

IV. Évfolyam 1. szám - 2009. március

Munk Sándor

Zrínyi Miklós Nemzetvédelmi Egyetem

munk.sandor@zmne.hu

Fleiner Rita

Budapesti Műszaki Főiskola

fleiner.rita@nik.bmf.hu

ADATBÁZISOK KRITIKUS INFRASTRUKTÚRÁKBAN

Absztrakt

Napjainkban a fejlett társadalmak egyre nagyobb mértékben függenek a különböző (energetikai, kommunikációs, informatikai, közlekedési, ellátási, stb.) infrastruktúráktól, a társadalmi, gazdasági és hétköznapi élet működési folyamatai, biztonsága így egyre inkább veszélyeztetettek a legfontosabb – kritikusnak nevezett – infrastruktúrák működésének, szolgáltatásainak megszakadása esetén. A kritikus infrastruktúrák működése ma már gyakorlatilag elképzelhetetlen az informatikai rendszerek, alkalmazások támogatása nélkül. Ily módon a kritikus infrastruktúrák működése veszélyeztethető az őket támogató informatikai rendszereken, illetve ezek egyes összetevőin, köztük adatbázisokon keresztül is. Jelen publikáció célja, hogy – egy kutatás részeként – hozzájáruljon az adatbázis-biztonság és a kritikus infrastruktúrák biztonsága közötti viszony feltárásához. Ennek érdekében rendszerezi és általánosságban értékeli az adatbázisok előfordulását, helyét és szerepét a különböző kritikus infrastruktúra szektorokban.

In our days developed societies increasingly depend on different (energetic, communication, information, transport, supply, etc.) infrastructures, and as a consequence, social, economical and every day processes are more and more threatened in case of disruption of the most important – so called critical - infrastructure services. Operation of critical infrastructures nowadays is practically unthinkable without the support of IT systems, applications, so critical infrastructures can be threatened through supporting IT systems, and their components, such as databases. The aim of this publication – as a part of a research – is to contribute to exploring relations between database security and critical infrastructure protection. For this purpose systematizes and gives an overall analysis of the presence and role of databases in different critical infrastructure sectors.

Kulcsszavak: *adatbázisok, kritikus infrastruktúra, kritikus infrastruktúra szektorok, felügyeleti és adatgyűjtő rendszerek, közhiteles nyilvántartások ~ databases, critical infrastructure, critical infrastructure sectors, supervisory control and data acquisition (SCADA) systems, public registers.*

Bevezetés

A fejlett XXI. századi társadalmak egyre nagyobb mértékben függenek a különböző (energetikai, kommunikációs, informatikai, közlekedési, ellátási, stb.) infrastruktúráktól és ezek az infrastruktúrák maguk is kölcsönösen függenek egymástól. A társadalmi, gazdasági és hétköznapi élet működési folyamatai, biztonsága így egyre inkább veszélyeztetettek a legfontosabb – kritikusnak nevezett - infrastruktúrák működésének, szolgáltatásainak megszakadása esetén.

A kritikus infrastruktúrák működése napjainkban már szinte elképzelhetetlen az informatika eszközeinek, rendszereinek, alkalmazásainak támogatása nélkül. Ez az informatikai támogatás részben önálló információs infrastruktúrák révén, részben önmagukban kritikus infrastruktúrát nem alkotó támogató összetevők révén jelenik meg. A támogató informatikai rendszerek jelentős részének működésében lényeges, esetenként kiemelt szerepet játszanak különböző adatbázisok is.

A kritikus infrastruktúrák működése számos különböző módon, ugyanakkor különböző összetevőiken keresztül veszélyeztethető (gátolható, akadályozható, csökkenthető). A veszélyeztetések lehetnek fizikai (anyagi) és információs jellegűek. Ez utóbbiak sajátossága, hogy a veszélyeztetett rendszerbe általa értelmezhető, feldolgozható információt juttat be, vagy a rendszer által kezelt információt, megvalósított információs tevékenységet módosít, töröl az adott rendszer saját folyamatai, résztevékenységei útján.

A banki szolgáltatásokra, egyes hálózatokra épülő szolgáltatásokra (energia-ellátás, közlekedés), vagy egyes közhiteles nyilvántartásokra gondolva legalábbis hipotézisként megfogalmazható, hogy az adatbázisok számos kritikus infrastruktúrában (ha nem valamennyiben) megtalálhatóak és ezek közül sok esetben biztonságuk megsértése (működésképtelenné tételük, meghamisításuk, adataik jogtalan megismerése) az adott kritikus infrastruktúra biztonságát fenyegeti. Ebből következően lényeges kérdés lehet az adatbázis biztonság kritikus infrastruktúra védelem szempontjából vett vizsgálata.

Jelen publikáció alapvető célja, hogy hozzájáruljon az adatbázisok biztonsága és a kritikus infrastruktúrák biztonsága összefüggéseinek feltárásához, az adatbázis biztonság kritikus infrastruktúra védelmen belüli helyének, szerepének meghatározásához. Ennek érdekében a publikáció feltárja, rendszerezi és általánosságban értékeli az adatbázisok előfordulását, helyét és szerepét a különböző kritikus infrastruktúra szektorokban.

