ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM
HADTUDOMÁNYI KAR
Hadtudományi Doktori Iskola

# DOKTORI (PhD) ÉRTEKEZÉS

**Dr. Beinschróth József**

# Informatikai rendszerekkel támogatott folyamatok működésfolytonossági kérdései a védelmi szférában

**Témavezető:**
**Dr. Munk Sándor**
**egyetemi tanár**

**2007.**

# Tartalomjegyzék

# Bevezetés

*„Az információs forradalom miközben széles lehetőségeket teremtett a modern társadalom számára (gyorsaság, hálózatépítés, hozzáférhetőség), másrészt viszont rendkívül sebezhetővé tette az informatikai rendszerekre építő társadalom zavartalan működését."*

*Részlet a Magyar Köztársaság Nemzeti Biztonsági Stratégiájából*

Általánosan ismert és elfogadott, hogy az utóbbi évtizedekben végbement hatalmas informatikai fejlődés következtében a különböző, polgári és védelmi szférabeli szervezetek működése az általuk alkalmazott informatikai rendszerektől erősen függővé vált. Működési folyamataik fenntarthatóságát, folyamatos működését döntően befolyásolja informatikai rendszereik rendelkezésre állása és megfelelő működése. Bár előfordulhatnak olyan működési folyamatok, amelyeknek nincs informatikai támogatottsága, egyre inkább általánossá válik, hogy a működési folyamatok különféle informatikai rendszerek működésére épülnek, a számítógépek, hálózatok, kommunikációs rendszerek egyre inkább küldetéskritikus (mission-critical) rendszereknek minősülnek. [1] Jelen doktori értekezés az informatikai rendszerekkel támogatott működési folyamatok vizsgálatára szorítkozik.

Bár az informatikai rendszerek kritikus szerepet játszanak a szervezetek működésében, nyilvánvaló, hogy a szervezetek elsődleges célja nem az informatikai rendszereik biztonságos üzemeltetése, hanem a működési folyamataik (elsősorban kritikus folyamataik) megszakadás nélküli, folyamatos működtetése, azaz az informatikai rendszerek megfelelő színvonalú üzemeltetése nem cél, hanem csupán egy szükséges feltétel. Ennek megfelelően a technológia működése önmagában még nem feltétlenül garantálja az IT rendszerekkel támogatott folyamatok működésfolytonosságát, azaz a működésfolytonosságnak léteznek további, szervezeti, szabályozási, humán stb. feltételei is. Ennél fogva nyilvánvaló, hogy a működésfolytonosság nem tárgyalható kizárólag technológiai kérdésként, komplex megközelítésre van szükség, amely egyaránt figyelembe veszi a technológiai, a szervezési, a szabályozási és egyéb jellegű veszélyforrásokat (fenyegetéseket) is, és ezekből kiindulva határozza meg a belőlük származó kockázatokat, valamint a velük szemben alkalmazható védekezési módszereket.

Mivel gyakorlatilag nem létezhet olyan védelmi módszer, amely bármiféle esemény (pl. nagy kiterjedésű, súlyos természeti katasztrófa, terrorcselekmények stb.) ellenében is garantáltan biztosítja a működési folyamatok megszakadás-mentességét, a működési

folyamatok folyamatos működésének problémái közé kell sorolnunk a katasztrófa helyzetekre való felkészülést is. Jelen értekezés az informatikai rendszerekkel támogatott folyamatokra fókuszál, ennek megfelelően ebben a kérdéskörben az informatikai katasztrófa helyzetekre helyezi a hangsúlyt, azaz azokra az esetekre koncentrál, amelyekben az informatikai rendszerek egyes elemeinek kiesése jelenik meg katasztrófaként, akadályozva ezzel a folyamatok kiesésmentes működését.

A különböző szervezetek alapvető funkcionalitásait biztosító kritikus működési folyamatainak kiesése nem, vagy csak meghatározott időre engedhető meg. A működési folyamatok kiesésmentes működése, illetve elfogadható, korlátozott időtartamnál rövidebb ideig tartó kiesése a támogató informatikai rendszerek rendelkezésre állásának fokozásán túlmenően megfelelő szabályozásokkal érhető el. Nyilvánvaló azonban, hogy az alkalmazott rendszerek megbízható működésének fokozása és a megfelelő szabályozás együttesen sem képesek garantálni a folyamatok kiesésmentes működését. Emiatt a működésfolytonosság biztosítása érdekében az informatikai rendszerek rendelkezésre állásának fokozásán, és a megfelelően kialakított szabályozásokon túlmenően szükség van arra is, hogy a védekezési módszerek között szerepeljenek előre kialakított, katasztrófa helyzetben alkalmazható iránymutatások, tervek is.

