütemezhető funkció).
- *Folyamatos önteszt:* a végződések vezérlése folyamatos öntesztet végez, a működéssel kapcsolatos funkciók állapotváltozásáról azonnali jelzést, illetve riasztást ad a központi egység felé. Ez alól kivételek a szirénaerősítők és a szirénadriverek (hangnyomók), amelyek ellenőrzésére csak a csendes tesztek alkalmával van lehetőség.

A tájékoztatás és riasztás kiadásának lehetőségei:

- A központi oldalon telepített vezérlő számítógépről a riasztási körzetek az előre tárolt lehetőségek szerint indíthatók.

- Az összes végződés egyidejű indítása.
- Előre képzett zónák és szektorok végződéseinek indítása: a zónák és szektorok a vezérlő számítógépben vannak tárolva. Később telepített végződések bármikor integrálhatók az adott zóna riasztási csoportjába.
- Előre definiált csoportok végződéseinek indítása: az adott települések végződései a vezérlő számítógépbe a települések nevével vannak tárolva. Amennyiben új végződés telepítésére kerül sor valamelyik településen, akkor az új végződés hozzárendelhető az adott település végződéseihez.
- Egyedi végződések indítása: a vezérlőrendszer alkalmas a telepített összes végződés egyedi címzésére és a kijelölt végződés indítására.
- Azonnali (dinamikus) csoportképzés a valós riasztási helyzetnek megfelelően: a rendszer biztosítja, hogy a pillanatnyi szituáció függvényében a végződések a terminálon tetszőlegesen összerendezhetők legyenek. Így a dinamikusan összerendelt riasztási zónákra a ténylegesen aktuális információ adható le. A dinamikusan szervezett csoport addig aktuális, amíg a kezelő a riasztási menüben van. A menüből való kilépéskor a csoport törlődik.



10. ábra: Az LTRR-zónák (forrás: BM OKF)

Az illetéktelen megszólaltatás ellen a rendszer különböző biztonsági elemekkel rendelkezik. A központi megszólaltatás biztonsági kártyához és PIN-kódhoz kötött, míg a végpontok egyedi megszólaltatásához csak PIN-kód szükséges. A jogosultsági szintek a kártyákhoz hozzárendelhetők. Az érintett települések polgármestereinek kérésére a rendszer tartalmaz egy úgynevezett „kisbíró” funkciót, amelyben az önkormányzatnál telepített konzolról a jogosítással rendelkező személy (a település polgármestere) élő szóban közleményeket adhat ki. A konzol az adott település végződéseire adja ki a közleményt.

A rendszer átviteli útként digitális trönkölt rádiórendszert használ. A rádiórendszer elemeinek gyártó oldali támogatása 2014-ben megszűnt. A megszűnéssel párhuzamosan elkezdődött a rendszer továbbfejlesztési lehetőségeinek vizsgálata. A lehetséges technológiák figyelembevételével a szakmai tervezőcsapat az EDR mint átviteli technológia használatát tűzte ki célul. 2014-ben a rendelkezésre álló források miatt 124 végpontot állítottak át EDR-es vezérlésre. Ennek kapcsán fejlesztették a központi vezérlőrendszert és az adott végpontokat is. A fennmaradó 104 végpont fejlesztése 2015. június 30-ig megtörtént.

4.4.3. Viharjelző rendszerek

A viharjelző rendszerek fontos, bár lokális elemei a lakossági riasztó- és tájékoztató rendszereknek. Magyarországon a Balatonon, Hille Alfréd (repülőezredes, meteorológus) kezdeményezésének és kitartásának köszönhetően először 1934-ben indult el viharjelzés. A kezdetleges szirénákból, jelzőkosarakból és különféle mentőcsónakokból álló rendszert 1951-ben szervezték át. Ettől az évtől a Belügyminisztérium irányításával már viharágyúkkal és jelzőrakétákkal valósult meg a fürdőzők tájékoztatása. A sárga és piros jelzőrakéta jele tiszta időben elég messziről volt észlelhető, azonban indításuk körülményes és lassú volt.

A balatoni viharjelző rendszer (a továbbiakban: BVR) 1988-tól jelentős fejlesztésen ment keresztül. A fejlesztés eredményeképp kiépült egy automata meteorológiai mérőhálózat a tó körül. A hálózat pontjainak mérése alapján egy 25 viharjelző lámpából álló rendszer felvillanó fényjelzéseket adott. A rendszer két medencére tagozódott annak érdekében, hogy a kis kiterjedésű időjárási képződmények miatt ne történjenek felesleges korlátozások. Szintén ebben az évben helyeztek üzembe két állomást a Velencei-tó partján is.