A kutatás következő feladata – és egy következő publikáció tárgya – lehet az adatbázis-biztonság helyének, szerepének részletesebb elemzése egyes kiválasztott kritikus infrastruktúra szektorokban. Ennek az elemzésnek célszerűen olyan szektorokra kell kiterjednie, amelyekben az adatbázisok jelentősebb, 'kritikus' szerepet játszanak.

Adatbázisok, kritikus infrastruktúrák alapjai

Az adatbázisoknak a kritikus infrastruktúrákban betöltött helye, szerepe elemzéséhez elsőként röviden összegezzük az adatbázisok, majd a kritikus infrastruktúrák alapjait, alapvető fogalmait.

Az **adatbázisok** előzményeit a hagyományos nyilvántartások – meghatározott körbe tartozó, azonos típusú objektumok kiválasztott jellemzőit tartalmazó jegyzékek – képezték. Alapvető rendeltetésük (volt), hogy a bennük rendelkezésre álló információk kinyerhetőek legyenek (pld. egy adott objektum szerepel-e a nyilvántartásban; mi egy adott objektum adott jellemzőjének/jellemzőinek értéke).

A nyilvántartások kezelésének számítógépes támogatására először a fájl-alapú megvalósítások szolgáltak, majd ezt követte az adatbázisok megjelenése, amelyet az egyedi nyilvántar-

tásokkal szemben a szervezeti szintű, egyben gazdaságos hasznosítás igényei hoztak életre. Az eredeti értelmezés szerint az adatbázis egymással kapcsolatban álló adatok összessége, amely alkalmas több felhasználó különböző adatigényeinek kielégítésére. [1, 16.o.; 2, 14.o.] Mai megfogalmazások szerint az adatbázis adatoknak számítógépekben tárolt, valamely adatmodell szerint strukturált gyűjteménye. Az adatbázisokban tárolt adatok kezelését speciális alkalmazások, az úgynevezett adatbázis-kezelő rendszerek biztosítják.

A **kritikus infrastruktúrák** általános fogalma alatt olyan infrastruktúrákat (működtető személyzet, folyamatok, rendszerek, szolgáltatások, létesítmények, és eszközök összessége) értünk, amelyek megsemmisülése, szolgáltatásaik vagy elérhetőségük csökkenése egy adott felhasználói kör létre, lét- és működési feltételeire jelentős negatív hatással jár. A kritikus infrastruktúra ezen általános fogalmán belül az érintett felhasználói körtől függően meg kell különböztetnünk a nemzeti, európai, védelmi/katonai, szövetségi, vagy szervezeti kritikus infrastruktúrákat. [3, 96-97.o.]

A szakirodalomban gyakorlatilag teljes körűen elfogadott a kritikus infrastruktúrák egymástól való kölcsönös függése (ún. interdependenciája). Az összekapcsolódó, összetett függési viszonyokban álló infrastruktúrák a közvetett veszélyeztetéseken keresztül így természetesen sérülékenyebbek is. Napjainkban ezek között is kiemelt jelentőséggel bír a különböző infrastruktúrák egyre növekvő mértékű függősége a tágabb értelemben vett informatikai – az információs tevékenységeket támogató, köztük pld. a hagyományos távközlési – hálózatok, rendszerek, eszközök szolgáltatásaitól.

A **kritikus információs infrastruktúra** ennek megfelelően információs tevékenységeket támogató rendszerek, eszközök olyan összessége, amely önmagában kritikus infrastruktúra, vagy lényeges szerepet játszik más kritikus infrastruktúrák működésében. Az előbbieket a szakirodalomban funkcionális információs infrastruktúráknak is nevezik. Ezek azok az "információs közművek", amelyek a társadalom alapvető információs szolgáltatásigényeit elégítik ki. [4, 74.o.]

A **kritikus infrastruktúrák osztályozása (ágazatokba, szektorokba sorolása)** értelem szerűen magán viseli a kritikus infrastruktúrák meghatározásaiban fennálló szemléletmódbeli eltéréseket, különbözőségeket. Ezt Muha Lajos részletesebben elemzi PhD értekezésében [5]. Az értekezésben feldolgozott EU, NATO és nemzeti osztályozások számos átfedéssel és kisebb érdemi különbözőségekkel 8-17 közötti ágazatot és ezeken belül 29-37 alágazatot tartalmaznak, amelyek alapján a szerző a Magyar Köztársaság szempontjából miniszteriális tagozódásban 42 alágazatra tesz javaslatot.

A kritikus infrastruktúra szektorok (ágazatok) közé jelen publikációban a kritikus infrastruktúrávédelem nemzeti programjáról szóló kormányhatározatban [6] foglaltaknak megfelelően a következőket soroljuk: energiaellátás; közlekedés; vízellátás; élelmiszerellátás; egészségügy; pénzügy; ipar; jogrend, kormányzat; közbiztonság, védelem; és végül az infokommunikációs szolgáltatások. A továbbiakban szektoronként röviden, általánosságban értékeljük az adatbázisok helyét, szerepét.