Az eddigiekből következik, hogy az informatikai rendszerekkel támogatott folyamatok működésfolytonossági kérdéseinek vizsgálata napjainkban nyilvánvalóan rendkívül időszerű tématerület. Ugyanezt bizonyítja, hogy a közelmúltban megjelentek, elérhetővé váltak olyan szoftver eszközök, amelyek a működésfolytonosság biztosítását támogatják (például a Precovery[1], ÜFO[2] stb.). A tématerület jelentősége a jövőben várhatóan még inkább fokozódni fog, hiszen a különböző szervezetek működési folyamatai egyre inkább függővé válnak az informatikai infrastruktúrától.

Mindezek természetesen nemcsak a polgári, hanem a védelmi szférára[3] is érvényesek. *„Az elkövetkezendő évtizedekben sem létszámából, sem haditechnikai felszereltségéből, sem a fejlesztésekhez rendelkezésre álló pénzeszközök volumenéből, sem a hadsereg fejlesztési lehetőségeit formáló politikai pártok szemléletmódjából adódóan nem valószínű, hogy a magyar haderő a világ „legfélelmetesebb" hadseregévé válhat. Arra viszont reális esély van, hogy az*

[1]A Sungard Availability Services Limited terméke
[2]Üzletmenet FOlytonossság tervező szoftver - a Humansoft Kft. terméke
[3]Mivel a védelmi szféra fogalom nagyon széles területet fed le, folyamatai pedig igen szerteágazók és sokfélék, az értekezés elsősorban a vezetési folyamatokra fókuszálva készült.

*elkövetkezendő évtizedekben a Magyar Honvédség a világ katonai élvonalába kerüljön a harmadik generációs hadviselés szempontjából! Az informatikai és kommunikációs szakmai fejlesztések eredményeként olyan tudás alapú haderő alakítható ki, amely nem csupán tiszteletet ébreszt a NATO-partnerekben, de követendő mintaként is szolgálhat a hadviselés és a biztonságpolitika jövőorientált fejlesztői számára.*" [2]

A katonai szféra kulcsfontosságú folyamata a katonai vezetés. „*A katonai vezetés olyan folyamat, melyben a katonai erők irányítását, koordinálását és ellenőrzését egy személyre bízták."* [3] A vezetési funkciók a gyakorlatban folyamatjelleggel jutnak érvényre és informatikai rendszerekkel egyre inkább támogatottak. [4]

A működési folyamatok és az informatikai infrastruktúrák egyre szorosabb kapcsolódása ugyanakkor korábban nem jelentkező problémákat állított előtérbe. „*Az információs társadalom nagyon fejlett, nagyon hatékony társadalom, ugyanakkor meglehetősen sebezhető társadalmi és gazdasági rendszer. Sebezhetőségének objektív alapját az adja, hogy ennek a társadalomnak működése szorosan kapcsolódik a globális, regionális és lokális (nemzeti) információs környezethez. Ennek következtében igen erősen függ az információs környezet fejlett, ám erősen korlátozható, vagy sebezhető integrált információs infrastruktúráitól, pl. a távközlési hálózatoktól és a nagyteljesítményű számítógép-hálózati rendszerektől.*" [5]

A működésfolytonosság kérdésköre elsősorban az informatikai biztonság területéből fejlődött ki és mára gyakorlatilag önálló szakterületnek számít. Bár a két szakterület számos ponton kapcsolódik egymáshoz, sőt bizonyos kérdésekben átfedések is léteznek közöttük, jelen értekezés nem foglalkozik az informatikai biztonság témaköreivel, csupán annyiban, amennyiben azok érintik a működésfolytonosságot.

A vizsgált tématerület kérdéseinek kutatása, a működésfolytonosság fenntartására, kiesések esetén a folyamatok vissza-, illetve helyreállítására irányuló tevékenységek vizsgálata már számos eredményre vezetett. Igen nagy mennyiségű (gyakran egymásnak ellentmondó megállapításokat tartalmazó) irodalom érinti az értekezés által vizsgált tématerületet, ugyanakkor nem lelhető fel közöttük olyan publikáció, amely általánosan elfogadottan rögzítené a működésfolytonosság alapkoncepcióját, megfelelően rendszerezné jellemzőit. Nem tisztázott, hogy a működésfolytonosság vizsgálata mennyiben végezhető el kizárólag a védelmi szférára vonatkoztatva, illetve, hogy mennyiben szükséges tárgyalásakor a polgári szféra egyes területeit, esetleg egészét figyelembe venni. Az ismert publikációk között nem szerepel olyan, amely a

működésfolytonosság kifejezetten a védelmi szférára jellemző kérdéseivel, illetve annak vizsgálatával foglalkozik, hogy mennyiben igényel eltérő megközelítést a védelmi és a polgári szféra ezen kérdéskörben.