2000-ben az Országos Katasztrófavédelmi Főigazgatóság megalakulásával a viharjelző rendszerek üzemeltetési feladatait a Somogy Megyei Rendőr Főkapitányságtól átvette a BM OKF. Az átadáskori műszaki, technikai, technológiai lehetőségekhez képest napjainkra jelentős változások történtek a viharjelzés terén. A 2001-től fokozatosan egy új, villanócsöves technológiát vezettek be. Az új villanócsövek jelentős energiamegtakarítást eredményeztek, azonban sajnos az üzemidejük rövidsége miatt a fenntartási költségek nem csökkentek az elvárásoknak megfelelően. 2014-től ezért egy új, LED-technológián alapuló rendszer bevezetésébe kezdtek.

2001-ben elfogadták az azóta többször módosított 46/2001. (XII. 27.) BM rendeletet. A rendelet értelmében jelenleg Magyarországon a Balatonon – keleti, középső és nyugati medencére bontva –, a Velencei-tavon, a Tisza-tavon és a Fertő tavon minden év április elsejétől október harmincegyedikéig vihar-előrejelző és viharjelző szolgálat működik. A vihar-előrejelző rendszer technikai előkészítését, fejlesztését, létrehozását, valamint – a Fertő tavi viharjelző rendszer kivételével – a működtetést a BM Országos Katasztrófavédelmi Főigazgatóság végzi.

A fenti BM rendelet értelmében az I. fokú viharjelzés (figyelmeztetés az elővigyázatosság betartására) percenként negyvenötször felvillanó sárga fényjelzése esetén a parttól 500 méternél nagyobb távolságra tilos fürödni. A II. fokú viharjelzés (figyelmeztetés a fenyegető veszélyre) percenként kilencvenszer felvillanó sárga fényjelzése esetén fürödni tilos.

13. kép: Balatoni viharjelző, 2015 (forrás: BM OKF)

Jelenleg a Balaton térségében 31 fixen telepített viharjelző végpont működik, amelyek közül már 12 korszerű LED-es technológiát használ. A rendszer lehetőséget kínál további mobil állomások integrálására, amelyek a fürdőzők által gyakrabban látogatott partszakaszokra helyezhetők ki. Ezek jellemzően a főszezonban működnek.

14. kép: Balatoni viharjelzők elhelyezkedése, 2015 (forrás: RSOE)

Fertőrákoson, a Fertő tó partján, az osztrák partner által működtetett rendszerhez kapcsolódóan egy magyarországi végpont működik. A Velencei-tó körül jelenleg 3 végpont üzemel, míg a Tisza-tó partján 5 viharjelző állomás működik. A mindenkori viharjelzést az Országos Meteorológiai Szolgálat adja ki. Az állomások, valamint a vezérlésüket kiszolgáló és az ehhez kapcsolódó adatátviteli rendszerek folyamatos korszerűsítése a pénzügyi és a technikai keretekhez igazodva folyamatosan zajlik.

4.4.4. A MoLaRi (Monitoring és Lakossági Riasztórendszer)

A MoLaRi kialakításának gondolata a 2000-es évek második felében fogant meg, amikor is felmerült az igény arra, hogy a veszélyes vegyi anyagokat feldolgozó üzemek körzetében élő lakosságot érintő biztonsági kockázatot a lehető legkisebb mértékűre csökkentsék.

A Katved. tv.-ben és a végrehajtási rendeleteiben foglaltak alapján a veszélyes anyagokkal foglalkozó üzemeket három kategóriába lehet besorolni: küszöbérték alatti, valamint alsó és felső küszöbértékű üzem. Az üzemekben előforduló anyagok összetételének, mennyiségének, valamint az üzem környezetében élő lakosság számának függvényében 21 alsó és felső küszöbértékű ipari létesítményt jelöltek ki. Ezek belterületén, illetve a közvetlen környezetükben monitoringvégpontok gyűjtik a veszélyes anyagok jelenlétére utaló adatokat. A mérő végpontokat üzemspecifikus szondákkal szerelték fel, amely szondák végpontonkénti duplikációja biztosítja a megfelelő redundanciát. A végpontok egy része meteorológiai információkat is szolgáltat. A mérések eredményeit a végpontok zárt belső hálózaton keresztül továbbítják a területi központokba. A központokba továbbított adatok az üzemben, az MKI-n, valamint az országos központban is megjeleníthetők.