Adatbázisok helye, szerepe kritikus infrastruktúrákban

Az adatbázisok **általános helye és szerepe** áttekintésének alapját elsőként az adott szektor főbb informatikai rendszereinek, informatika-alkalmazási szintjének, informatika-függőségének megítélése képezi (ennek során figyelmen kívül hagyásra kerülnek a nem szakterület-specifikus – pld. vezetési, gazdálkodási, stb. – informatikai rendszerek). Ezt követően kerül sor a főbb szakterületi adatbázisok áttekintésére és az alaprendeltetés szempontjából vett kritikus-ságuk előzetes értékelésére.

Az **energiaellátás** területén az informatika alkalmazása a kőolaj, földgáz és villamos-energia termelés, tárolás, elosztás és rendszerirányítás támogatására irányul. Ezen belül informatikai rendszerek, alkalmazások támogatják az egyes termelő egységek, erőművek tevékenységét, valamint a kőolaj-, földgáz és villamos-energia hálózat működtetését, az energia-elosztás rendszerirányítását. A szakterület jellemző, informatikai eszközökkel támogatott rendszerei az ún. felügyeleti és adatgyűjtő (SCADA¹) rendszerek közé tartoznak.

Mind az üzemi, erőművi informatikai rendszerek, mind a szállító, elosztó hálózatok rendszerirányító rendszereinek rendeltetése az irányított rendszerben zajló folyamatok, események valós idejű figyelemmel kísérése, illetve befolyásolása. E rendszerek – pld. MAVIR SPECTRUM [7; 8], MOL OTR IIM [9] – működése valós idejű helyzetismeret adatbázisokra épül, amelyek jellemzően két összetevőt, részadatbázist tartalmaznak. Az egyik az irányított rendszer, hálózat topológiáját (ritkábban változó jellemzőit) tárolja, a másik pedig az egyes összetevők, objektumok dinamikusan változó aktuális állapotát. E két adatbázis az eltérő követelmények miatt általában különböző adatbázis-kezelési megoldásokkal kerül megvalósításra.

Az energiaellátó rendszerek, hálózatok más kritikus infrastruktúra szektorokhoz hasonlóan lényegében működésképtelenek a támogató – mindenekelőtt a rendszerirányításban alkalmazott – informatikai rendszerek, alkalmazások nélkül. Országos szintű hatással elsősorban az országos hálózati rendszerirányító (SCADA) rendszerek adatbázisainak veszélyeztetései, illetve egyes, jelentős szerepet játszó energia-előállító szervezetek (pld. Paksi Atomerőmű) rendszerirányító adatbázisait érintő támadások járhatnak.

A **közlekedés** területén az informatika-alkalmazás (közlekedési informatika) szakterületi szempontból a következő részterületekre osztható: személyszállítási, áruszállítási és forgalomirányítási informatika. Ezen belül az egyes közlekedési alágazatok – közúti, vasúti, vízi, légi, városi – természetesen sajátosságokkal is rendelkezhetnek. A következőkben foglaltakat nagyrészt Szászi Gábor jegyzetére [10] alapozva tárgyaljuk.

A személyszállítás esetében informatikai rendszerek támogatják a tervezést, előkészítést (kapacitás és menetrend tervezés), az utazás előkészítését (menetrendi információszolgáltatás, helyfoglalás, menetjegy kiadás), valamint az utazást magát (utastájékoztató, fedélzeti tájékoztató). A fenti szolgáltatások számos különböző adatbázis alkalmazására épülnek. Ilyenek mindenekelőtt a következők: menetrendi, járat, tarifa, helyfoglalási és menetjegy adatbázisok.

Az áruszállítás informatikával támogatandó folyamatai közé a rakodás-kirakodás, az útvonal közlekedés-irányítás és az árurendezés tartozik. Az adatbázisok ezen a területen is jelentős szerepet játszanak, köztük például: szállítóeszköz, szállítási feladat, valamint közlekedési hálózat adatbázisok.

A forgalomirányítás informatikai támogatása a két előző területtel szemben nem közlekedési szervezetekhez, hanem több szereplő által használt közlekedési hálózatokhoz, hálózatrészekhez kapcsolódik (pld. városok, autópályák, stb.). E területen elsősorban a felügyelt körzet közlekedési hálózatát leíró adatbázis játszik jelentősebb szerepet.

Napjainkban a kritikus infrastrukturális közlekedési szolgáltatások a támogató informatikai rendszerek és adatbázisaik nélkül gyakorlatilag működésképtelenek, egyes részfolyamataik ugyan korlátozott mértékben, hagyományos támogatással is működtethetőek, azonban a rendszer egésze nem. Egyes adatbázisok megrongálása, vagy meghamisítása teljes közlekedési káoszhoz és tovagyrűző hatásokhoz vezet, sőt emberi életet, jelentős anyagi javakat veszélyeztet. Ezek közül országos szintű hatást elsősorban a MÁV és a Ferihegyi repülőtér üzemeltető szervezet egyes adatbázisainak támadása válthat ki, emellett regionális hatású lehet az egyes VOLÁN vállalatok adatbázisainak támadása.