A különböző szervezetek megfelelő szintű üzemeltetői, döntéshozói, parancsnokai részéről jogos elvárás, hogy a kompetencia területükhöz tartozó, informatikai rendszerekkel támogatott folyamatok megfelelően szabályozott, kiesésmentes működtetéséhez szabványok, illetve ajánlások formájában segítséget kapjanak. Sem a hazai, sem a nemzetközi ajánlások között nem szerepel azonban olyan, amely kifejezetten a működésfolytonosság biztosítására vonatkozóan tartalmazna normatívákat. Mivel a különböző szervezetek működése nagymértékben támaszkodik az általuk alkalmazott informatikai rendszerekre, ezek megbízható működésére, a folyamatok működésfolytonosságának biztosítása jelentős mértékben támaszkodhat az informatikai rendszerek megbízható működését meghatározó informatikai biztonsági és üzemeltetési ajánlásokra. Az informatikai rendszerek biztonságára és üzemeltetésére vonatkozóan számos különböző szintű ajánlás, szabályozás létezik mind a polgári, mind a védelmi szférában. Ezen ajánlások és szabályozások azonban többnyire technológiai szemléletűek, egymással nem, vagy csak többé-kevésbé konzisztensek, a működésfolytonosság tekintetében nem is mindegyikük tekinthető relevánsnak.

Az egyes szervezetek működésfolytonosságának biztosítása konkrét védelmi intézkedések alkalmazásával valósítható meg. Ezek megkövetelik a releváns veszélyforrások számbavételét, bekövetkezési valószínűségük meghatározását, valamint feltételezhető hatásuk felmérését és rájuk vonatkozó kockázatelemzés végrehajtását. Nem ismert azonban olyan kutatási eredmény, amely kifejezetten ezen kategóriák tárgyalására fókuszálna.

Az előzőekhez hasonlóan a döntéshozók, parancsnokok részéről ugyancsak jogos elvárásként jelenik meg, hogy folyamatosan nyomon követhessék a működésfolytonosság megvalósult, aktuális szintjét, illetve arra vonatkozóan elvárásokat fogalmazhassak meg, esetlegesen összevessék a megvalósult szinteket más, hasonló szervezetek jellemzőivel. Mindezek egy megfelelően kidolgozott minősítési rendszer alapján képzelhetők el, azonban a szakterülethez tartozó irodalomban nem lelhető fel olyan mérési, minősítési eljárás, amely alapján mindezek megtehetők.

A rögzítettekből kiindulva jelen doktori értelezés célkitűzései a működésfolytonosság

kérdéseinek kutatására irányulnak. A kutatási célok a következők:

1. A működésfolytonosság alapkoncepciójának kidolgozása, szemléletének megfogalmazása, jellemzőinek rendszerbe foglalása olyan módon, hogy a rendszerezett jellemzők felhasználásával a működésfolytonosság törvényszerűségei tárgyalhatók legyenek.
2. Az informatikai biztonságra és az informatikai rendszerek üzemeltetésére vonatkozó ajánlások olyan megközelítésű elemzése, melynek eredményeképpen kiválaszthatók közülük azok, amelyek a védelmi szférában működésfolytonosság tekintetében is relevánsnak tekinthetők.
3. A működésfolytonosságot veszélyeztető veszélyforrások elemzése, a működésfolytonosság biztosítását alkotó összetevők meghatározása.
4. A működésfolytonosságra vonatkozó minősítési rendszer koncepciójának kidolgozása.

Az értekezés szerkezete a kitűzött célokat követi, négy részre tagolódik, az egyes fejezetek rendre egy-egy kutatási célhoz kapcsolódnak.

Az első fejezet a működésfolytonosság koncepciójáról, értelmezésről, jelentéséről szól, egységesíti a releváns irodalomban fellelhető kiinduló gondolatokat, alapelveket, továbbá annak vizsgálatát tartalmazza, hogy a védelmi és a polgári szféra mennyiben jelent eltérő kihívásokat a működésfolytonosság biztosításának szempontjából, illetve a normál, mindennapi rutinszerű tevékenységekhez képest a védelmi szférára különösen jellemző művelet-orientált tevékenység rendszer esetén. A fejezet annak tárgyalására is kitér, hogy a működésfolytonosság mennyiben fed át más szakterületeket, és mennyiben kapcsolódik hozzájuk. Rendszerezi a működésfolytonosság jellemzőit úgy, hogy a kialakított rendszer alapján a működésfolytonosság törvényszerűségei viszonylag egyszerűen tárgyalhatók legyenek.

A második fejezet a széles körben ismert és elterjedten használt, az informatikai biztonsághoz, valamint az informatikai rendszerek üzemeltetéséhez leginkább kapcsolódó ajánlások vizsgálatáról és összehasonlításáról szól, arra fókuszálva, hogy mi az alapvető céljuk, továbbá, hogy mennyiben tekinthetők relevánsnak működésfolytonossági kérdésekben, mennyiben alkalmazottak, illetve alkalmazhatók a

védelmi szférában.[4] A vizsgálat – elsősorban a terjedelmi korlátok miatt – nem terjed ki a komplex információbiztonság valamennyi összetevőjére, az elemzés elsősorban a megjelölt ajánlásokra koncentrál.