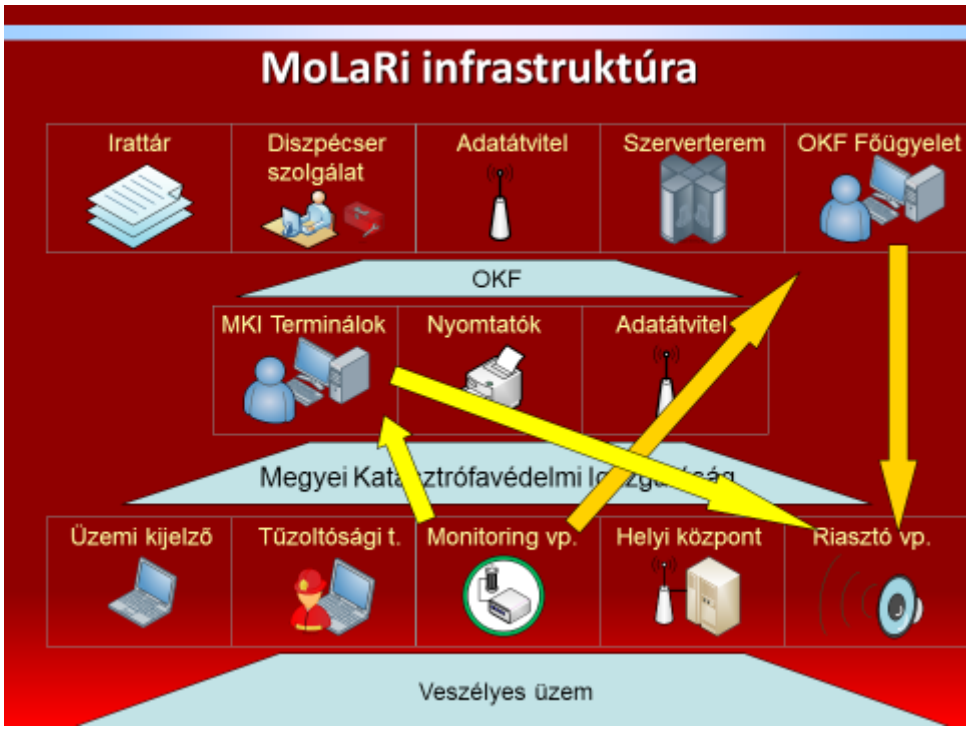
11. ábra: A MoLaRi elvi vázlata (forrás: Endrődi István előadása, 2015)

A rendszer bázisát képező szerverek, valamint az aktív adatátviteli berendezések konstrukciója rendkívül robusztus. A szerverközpont tartalék energiaellátását pufferüzemben töltött akkumulátorok, leválasztó inverter és automatikusan induló áramfejlesztő biztosítja. A végpontok tartalék energiaellátása szünetmentes tápegységről történik.

A szerverközpont, a regionális kommunikációs központok és a helyi központok közötti adatátvitelt egy 100%-osan tartalékolt IP-hálózat valósítja meg. Az IP-hálózat elsődleges útvonalai optikai szál, valamint mikrohullámú technológia segítségével valósulnak meg. A tartalék útvonal kiépítése (jellemzően) mikrohullámú vagy ISDN-technológia alkalmazásával történik. A helyi központok és az érzékelő, valamint szirénavégpontok közötti adatátvitel ipari szabványokon alapul. A rendszer kliens-szerver architektúrájú, így a magas rendelkezésre állása és rugalmassága (skálázhatósága) is biztosítható. A MoLaRi rendszerben vékony klienstechnológia is megtalálható. A MoLaRi biztosítja – az arra jogosult felhasználók számára – a hozzáférést, míg a jogosulatlan hozzáférést egyértelműen kizárja és naplózza, tehát biztosítja a felhasználóhoz és művelethez kötött naplózás lehetőségét.

A MoLaRi működésének alapját az alábbi folyamat jelenti:

A veszélyes üzemben egy esetlegesen kialakuló meghibásodás/baleset miatt veszélyes vegyi anyag (gáz) kerülhet a levegőbe, amelynek koncentrációját a telepített mérőszondák (monitoringvégpontok) mérik, és ezzel párhuzamosan jelzik az értéket a katasztrófavédelem ügyeletén is.