¹ Supervisory Control and Data Acquisition.

A **vízellátás** területén az informatika-alkalmazás – a kritikus infrastruktúra védelem szempontjából – a megfelelő minőségű ivóvíz szolgáltatás és szennyvízelvezetés/tisztítás biztosításához, valamint az árvízvédelemhez kapcsolódik. A vízügyi informatikai rendszerek, más területekhez hasonlóan országos és területi/szervezeti rendszerekre csoportosíthatóak.

Az országos szintű vízügyi rendszerek közül a legjelentősebbek közé a Vízgazdálkodási, a Vízkárelhárítási Védekezési és a vízminőségi Kárelhárítási Információs Rendszerek tartoznak. Ezek működését számos, országos szintű adatbázis – köztük az Objektum és Törzsadatkezelő Rendszer és a Magyar Hidrológiai Adatbázis – támogatja, amelyek nagyjából vízügyi objektumokra vonatkozó leíró adatokat, valamint hidrológiai mérési, megfigyelési eredményeket tartalmaznak. [11]

A területi/szervezeti szintű vízügyi informatikai rendszerek közül a vízellátás és szennyvízelvezetés szempontjából a vízművek, az árvízvédekezés szempontjából pedig a regionális vízügyi igazgatóságok rendszerei érdemelnek figyelmet. A vízművek üzemirányító rendszerei a felügyeleti és adatgyűjtő rendszerek csoportjába tartoznak, helyzetismeret adatbázisaik más alkalmazási területekhez hasonlóan térinformatikai alapú, ritkán változó leíró adatokat és dinamikus változó mérési adatokat tartalmaznak. Az értékesítést támogató rendszerek adatbázisai a végrehajtott szolgáltatások adatait tárolják. [12] A vízügyi igazgatóságokon speciális informatikai rendszerek, adatbázisok gyakorlatilag nincsenek, a meglévő rendszerek, adatbázisok a már említett országos rendszerek részét képezik.

A vízügyi adatbázisok megrongálása, meghamisítása egyes esetekben jelentős – de alapvetően csak regionális, vagy helyi – problémákat okozhat a vízellátásban, esetleg az árvízvédekezésben. Országos szintű hatást kiváltó fenyegetés megvalósítására azonban jelenleg nem látszik lehetőség.

Az **élelmiszerellátás** kritikus infrastruktúra jellege az élelmiszer-ellátási lánc egészére – a termelésre, feldolgozásra és forgalmazásra – kiterjed. Ezen belül speciális részterület az egészséget veszélyeztető hatások kiküszöbölésére irányuló élelmiszer-biztonság. Az informatikai támogatás az általános alkalmazási területek mellett elsősorban az élelmiszerek nyomon követésére, szennyeződésének figyelésére, illetve az élelmiszer eredetű megbetegedések jelzésére szolgáló adatgyűjtő és értékelő rendszerek esetében játszik kiemelt szerepet. [13]

Az élelmiszer-biztonságot szolgáló nemzeti hálózat és adatbázisok szoros együttműködésben állnak európai és más nemzetközi rendszerekkel. A szakterület témánk szempontjából fontos, létező és tervezett adatbázisai közé a viszonylag állandó jellegű, leíró adatokat tartalmazó adatbázisok, valamint az előírt bejelentésekből, ellenőrzésekből, laboratóriumi vizsgálatokból származó adatokat tartalmazó adatbázisok tartoznak. Az előzőekre alapozva egy Európai Unió projekt keretében jelenleg tervezett egy egységes nemzeti élelmiszer-biztonsági adatbázis kialakítása. [14]

Az élelmiszer-biztonsági adatbázisok veszélyeztetettsége önmagában csak különleges esetekben járhat országos szintű hatással, azonban más biztonsági fenyegetésekhez hozzáadódva növelheti, erősítheti azok káros következményeit.

Az **egészségügy** területén az informatika-alkalmazás (egészségügyi informatika) több más mellett a következő részterületekre osztható: kórházi, ápolási, orvosi képző, közegészségügyi, fogorvosi, gyógyszerészeti, illetve egészségbiztosítási informatika. Az egészségügyben alkalmazott informatikai rendszerek alkalmazásuk hatókörét tekintve feloszthatóak intézményi (kórházi, háziorvosi, gyógyszerészeti, stb.), intézményközi és országos szintű rendszerekre. Az egészségügy informatikai támogatása folyamatosan fejlődik. Ez megnyilvánul mind az egészségügyi igazgatás, mind az egészségügyi ellátás, szolgáltatások területén.

Az egészségügyi intézményi informatikai rendszerek szakmai adatbázisai alapvetően az ellátásban részesülők intézményi kezelésével kapcsolatos információkat tartalmaznak. Ezek kö-

zé mindenekelőtt a diagnosztikai és terápiás információkat tároló, köztük a képalkotó diagnosztikai adatbázisok tartoznak.