A harmadik fejezet a működésfolytonosság biztosítását, annak fő összetevőit tárgyalja, így érinti a helyzetfeltárás, a veszélyforrások, a kockázatelemzés, a védelmi feladatok kijelölése, a működésfolytonosságra vonatkozó felkészítés, a tesztelés, az aktualizálás valamint a katasztrófa helyzet kezelés témaköreit, továbbá azt vizsgálja, hogy a működésfolytonosság biztosítása mennyiben okoz hasonló problémákat a védelmi és a polgári szférában, a normál mindennapi, illetve művelet-orientált működés esetén. Az egyes fenyegetések ellen alkalmazható védelmi intézkedések (például konkrét technológiai megoldások) részletes tárgyalását azonban (elsősorban terjedelmi okokból) nem tartalmazza.

A negyedik fejezet annak vizsgálatát tartalmazza, hogy egy a működésfolytonosság aktuális állapotára vonatkozó mutatószám rendszernek milyen követelményeket kell kielégítenie. Ebből kiindulva javaslatot tesz olyan minősítési rendszer kialakítására, amely egy-egy szervezeten belül alkalmas a működésfolytonosság aktuális szintjének jellemzésére, továbbá lehetővé teszi a különböző szervezetek, alakulatok működésfolytonossági szintjeinek összevetését, a működésfolytonosság időbeli változásainak követését, illetve objektív célkitűzések megfogalmazását.

A dolgozat korszerű informatikai eszközök alkalmazásával jött létre, a szövegszerkesztés, az ábrák és a táblázatok az MS Office programcsomag felhasználásával (Word, Excel, Power Point) készültek. A nem idézett szövegrészek, a forrásmegjelölés nélküli ábrák és táblázatok valamennyien a jelölt saját eredményei.

Az értekezés több éves kutatómunka eredményeinek felhasználásával jött létre, a jelölt a témához kapcsolódóan számos publikációt készített, melyek különböző tudományos folyóiratokban kerültek publikálásra. A kidolgozás kapcsán sor került a működésfolytonosság szakterületén és a kapcsolódó különböző szakterületeken fellehető releváns szakirodalom (technológiai, jogi, szabályozási valamint vezetési-szervezési témájú könyvek, dokumentumok, jegyzetek, tanulmányok, szabványok) feldolgozására, elemzésére. A kutatómunka egyaránt kiterjedt a nyomtatott és az

[4]Több NATO dokumentum is rögzíti, hogy a civil szférabeli szabványokat fel kell használni ahol csak lehetséges. Például a NATO Logistics Handbook, 1997.: (Chapter 7: NATO Principles and Policies for Logistics) szerint: „…design of military equipments and systems should take account, wherever possible, of civil components and standards". – …a katonai berendezések és rendszerek tervezésekor figyelembe kell venni a civil komponenseket és szabványokat, ahol csak lehetséges.

interneten elérhető elektronikus irodalom feldolgozására. A kutatás során egyaránt alkalmazásra kerültek az általános és a különös kutatási módszerek, az analízis, a szintézis, az indukció és a dedukció módszerei.

Az értekezés tartalmába beépültek azok a gyakorlati tapasztalatok, amelyeket az értekezés szerzője különböző szervezeteknél lefolytatott számos informatikai, informatikai biztonsági, illetve informatikai működésfolytonossági jellegű projekt során mint nemzetközi minősítésekkel rendelkező informatikai szakember (CISA[5], illetve ITIL[6] minősítés) szerzett. Az értekezés tartalmába ugyancsak beépültek azok a több éves oktatás során oktatóként szerzett tapasztalatok is, melyeket a jelölt a Budapesti Corvinus Egyetem postgraduális MBA képzésén az Informatikai biztonság – üzletmenet folytonosság című, illetve a Budapesti Műszaki Főiskola Kandó Kálmán Villamosmérnöki Főiskolai Karán az Adat és információvédelem, valamint az Informatikai rendszerek üzemeltetése és biztonsága című előadássorozataiban szerzett.

A kutatási téma interdiszciplináris jellegéből következően a kutatómunka során fontos szerepet kaptak a hasonló és kapcsolódó kutatási és tudományos területen tevékenykedő szakemberekkel történő konzultációk, megbeszélések, tapasztalatok és eredmények megosztása.

A jelölt ezúton mond köszönetet azoknak a következőkben felsorolt szakembereknek, kollégáknak, akik véleményükkel, tanácsukkal, konzultációs segítségükkel támogatták a dolgozat elkészítését.

- Bartók Sándor Péter, CISA;
- Dr. Báthy Sándor, nyá. ezredes, egyetemi tanár;
- Dr. Cziva Oszkár, tűzoltó ezredes;
- Dr. Drótos György, egyetemi docens;
- Dr. Fodor Imre, nyá. mérnök. ezredes, főiskolai tanár;
- Dr. Gorza Jenő, nyá. mérnök. ezreds, c. egyetemi docens, informatikai igazgató;
- Dr. Haig Zsolt, mérnök alezredes, egyetemi docens;
- Dr. Kende György, nyá. mérnök. ezredes, egyetemi tanár;
- Dr. Kovács Gábor, határőr alezredes, egyetemi docens;