12. ábra: A MoLaRi infrastruktúrájának működési elve (forrás: BM OKF)

A rendszerbe implementáltak egy olyan döntéstámogató modult, amelyben a mért adatok automatikusan megjelennek, és a bementi adatok alapján egy egzakt modellezés futtatható le a kiszabadult veszélyes anyag terjedésének irányára és sebességére vonatkozóan. A modellezés alapján az ügyeleti szolgálatok kiválasztják az érintett lakosság területén lévő riasztó végpontokat, amelyek segítségével tájékoztathatják, illetve riaszthatják a veszélyeztetett személyeket. A szirénarendszerrel történő tájékoztatás tartalmazhat magatartási szabályokat, gyülekezési helyeket, menekülési útvonalakat is. A rendszer jelenlegi kiépítettségében mintegy 440 ezer lakos biztonságát szolgálja.

A rendszerben lévő eszközök mennyisége megyénkénti bontásban:

- Borsod-Abaúj-Zemplén: 90 monitoringvégpont, 45 riasztó végpont;
- Csongrád: 6 monitoringvégpont, 5 riasztó végpont;
- Heves: 6 monitoringvégpont, 19 riasztó végpont;
- Fejér: 29 monitoringvégpont, 59 riasztó végpont;
- Komárom-Esztergom: 33 monitoringvégpont, 37 riasztó végpont;
- Pest: 37 monitoringvégpont, 27 riasztó végpont;
- Tolna: 13 monitoringvégpont, 19 riasztó végpont;
- Veszprém: 47 monitoringvégpont, 50 riasztó végpont;
- Zala: 8 monitoringvégpont, 8 riasztó végpont;
- Budapest: 52 monitoringvégpont, 317 riasztó végpont.

A MoLaRi rendszer fejlesztése természetesen nem állt le. A 2014-ben, Budapesten letelepített végpontok már az EDR-rendszeren működő rádiókkal üzemelnek. A következő fejlesztési ciklusban elérhető uniós támogatás megléte esetén további üzemek, és ezáltal Magyarország lakosságának további része kerülhet nagyobb biztonságba.

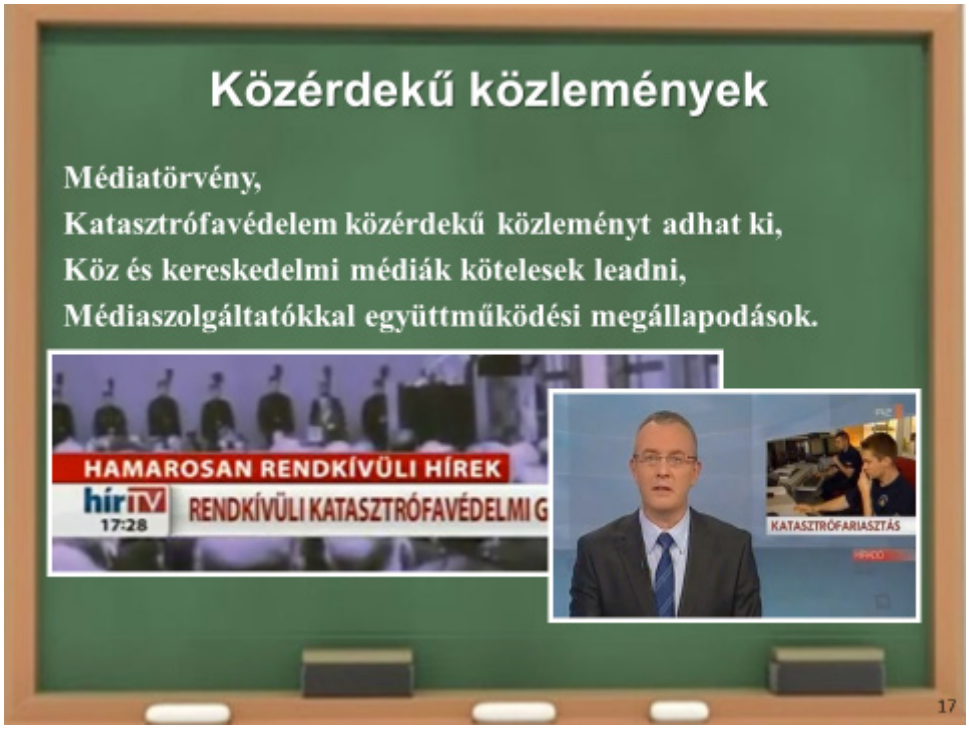
A MoLaRi megvalósulása esetén az alábbi eredmények várhatók:

- A veszélyes üzemek környezetében élő lakosság biztonságát jelentős mértékben javítja.
- A külső védelmi tervekben, illetve a települési veszélyelhárítási tervekben a súlyos ipari balesetekkel kapcsolatos lakosságvédelmi döntések, intézkedések a rendszer működése esetén lényegesen rövidebb idő alatt hozhatók meg, ezáltal az emberi életben és egészségben okozott károk kockázata csökken.
- A veszélyhelyzet kezelésében részt vevő (hivatásos) szervek megalapozott döntéshozatalát segíti elő.

4.5. A lakosság veszélyhelyzeti riasztását, tájékoztatását szolgáló egyéb eszközök, rendszerek, szolgáltatások

A lakosság védelme komplex feladatrendszer, amelynek részét képezik a katasztrófavédelem által működtetett lakossági riasztó, riasztó-tájékoztató végpontok. Az emberi élet, anyagi javak védelme érdekében – a lehetőségekhez képest – minden olyan eszközt fel kell használni, amely az adott veszélyhelyzetben rendelkezésre áll, és lehetőséget biztosít a katasztrófavédelem számára, hogy az adott területen élőket riassza, tájékoztassa. A teljesség igénye nélkül az alábbi rendszereket, szolgáltatásokat említhetjük, amelyeket a katasztrófavédelem használhat e célra:

- Marathon Terra;
- rádióközlemény, tv-szalagsávon megjelenő felhívás;
- Facebook;
- honlap;
- mobiltelefonos alkalmazások (a „mobiltelefóniában” használt, illetve az internet által elérhető szolgáltatások igénybevétele, pl.: SMS, VÉSZ, Tavihar alkalmazás);
- mobil kihangosító eszköz (autóba, esetleg utánfutóra szerelt hangosító berendezés), mobil kivetítő, fényjelző eszköz;
- egy adott rendezvény, gyáregység kihangosító vagy képi megjelenítő rendszere;
- szükségriasztó eszközök.



13. ábra: A lakossági tájékoztatás elektronikus formái (forrás: Endrődi István előadása, 2015)

4.6. Mobil vezetési pontok

Katasztrófahelyzetekben, illetve az azokat közvetlenül megelőző időszakban a beavatkozást végző hivatásos és önkéntes szervezetek munkáját a hivatásos katasztrófavédelmi szervek békeidejű települési helyein operatív törzsek vezetik, koordinálják. Az operatív törzsek úgynevezett stabil vezetési pontokban végzik munkájukat. Ezeket a helyiségeket a katasztrófahelyzeteket megelőző időszakban felszerelték a lehető legkorszerűbb informatikai, távközlési eszközökkel. Az eszközök működését természetesen a megfelelő szintű rendelkezésre állású, sávszélességű hálózatok biztosítják. Ezek a vezetési pontok mindaddig elégségesek, amíg a katasztrófahelyszínen lévő beavatkozó erők száma csekély, vagy amíg a helyszínen lévő informatikai, távközlési infrastruktúra elegendő a beavatkozó erők irányításához. Hosszabb időn át tartó, nagyobb erők jelenlétét kívánó katasztrófahelyzetek esetén vagy nem megfelelő távközlési infrastruktúrával rendelkező helyszíneken azonban a helyi erők koordinációját végző mobil vezetési pont felállítása válhat szükségessé. Ezekre az esetekre felkészülve a BM OKF három, mobil vezetési pontként vagy azok támogatásaként használható, úgynevezett mobil vezetési pont járművet üzemeltet.

A mobil vezetési pontok különféle terepen alkalmazhatók és különféle átviteli utakat biztosítanak. Mindhárom jármű képes több napon keresztül önálló működésre, vezetékes vagy WIFI-hálózat létesítésére a helyi operatív törzs részére, a beavatkozó erők számára EDR-rádiókkal történő megerősítésre, GSM- vagy műholdas átviteli úton a katasztrófavédelem belső informatikai hálózatán lévő erőforrások használatára. A járművekben málházott eszközök lehetőséget nyújtanak gyenge EDR-lefedettségű földrajzi helyeken EDR-átjáróval vagy DMO-ismétlőállomással a hálózati hozzáférés kiterjesztésére is. A járművek az analóg URH-rádiórendszereket használó civil szervetekkel történő együttműködés érdekében rendelkeznek szabadon programozható rádiókkal is. A járművek hivatalos rendszerbe állítása 2015-ben történt meg, a felhasználásuk szabályait főigazgatói intézkedés szabályozza.