A Magyarországon még csak tervezett intézményközi rendszerek az ellátottakra vonatkozó összes egészségügyi információ központi, vagy regionális tárolására épülnek. Ezek a személyi egészségügyi életút adatbázisok várhatóan jelentős mértékben javítják majd az egészségügyi ellátórendszer globális teljesítményét. [15]

Az országos szintű rendszerek adatbázisai közé elsősorban az olyan közhiteles nyilvántartások tartoznak, mint a különböző személyi, szervezeti nyilvántartások; gyógyszer, orvostechnikai eszköz és gyógyászati segédeszköz nyilvántartások; TAJ adatbázis; szakmai kódrendszerek (betegségek, orvosi eljárások, stb.), illetve finanszírozási, besorolási kategóriák. [16; 17; 18]

Az egészségügyi szolgáltatások ma már gyakorlatilag szintén működésképtelenek az informatikai támogatás nélkül. Az előzőekben említett adatbázisok elleni támadások elsősorban egészségügyi ellátási képességeket, kapacitásokat rombolnak, befolyásolnak és ezzel közvetve, vagy közvetlenül – az ellátás elmaradásával, vagy hibás kezeléssel – emberi életeket veszélyeztetnek. Ezek közül országos szintű hatással elsősorban egyes közhiteles nyilvántartások támadása járhat, regionális hatású pedig a súlyponti kórházak veszélyeztetése lehet.

A **pénzügyi** területen az informatika-alkalmazás két nagy területre csoportosítható: a pénzügyintézetek tevékenységének támogatására és a pénzügyintézetek közötti fizetési forgalom, elszámolások támogatására. Mind a pénzügyintézeti, mind az elszámolási tevékenység élenjáró területe az informatikai rendszerek, szolgáltatások alkalmazásának.

A pénzügyintézeti (ezen belül pld. a banki) tevékenység szinte egésze ma már informatikai folyamatokon keresztül valósul meg, amelynek alapját az alapvető pénzügyintézeti – pld. ügyfél-, számla-, valamint tranzakciós – adatbázisok képezik. Napjainkra már az ügyfelek oldalán is egyre jobban terjed az informatikai eszközök segítségével, az elektronikus banki szolgáltatások igénybevételével történő ügyintézés. [19]

A pénzügyintézetek közötti fizetési, elszámolási tevékenység hatékonyan és gyorsan csak informatikai rendszerek segítségével lehetséges. Ilyen rendszerek a világ számos országában működnek, Magyarországon ide sorolhatóak a GIRO, VIBER és KELER² rendszerek. Ma már ezen rendszerek is belső adatbázisokra épülnek, amelyek biztonságának megsértése a bankközi forgalom felborulását is eredményezheti. Egyes vizsgálatok ezt már akár egyetlen résztvevő rendszerének kiesése esetén is valószínűsítik. [20]

A fejlett államokban a pénzügyi rendszerek ma már működésképtelenek az informatikai támogatás és ezen belül az alapvető pénzügyi adatokat tartalmazó adatbázisok rendelkezésre állása, sértetlensége és hitelessége nélkül. Ezen adatbázisok megrongálása, vagy meghamisítása a pénzügyi folyamatok leállítását, vagy hibás megvalósulását vonja maga után és ezzel általában országos szintű káros hatás kiváltására is alkalmas.

Az **ipar** területén a kritikus infrastruktúrák közé a vegyi anyagok előállítás, tárolása és feldolgozása; a veszélyes anyagok, hulladékok kezelése, tárolása, szállítása; a nukleáris anyagok előállítás, tárolása, feldolgozása; valamint az oltóanyag és gyógyszergyártás során felhasznált infrastruktúrákat sorolják, mivel ezek sérülése, hibás működése a lakosságot veszélyeztető ipari balesetekhez vezethet. A veszélyes anyagok kezeléséhez kapcsolódó jelentősebb informatikai rendszerek, alkalmazások két nagy csoportba sorolhatóak: az elsőt a más területeken korábban már említett folyamatirányítási, rendszerfelügyeleti rendszerek képezik, míg a másodikba a veszélyes anyagokkal kapcsolatos nyilvántartási és tájékoztató rendszerek tartoznak.

² GIRO = bankközi fizetési forgalmat lebonyolító elszámolási rendszer; VIBER = Valós Idejű Bruttó Elszámolási Rendszer a nagy értékű átutalások teljesítésére; KELER = értékpapír elszámoló rendszer.

A nyilvántartási és tájékoztató rendszerek fenntartását az Európai Unió a SEVESO II. irányelvben határozta meg. Az ebben foglalt követelményeknek megfelelően került kialakításra a Seveso Üzemek Nyilvántartási Rendszere (SPIRS) [21], Súlyos Balesetek Jelentési Rendszere (MARS) [22], valamint a Veszélyes Anyagok Adatkezelő Rendszere (DSDMS)³. A két előbbi rendszer alapját egy-egy elosztott – egy központi és a tagállamok illetékes szervezeteinél működő helyi összetevőkből felépülő – adatbázis képezi, amelyek a veszélyes anyagokat kezelő főbb európai ipari létesítmények veszélyhelyzet-kezeléséhez szükséges, valamint a súlyos balesetekre vonatkozó alapvető információkat tartalmazzák. Ehhez kapcsolódóan az egyes országok, köztük Magyarország is működtet saját nemzeti nyilvántartásokat és az ezeket támogató informatikai rendszereket.⁴

A folyamatirányítási és rendszerfelügyeleti rendszerek adatbázisainak veszélyeztetése egyes vegyi és nukleáris létesítményekben, üzemekben (pld. Paksi Atomerőmű) közvetlenül országos hatású súlyos ipari balesetekhez vezethet. A nyilvántartási és tájékoztató rendszerek adatbázisainak sérülése ezzel szemben közvetett módon, az esetlegesen bekövetkező ipari balesetek elleni védekezés eredményességének, hatékonyságának csökkentésén keresztül jelent fenyegetést az állampolgárok életére, egészségére, valamint a szervezetek és állampolgárok vagyoni javaira.