[5]Certified Information System Auditor – információbiztonsági ellenőr minősítés
[6]Foundation Certificate in IT Service Management – IT szolgáltatás menedzsment minősítés

- Dr. Kovács László, mérnök őrnagy, főiskolai docens;
- Dr. Lukács György, főiskolai docens, intézetigazgató;
- Dr. Maros Dóra, főiskolai docens;
- Dr. Munk Sándor, mérnök ezredes, egyetemi tanár;
- Dr. Négyesi Imre, mérnök őrnagy, egyetemi docens
- Dr. Rajnai Zoltán, mérnök alezredes, egyetemi docens;
- Dr. Turcsányi Károly, nyá. mérnök ezredes; egyetemi tanár;
- Dr. Ványa László, mérnök alezredes, egyetemi docens;
- Dr. Vass Sándor, alezredes, egyetemi docens;
- Vasvári György, CISA, c. egyetemi docens;
- Dr. Viharos Zsolt János, tudományos főmunkatárs.

# 1 A működésfolytonosság biztosításának védelmi szférabeli koncepciója

*„Nem félek a számítógépektől. A hiányuktól félek."*

*Isaac Asimov*

## 1.1 A működésfolytonosság, mint az információs társadalom egyik jelentős kihívása

A XXI. század társadalma, az információs társadalom fejlett, hatékony társadalmi formáció, amelyet számos korábban nem ismert és realizált érték jellemez. Azzal, hogy az információs társadalom döntő mértékben támaszkodik az informatikai technológiára és az általa támogatott működési folyamatokra, felépülése során megjelentek és megjelennek újfajta kihívások, olyan negatív összetevők is, amelyek működését bizonytalanná tehetik, esetleg teljes működésképtelenségét okozhatják. [6]

Ezen összetevők közül egyik legnagyobb jelentőséggel a működésfolytonosság problémája rendelkezik. Ennek az az oka, hogy az egyes szervezetek[7] kritikus funkcionalitásait biztosító működési folyamatok nagymértékben támaszkodnak az informatikai infrastruktúrára, amely jelenlegi fejlettségi szintjén nem képes arra, hogy szolgáltatásait garantáltan kiesésmentesen nyújtsa. Az informatikai infrastruktúra, az egyes informatikai rendszerek bármilyen okból történő meghibásodása, kiesése az egyes szervezetek működési folyamatainak kiesését okozhatja, amely azt eredményezheti, hogy az illető szervezet nem lesz képes kritikus funkcionalitásait biztosítani. Bizonyos szervezetek esetén ez a probléma messze túlmutathat a szervezet határain, olyan regionális, nemzeti, sőt globális méretű kiesések következhetnek be, amelyeknek hatásai beláthatatlanok. (Az Egyesült Államok kormányzata szövetségi állami és helyi folytonossági és visszaállítási szinteket – continuity and restoration - különböztet meg. [7]) Annál is inkább így van ez, mert az információs társadalom kialakulása során az informatikai infrastruktúra a nemzeti méreteket meghaladóvá, globálissá, világméretűvé vált, emiatt bizonyos informatikai rendszerek kiesése további rendszerek kiesését is okozhatja. Mindezek alapján kijelenthető, hogy a működésfolytonosság kérdésköre akár nemzetbiztonsági szintű problémaként is megjelenhet. Itt szükséges megemlíteni, hogy mindezekhez szorosan kapcsolódik a kormányzati működés folytonosságának [8] problémája (Continuitiy of Government - COG) is.

[7] A továbbiakban a szervezet fogalmába a meghatározott feladatok végrehajtására létrehozott szervezet-integrációkat, katonai szövetségeket is beleértjük.

A leírtak összhangban vannak a Magyar Köztársaság Nemzeti Biztonsági Stratégiájával, amely a következőket mondja ki: „*A hosszú távú lemaradás hátrányos következményeinek elkerülése érdekében Magyarország számára kiemelt feladat a felzárkózás a fejlett világ információs és telekommunikációs színvonalához. Az információs forradalom vívmányainak mind szélesebb körű megismertetése, az oktatás színvonalának emelése kulcsfontosságú érdek, ami közvetve pozitív hatással van a gazdaságra, a társadalom életére és az ország érdekérvényesítő képességére. Az informatikai infrastruktúra technikai és szellemi feltételeinek biztosítása mellett ügyelni kell e rendszerek védelmére és a megfelelő tartalékok képzésére is. Az informatika számtalan lehetőséget teremtett a társadalom számára, de fokozta annak veszélyeztetettségét.*” [9] Az idézett gondolatban a működésfolytonosság fogalma ugyan nevesítetten nem jelenik meg, de a rendszerek védelmére, veszélyeztetettségére, valamint a tartalékok szükségességére való egyértelmű utalással nyilvánvalóan a kiesések elkerülésének fontosságára hivatkozik. Bár az anyag a tartalékok képzésén túlmenően nem említ további olyan módszereket, amelyek a kiesések ellenében alkalmazhatók, nyilvánvaló, hogy léteznek alternatív lehetőségek is, továbbá, hogy a kiesések kizárólag tartalékok képzésével nem, vagy csak extrém nagy költségekkel kerülhetők el.