FELHASZNÁLT IRODALOM ÉS JOGFORRÁSOK

Magyarország Alaptörvénye

1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról

2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről

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

2011. évi LXXVIII. törvény a Genfben, 2000. május 26. napján kelt, a Veszélyes Áruk Nemzetközi Belvízi Szállításáról szóló Európai Megállapodáshoz (ADN) csatolt Szabályzat kihirdetéséről és belföldi alkalmazásáról

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

2013. évi CXCII. törvény egyes törvényeknek a katasztrófák elleni védekezés hatékonyságának növelésével összefüggő módosításáról

190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről

219/2011. (X. 20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről

234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

290/2011. (XII. 22.) Korm. rendelet a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény egyes rendelkezéseinek végrehajtásáról

312/2011. (XII. 23.) Korm. rendelet a hivatásos katasztrófavédelmi szerv eljárásai során a veszélyes áruk vasúti és belvízi szállításának ellenőrzésére és a bírság kivetésére vonatkozó egységes eljárás szabályairól, továbbá az egyes szabálytalanságokért kiszabható bírságok összegéről, valamint a bírságolással összefüggő hatósági feladatok általános szabályairól

139/2012. (VI. 29.) Korm. rendelet a katasztrófa-egészségügyi ellátásról

367/2012. (XII. 17.) Korm. rendelet a BM Országos Katasztrófavédelmi Főigazgatóság piacfelügyeleti eljárásának részletes szabályairól

57/2013. (II. 27.) Korm. rendelet a telepengedély, illetve a telep létesítésének bejelentése alapján gyakorolható egyes termelő és egyes szolgáltató tevékenységekről, valamint a telepengedélyezés rendjéről és a bejelentés szabályairól

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének tartalmáról

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

45/2014. BM OKF főigazgatói intézkedés a BM Országos Katasztrófavédelmi Főigazgatóság Informatikai Biztonság Politikájának, továbbá annak megvalósítását célzó Informatikai Biztonsági Szabályzatának kiadásáról

66/2014. BM OKF főigazgatói intézkedés a hivatásos katasztrófavédelmi szervek informatikai szakterületének Gazdálkodási Szabályzatáról szóló 6/2013. számú BM OKF főigazgatói intézkedés módosításáról

53/2015. BM OKF főigazgatói intézkedés a BM Országos Katasztrófavédelmi Főigazgatóság, mint EDR VPN gazda szervezetnek az egységes digitális rádiótávközlő rendszer 52-es virtuális magánhálózat üzemeltetésének és használatának általános VPN szabályairól

3/2016. (IV. 29.) BM OKF utasítás a BM Országos Katasztrófavédelmi Főigazgatóság Szervezeti és Működési Szabályzatának kiadásáról

Bognár Balázs, Bonnyai Tünde, Görög Katalin, Kátai-Urbán Lajos, Vass Gyula (2015): *Létfontosságú rendszerek és létesítmények védelme.* Kézikönyv a katasztrófavédelmi feladatok ellátására. Budapest, NKE.

Endrődi István (2013): *A katasztrófavédelem feladat- és szervezetrendszere.* Egyetemi jegyzet, Budapest, NKE.

Endrődi István (2015): *Polgári védelmi szakismeret 1.* Egyetemi jegyzet, Budapest, NKE.

Schweikhardt Gotthilf (2013): *Katasztrófavédelmi igazgatás.* Egyetemi jegyzet, Budapest, NKE.

Vass Gyula, Kátai-Urbán Lajos, Cimer Zsolt (2004): Veszélyes ipari üzemek nyilvántartása. In: *Védelem. Katasztrófa-, Tűz- és Polgári Védelmi Szemle,* 11. évf. 3. sz. 45–47.

A Nemzeti Közszolgálati Egyetem kiadványa

Nordex Nonprofit Kft. – Dialóg Campus Kiadó • www.dialogcampus.hu • www.uni-nke.hu
1094 Budapest, Márton utca 19. • Telefon: (1) 608 1488 E-mail: info@dialogcampus.hu
A kiadásért felel: Petró Ildikó kiadó- és nyomdavezető • Kiadói szerkesztő: Balla Zsófia • Tördelés: Corrigendum Kft.

ISBN 978-615-5680-18-2