A **jogrend és kormányzat** területén a kritikus infrastruktúra védelem szempontjából a kormányzati/közigazgatási létesítmények és eszközök működőképessége, valamint a közigazgatási szolgáltatások rendelkezésre állása játszik jelentős szerepet. A közigazgatási szolgáltatások informatikai rendszerekkel, eszközökkel támogatott megvalósítása, az úgynevezett e-kormányzat, vagy e-közigazgatás napjaink egyik legfontosabb célja, megvalósulóban lévő eredménye.

A közigazgatási szolgáltatások informatikai támogatása két jól elkülöníthető, de egyformán fontos területre bontható: a közszolgálati intézmények belső működésének támogatása (back office) és a lakosság, valamint a gazdálkodó szervezetek kapcsolattartása ezen intézményekkel (front office). Az elektronikus – vagyis informatikai rendszerekkel, eszközökkel támogatott – ügyintézés és az elektronikus ügykezelés alapvető rendeltetése a szolgáltatási igények kielégítése, illetve a közigazgatási folyamatok hatékonyságának növelése. [23]

Az informatikai támogatással működő közigazgatás alapvető feltétele a tevékenység során felhasznált, naprakészen tartott nyilvántartások, adatbázisok megléte, elérhetősége. Ezek között vannak alap-, vagy köznyilvántartások amelyek az adott területen (vagy az ország területén) élő személyek, szervezetek, események adatait közhiteles módon tárolják és vannak ágazati, vagy szakági rendszerek, amelyek az adott szakterület (tárca) funkcióihoz igazodnak, a szakterületi informatikai rendszerek szerves részét képezik. A közhiteles nyilvántartások, adatbázisok közé tartoznak többek között a néesség-, anyakönyvi, közműtulajdon-nyilvántartások, míg az ágazati csoportba a rendőrségi, bírósági, oktatási, adóügyi, vámügyi, társadalombiztosítási, földhivatali, stb. nyilvántartások tartoznak.

A fentiekben is említett adatbázisok napjainkban már kulcsfontosságú szerepet töltenek be a közigazgatásban. Sérülésük, meghamisításuk alapvető közigazgatási szolgáltatásokat hiúsít meg, vagy tesz megbízhatatlanná. Számos szolgáltatás hiánya a mindennapi és a gazdasági élet lényeges folyamatainak megvalósulását országos szinten akadályozza.

A **közbiztonság és védelem** területéhez a honvédelmi és rendvédelmi rendszerek, hálózatok, infrastruktúrák sorolhatóak. A védelmi szféra harmadik jelentős részterülete, a katasztrófavédelem kérdései alapvetően már tárgyalásra kerültek az iparhoz és a vízellátáshoz kapcsolo-

³ Seveso Plants Information Retrieval System, Major Accident Reporting System, Dangerous Substances Data Management System.

⁴ Ipari Katasztrófaelhárítási Információs Rendszer (IKIR).

lódó szektorokban. Ezen a területen nemzeti szempontból azon infrastruktúrák kritikusak, amelyek kiesése, működéscsökkenése közvetlenül van hatással a társadalom életére.

A honvédelem, a haderő esetében kritikus infrastruktúrákat megítélésünk szerint alapvetően a műveleti rendszerek képeznek, a mindennapi működéshez kapcsolódó igazgatási rendszerek károsodásai kevésbé jelentenek közvetlen veszélyt a társadalmi, gazdasági és mindennapi élet folyamataira. A műveleti rendszerek veszélyeztetése ezzel szemben a katonai erőt, katonai képességeket és ezzel az ország védelmi képességét fenyegeti. A műveleti rendszerek alapvető adatbázisai közé mindenekelőtt a helyzetismeret adatbázisok tartoznak, amelyeknek részét képezik a térbeli helyzetinformációk időben lassan változó részét tartalmazó térképészeti adatbázisok, a mobil objektumok helyzetét tartalmazó 'nyomvonal' adatbázisok, valamint a leíró helyzetinformációkat tartalmazó hagyományos adatbázisok. [24] A katonai informatikai rendszerek adatbázisainak támadásai elsősorban akkor tekinthetők kritikus infrastruktúra fenyegetésnek, amikor az adott erők az ország védelmében vesznek részt.