A működésfolytonosság kérdése azonban nem korlátozódik az informatikai rendszerek kiesésmentes üzemeltetésére. A szervezetek nem egyszerűen informatikai rendszereik, hanem működési folyamataik megszakadás nélküli működtetésében érdekeltek, aminek csak az egyik feltétele az informatikai rendszereik rendelkezésre állása. Emiatt a működésfolytonosságnak léteznek további feltételei is. A működésfolytonosság komplex megközelítést igényel, amely egyaránt figyelembe veszi a technológiai, a szervezési, a szabályozási és egyéb feltételeket is. Például a 2006. augusztus 20-i budapesti tűzijátékhoz kapcsolódó katasztrófa bekövetkezését megelőzően és annak idején minden érintett szervezet (Országos Meteorológiai Szolgálat, Országos Katasztrófavédelmi Főigazgatóság, rendezvényszervező stb.) informatikai rendszere rendelkezésre állt, és biztosította az elvárt szolgáltatásokat, a katasztrófa megelőzéséhez és kezeléséhez kapcsolódó folyamatok mégsem mentek megfelelőképpen végbe.

## 1.2 A működésfolytonosság meghatározása

A működésfolytonosság problémája a hidegháború időszakában a kormányzati

szférában jelent meg legkorábban: nyilvánvaló, hogy maga a kormányzás egy esetleges nukleáris háború esetén sem eshetett volna ki, emiatt erre vonatkozóan különböző tervek születtek. [8] A magyar nyelvben a működésfolytonosság mint fogalom csak a legutóbbi időkben jelent meg, ezzel a címszóval nem találkozhatunk a lexikonokban. Hozzá nagyon közelálló, elterjedten használt fogalom az üzletmenet folytonosság, illetve az üzletmenet folytonosság tervezés[8] fogalma. Az Informatikai biztonság kézikönyve [10] az üzletmenet folytonosság tervezés fogalmát a következőképpen határozza meg: „*Az informatikai rendszer rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetők legyenek.*" Az informatikai biztonságot tárgyaló MSZ ISO IEC 17799:2006 szabvány [11] korábbi, 2002-es változatától [12] eltérően már nem az üzletmenet folyamatosságának menedzselésére, hanem a működés folytonosságának irányítására hivatkozik. Nem rendszerre, hanem folyamatra, tevékenységre koncentrál. A szabvány „*A működés folytonosságának irányítása*" című fejezetében célkitűzésként a következőt jelöli meg: *„… védjék meg a kritikus működési folyamatokat az információs rendszerek nagy hibáinak vagy az üzemzavaroknak a hatásától…*".

Az üzletmenet folytonosság fogalom nyilvánvalóan az üzleti szféra szóhasználatát követi. Az üzleti szférán túlmenően azonban számos olyan szféra létezik (például a védelmi, a közszolgálati stb.), amelyek működési folyamatai nem üzleti jellegű folyamatok, emiatt meglehetősen különös lenne rájuk ezt a fogalmat közvetlenül alkalmazni.[9]

A fogalom a magyar nyelvbe az üzleti szférán keresztül, nyilvánvalóan az angol „*business continuity"* kissé pontatlan fordításával került be. Kétségtelen, hogy az angol business szót gyakran fordítják üzletként, azonban a szótárak szerint léteznek ettől eltérő jelentései is. Így például találkozhatunk a foglalkozás, szakma, ügy dolog, munka, kötelesség [13] értelmezésével is.

Ezzel összhangban van a business szó angol nyelvű általános értelmezése [14]: „*one's usual occupation*", amely kifejezés rendszeres elfoglaltságot, foglalkozást, hivatást jelent. Mindezek alapján megállapítható, hogy a működésfolytonosság az eredeti angol „*business continuity*" üzletmenet folytonosságnál pontosabb fordításának tekinthető, így

[8]Az angol nyelvű szakirodalomban erre szokásosan a BCP – Business Continuity Planning (Üzletmenet folytonosság tervezés), a BPC – Business Process Continuity (Üzleti folyamatok folytonossága), illetve a BCM – Business Continuity Management (Üzletmenet folytonosság menedzselése) elnevezéseket használják.

[9]Az ISACA Hungarian Chapter 2006. 09.14-i összejövetelén Bíró László (CISA, CISM) „A BCP buktatói" című előadásában a BCP rövidítésnek magyarul az üzemmenet-folytonosság kifejezést feleltette meg.

az elterjedten használt üzletmenet folytonosság helyett minden esetben használható, ezen túlmenően használata az üzleti szférától eltérő szférákhoz való jobb illeszkedést is eredményezi. Érdemes azonban megjegyezni, hogy a kérdéses fogalomra az angol nyelvben sem teljesen általános a business continuity kifejezés használata, ennek szinonimájaként számos helyen megtalálható a Continuity of Operation (COOP) [15] kifejezés is, amely teljesen egyértelműen a működés folytonosságaként fordítható le. Így például többek között az Egyesült Államok hadseregére vonatkozóan kifejezetten a működésfolytonosságra koncentráló szabályozás [15], illetve az Egyesült Államok Védelmi Minisztériumának (Department Of Defense) védelmi folytonossági programja (Defense Continuity Program) [16] is ezt a szóhasználatot követi.