A rendvédelmi területen számos olyan adatbázis található, amelynek működőképessége és hitelessége a különböző – bűnügyi, közrendvédelmi, határrendészeti, közlekedésrendészeti – szakterületek tevékenységének alapvető feltétele. Ezen adatbázisok közé sorolhatóak például a különböző bűnügyi nyilvántartások (büntettesek, büntetőeljárás alatt állók, körözöttek, fogvatartottak, ujj és tenyérnyomatok, fényképek, stb.), a közlekedésrendészeti nyilvántartások (vezetői engedélyek, járművek tulajdonosai, stb.), valamint a határforgalom ellenőrzési és idegenrendészeti nyilvántartások.

Az **infokommunikációs szolgáltatások** a kritikus infrastruktúrák egyik legfontosabb területét képezik. Ide tartoznak a vezetékes és mobil távközlési hálózatok, a műholdas és a rádiós távközlés és navigáció, az Internet hálózat, a műsorszóró hálózatok, a postai szolgáltatások. A korábban már említett szektorokhoz is kapcsolódnak a kormányzati (és védelmi) zártcélú hálózatok, valamint az automatikai és ellenőrző rendszerek.

A távközlési hálózatok esetében témánk szempontjából elsősorban a működés során felhasznált adatbázisok érdekesek. A mobil hálózatok működése alapvetően az előfizetői adatbázisokra épül, amelyek sérülése lehetetlenné teszi a szolgáltatást. Napjainkban már a vezetékes telefonközpontok is számos működéstámogató adatbázist használnak. A helymeghatározó, illetve műsorszóró hálózatokban, valamint a postai szolgáltatások esetében viszont az adatbázisok nem játszanak jelentős szerepet.

Az Internet hálózatokban működési szempontból elsősorban az útvonalválasztó adatbázisok (routing táblák) és a tartománynév (DNS) adatbázisok játszanak kritikus szerepet. Amennyiben tágabban értelmezzük, akkor számos internetes szolgáltatás (elektronikus levelezés, valós idejű társalgás, online játékok, stb.) elsősorban a felhasználókra vonatkozó információkat tartalmazó adatbázisait is ide sorolhatjuk.

Egyes infokommunikációs szolgáltatások esetében tehát az alapvető, többnyire sajátos technológiájú működési adatbázisok jelentős szerepet játszanak, sérülésük, meghamisításuk a szolgáltatások jellegéből következően országos méretű hatással jár.

Összegzés, következtetések

A kritikus infrastruktúra szektorok gyakorlatilag mindegyikére – mint a társadalmi tevékenység minden területére – elmondható, hogy rendszereik, folyamataik, szolgáltatásaik egyre fokozódó mértékben támaszkodnak informatikai rendszerek, eszközök támogatására. Számos területen ez már most olyan szintet ért el, hogy az informatikai szolgáltatások nélkül az alapfolyamatok teljesen, vagy nagyrészt működésképtelenné, a szolgáltatások elérhetetlenné, vagy jelentős mértékben csökkentett színvonalúvá válnak.

A növekvő informatika-függőségből következik, hogy a kritikus infrastruktúra szektorok gyakorlatilag mindegyikében találhatóak olyan (számítógépes) adatbázisok, amelyek szerepe jelentős, sértetlensége, hitelessége az adott alkalmazási terület alapvető működési feltételei közé tartozik. Jelen publikációban ezek – mint már korábban is jeleztük – csak egy átfogó áttekintésre alapozottan kerültek meghatározásra. Ez így elegendő bizonyos előzetes következtetések levonására, azonban a részletes vizsgálatot a jövőben minden egyes, vagy az adatbázisok alkalmazása szempontjából kiemelt szakterületen külön-külön el kell végezni.

Az előzőekben szereplő szakterületenkénti áttekintések, értékelések alapján tehát összességében megállapítható, hogy a kritikus infrastruktúrákban vannak olyan adatbázisok, amelyek biztonsága az adott kritikus infrastruktúra biztonságának alapvető összetevője. Ezen adatbázisok megnevezésére – legalábbis a kritikus infrastruktúra védelem vonatkozásában – célszerűnek látszik bevezetni a kritikus adatbázisok kifejezést. Az ebbe a csoportba tartozó adatbázisok meghatározásához először az érintett infrastruktúra kritikus jellegét, majd ezen belül az adott adatbázis működéskritikus (mission critical) jellegét kell meghatározni.

A publikáció előző részében foglaltak alapján megállapítható az is, hogy a kritikus infrastruktúrákban előforduló adatbázisok a következő nagyobb csoportokba sorolhatóak: a közhiteles nyilvántartások; a folyamatirányítási, rendszerirányítási, illetve a felügyeleti és adatgyűjtő (SCADA) rendszerek jellemzően helyzetismeret-adatbázisai; valamint egyes hagyományos relációs, esetleg objektum-orientált (pld. egészségügyi, pénzügyi/banki) adatbázisok. A felsorolt adatbázisok jelentős sajátosságokkal (típusuk, megvalósításuk, méretük, elérhetőségük, stb.) is rendelkeznek, amelyek a kritikus infrastruktúrávédelem szempontjából típusonként külön-külön önálló vizsgálatot indokolnak. Mindez azonban már további kutatások, publikációk tárgyát képezhetik.