A működésfolytonosság kifejezés a legutóbbi időkben megjelent a magyar szakirodalomban is. Használja például az Állami Számvevőszék az informatikai rendszerek kontrolljainak ellenőrzéséhez kidolgozott módszertanában [17] és ennek megfelelően jelentéseiben, továbbá ez a kifejezés jelenik meg az Európai Unió Hivatalos Lapjában megjelenő információbiztonsághoz kapcsolódó pályázati felhívásban [18]. Az MTA SZTAKI az „*Internet védelmi rendszer struktúrájának kidolgozása*” elnevezésű projekt keretében készített tanulmányában az ISO/IEC 17799 szabványban szereplő „*business continuity*” kifejezést az előzőekkel összhangban nem üzletmenet folytonosságként, hanem működésfolytonosságként idézi. [19]

Az üzletmenet folytonosság, illetve a működésfolytonosság kérdéskörét az előző időszakban gyakran azonosították a katasztrófa helyzet kezelésének kérdésével[10], ez azonban mára már túlhaladott megközelítés, a katasztrófa helyzet kezelés a működésfolytonosság biztosításának csupán az egyik összetevője.

## 1.3 A védelmi és a polgári szféra tevékenységrendszerei

### 1.3.1 Tevékenységrendszer változatok

Azon túlmenően, hogy az információs társadalomban a polgári szféra szinte minden területe egyre inkább támaszkodik az informatikai infrastruktúrára, az informatikai rendszerek felhasználása hasonlóképpen jellemző a szűkebb és a tágabb értelemben vett védelmi szférában[11] is. Így a működésfolytonosság kérdése, amely alapvetően a folyamatokhoz, tevékenységrendszerekhez kapcsolódik, relevánsnak tekinthető a védelmi és a polgári szférában egyaránt. A két szféra azonban – bár napjainkban

[10] Az angol nyelvű szakirodalomban erre szokásosan a contingency planning illetve DRP – Disaster Recovery Planning elnevezéseket használják.
[11] Lásd az 1.3.2 A polgári és a védelmi szféra kapcsolata c. fejezetet.

kapcsolatukat erőteljes konvergencia jellemzi [20] – működésfolytonossági szempontból némiképpen eltérő sajátosságokkal rendelkezik. A védelmi szférában például nyilvánvalóan léteznek olyan sajátos, a működésfolytonosságot veszélyeztető veszélyforrások, amelyek a polgári szférában nincsenek jelen.

A működésfolytonosság kérdéséhez kapcsolódóan a védelmi és a polgári szférabeli eltérő sajátosságokon túlmenően létezik egy másik dimenzió, amely mentén ugyancsak különböző jellemzők tapasztalhatók. Mindkét szférára igaz ugyanis, hogy szervezeteik eltérő tevékenységrendszereket hajthatnak végre. A működésfolytonosság vizsgálata szempontjából különbséget kell tennünk a rutinszerű, mindennapi működés, illetve a művelet-orientált működés mint tevékenységrendszer között. A kétféle tevékenységrendszert ugyanis a vizsgált szempontból eltérő tulajdonságok jellemzik. Művelet-orientált működés esetén például megjelennek olyan, a működésfolytonosságot veszélyeztető veszélyforrások, amelyek a mindennapi, rutinszerű működésre egyáltalán nem jellemzőek. A kétfajta tevékenységrendszer – bár nem azonos súllyal jelennek meg bennük - mindkét szférára jellemző: mind a rutinszerű, mind a művelet-orientált működés egyaránt megjelenik a védelmi és a polgári szférában is.

A továbbiakban áttekintjük a védelmi és a polgári szféra művelet-orientált és rutinjellegű tevékenységrendszereit, megfogalmazzuk a működésfolytonossági szempontból relevánsnak tekinthető sajátosságaikat.

### 1.3.2 A védelmi és a polgári szféra kapcsolata

A védelmi és a polgári szféra nem teljes mértékben elkülönülő, diszjunkt objektumok, közöttük nem húzható egyértelmű határvonal. Elkülönülésükre vonatkozóan többféle megközelítés létezik, ezeknek megfelelően a védelmi szférát különféleképpen értelmezhetjük. A legszűkebb értelemben vett védelmi szféra alatt a kifejezetten a fegyveres küzdelem, illetve válságreagáló műveletek végrehajtása céljából létrehozott katonai szférát értjük. A tágabb értelemben vett védelmi szférába tartoznak a rendvédelmi, határvédelmi és katasztrófavédelmi erők [21] is, amelyek tipikusan hatósági, igazgatási, rendészeti, illetve humanitárius feladatokat látnak el.