Felhasznált irodalom

- [1] KOVÁCS Magda: *Mikroszámítógépek alkalmazása értelmező szótár II. Értelmező szótár 1. A-F.* – LSI Oktatóközpont Alapítvány, Budapest, 1991.
- [2] JODÁL Endre: *Számítástechnikai alaplexikon I. Általános fogalmak.* – Cédrus Kiadó, Budapest, 1991.
- [3] MUNK Sándor: A kritikus információs infrastruktúrák védelme információs támadások ellen. – *Hadtudomány*, 2008/1-2. (95-106.o.)
- [4] HAIG Zsolt-VÁRHEGYI István: *Hadviselés az információs hadszíntéren.* – Zrínyi Kiadó, Budapest, 2005.
- [5] MUHA Lajos: *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. Doktori (PhD) értekezés.* – Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2007.
- [6] 2080/2008. (VI.30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.
- [7] KASZÁS Árpád: A MAVIR Rt. informatikai stratégiája. – *A Magyar Villamos Művek Közleményei*, 2001 (XXXVIII.)/3. (21-27.o.)
- [8] KASZÁS Árpád: Az MVM-MAVIR-ban az ÜRIK keretében létesített számítógéprendszer kialakítása. A SPECTRUM funkciók összefoglalása. – *Elektrotechnika*, 2002 (95.)/különszám (6-16.o.)
- [9] *MOL Rt., KFÜ: OTR-IIM projektek (ismertetés).* – X-Prompt Automatizálási Szakértői Kft., Budapest, 2006.

[http://www.x-prompt.hu/Portal.php?Page=PROJ/OTR2M_2008.12.12.]

- [10] SZÁSZI Gábor: *Közlekedési informatika*. – Bolyai János Katonai Műszaki Főiskola, Budapest, 1999.
- [11] *A vízügyi informatika fejlődése, szerepe és kapcsolódásai a többi környezeti informatikai rendszerhez*. – EKOSPEKTRUM Kft., Budapest, 2004.
- [12] TOLNAI Béla (szerk.): *A térinformatikai szerepe a vízi közműszolgáltatásban (Fogalmak, feladatok, eszközök, elvárások, szabványok)*. – Víz- és Csatornaművek Országos Szakmai Szövetsége, Budapest, 2003.
[http://www.tova-partner.hu/letoltesek/a_terinformatika_szerepe.pdf
2008.12.12.]
- [13] NAGY Rudolf-VINCZE Árpád: Az élelmiszer-biztonság a környezetbiztonság szemszögéből. – *Hadmérnök*, 2007 (II.)/4. (38-45.o.)
- [14] AMBRUS Árpád-VANYUR Rozália: Az élelmiszer-biztonsági intézményrendszer megerősítése az EU támogatásával. – *Élelmiszer-biztonság*, 2008 (VI.)/2. (22-27.o.)
- [15] JÁVOR András-SURJÁN György-TÓTH Annamária: Személyi Elektronikus Egészségügyi Életút Archívum. – *Informatika és Menedzsment az Egészségügyben*, 2003 (II.)/3. (30-36.o.)
- [16] SINKÓ Eszter: Közhiteles nyilvántartások az egészségügyben. I. rész. – *Informatika és Menedzsment az Egészségügyben*, 2005 (IV.)/3. (43-45.o.)
- [17] SINKÓ Eszter: Közhiteles nyilvántartások az egészségügyben. II. rész. – *Informatika és Menedzsment az Egészségügyben*, 2005 (IV.)/4. (44-48.o.)
- [18] SINKÓ Eszter: Közhiteles nyilvántartások az egészségügyben. III. rész. – *Informatika és Menedzsment az Egészségügyben*, 2005 (IV.)/5. (38-43.o.)
- [19] BURIÁN Gábor: Az Internet banking kockázatai. – *Hitelintézeti Szemle*, 2005 (IV.)/2. (36-56.o.)
- [20] LUBLÓY Ágnes-TANAI Eszter: A működési kockázat és a hazai nagy összegű fizetési rendszer (VIBER). – *Hitelintézeti Szemle*, 2007 (VI.)/4. (324-357.o.)
- [21] *SPIRS 2.0, Seveso Plants Information Retrieval System (SPIRS), an Electronic Documentation and Analysis System for Industrial Establishments Data. User's Manual*. – European Commission, 2001.
- [22] *MARS 4.0, Major Accident Reporting System (MARS), an Electronic Documentation and Analysis System for Industrial Accidents Data. User's Manual*. – European Commission, 2001.
- [23] *eKormányzat 2005, e-Kormányzat stratégia és programterv*. – Miniszterelnöki Hivatal, Elektronikus Kormányzat Központ, 2004.
- [24] MUNK Sándor: Helyzetismeret-bázisok a katonai vezetésben, helyzetinformációk gyűjtése és feldolgozása. – In. HORVÁTH István-KISS Jenő (szerk.): *Válogatás a Honvédelmi Minisztérium 2001. évi kutatási eredményeit összegző tanulmányokból, pályázatokból*. HM Oktatási és Tudományszervező Főosztály, Budapest, 2001. (143-156.o.)