Bár alapvetően a polgári szférához tartoznak, az előzőekben felsorolt feladatokon túlmenően a kritikus infrastruktúrák védelme (Critical Infrastructure Protection – CIP) is egyre inkább megjelenik a védelmi szféra feladatai között, mivel a kritikus infrastruktúrák kiesése, sérülése, folytonos működésének megszakadása esetén alapvető állami feladatok sérülhetnek és emiatt nemzetbiztonsági problémák következhetnek be. Az

ezredfordulón szükséges dátumváltási probléma informatikai kockázatának megjelenése jó példát szolgáltatott erre. A kormányok, a különböző szolgáltatók, pénzintézetek stb. nem voltak képesek előre meghatározni, hogy a különböző, egymással kapcsolatban álló informatikai rendszereket alkalmazó kritikus infrastruktúrák közül melyek esetében kell kiesésekkel számolni az évforduló időpontjában, továbbá, hogy a kieséseknek lesznek-e nemzetbiztonsági vonzatai.

A kritikus infrastruktúra védelem európai programjáról szóló zöld könyv [22] 11 ágazat, mint például az energiaellátás, információs és kommunikációs technológiák vagy a közlekedési ágazatok 37 termékét, szolgáltatását sorolja be a kritikus infrastruktúrák közé.

A leginkább tipikusnak tekinthető kritikus infrastruktúrák [5] a következők:

- szállító infrastruktúra;
- vízellátó rendszerek;
- távközlési rendszerek;
- banki és pénzügyi infrastruktúra;
- energiatermelő szállító és tároló infrastruktúra;
- kormányzati és önkormányzati szervek;
- vészhelyzeti és katasztrófakezelési infrastruktúra.

„*Napjainkban az országok túlélő képességét már nem a stratégiai infrastruktúrák, és objektumok védelmével lehet biztosítani. A 94/1998. (XII.29.) OGY határozat alapján a Magyar Köztársaság nemzeti biztonsági stratégiájáról szóló 2144/2002. (V.6.) Korm. határozat, majd ezt követően a 2073/2004. (IV. 15.) Korm. határozat is ennek szellemében határozza meg a stratégiát. A határozat 1. c) pontjában előírtak teljesítéseként készült a hazai „Informatikai és információvédelmi nemzeti biztonsági stratégia”, amelynek első számú prioritásai között szerepel a kritikus információs infrastruktúrák védelme.”* [23]

A védelmi és a polgári szféra nemcsak a kritikus infrastruktúravédelem problémája miatt kapcsolódik össze. Napjainkban ezen szférák erőteljes konvergenciája figyelhető meg. Ennek a folyamatnak lényeges összetevője, hogy egyre inkább szükségessé válik, és előtérbe kerül a két szféra közötti mind szorosabb együttműködés (CIMIC – Civil-Military Co-operation, polgári–katonai együttműködés) [20]. Gyakori, hogy védelmi szférabeli szervezetek számára szolgáltatásokat nyújtanak, beszállítóként jelennek meg polgári szférabeli szervezetek, mind a normál mindennapi, mind pedig művelet-orientált

működés esetén. További fontos összetevő, hogy - kifejezetten gazdasági megfontolásokból - informatikai rendszerként jelenleg mind a polgári, mind a védelmi szférában jellemzően COTS [24] (Commercial Off The Shelf - a kereskedelmi forgalomból beszerezhető, "*polcról levehető*" és azonnal üzembe helyezhető) rendszereket használnak. Ugyancsak ezt a konvergencia folyamatot igazolja, hogy a tapasztalatok szerint az aszimmetrikus hadviselés előtérbe kerülésének következményeként, a támadások számottevő része egyre inkább polgári célpontokra irányul és céljuk nem is azok teljes megsemmisítésére, hanem működésfolytonosságuk akadályozása. [20]

Mindezeknek megfelelően a működésfolytonosság tárgyalásakor a kritikus infrastruktúrák folyamatos működésének biztosításához fűződő kérdéseket kiemelkedő jelentőségűnek kell tekintenünk, így nem szorítkozhatunk a védelmi szféra szűkebb vagy tágabb értelemben vett értelmezésére, a polgári szférába tartozó kritikus infrastruktúrák működésfolytonossági kérdéseit is figyelembe kell vennünk.

Mindezek miatt a védelmi szféra működésfolytonossági kérdéseinek tárgyalása során a védelmi szféra tágabb értelmezését kell alapul vennünk, azaz feladatai közé soroljuk a fegyveres küzdelem, illetve válságreagáló műveletek végrehajtásán kívül a rendvédelmi, a határvédelmi, a katasztrófavédelmi tevékenységeket is. Ezeken túlmenően, kiemelkedő védelmi stratégiai jelentőségük miatt, az alapvetően a polgári szférába tartozó kritikus infrastruktúrák védelméhez köthető tevékenységeket is ide tartozónak tekintjük. Az eddigiekből az is következik hogy a polgári és védelmi szféra előzőekben ismertetett egyre szorosabb kapcsolódása, egymástól való függősége nem teszi lehetővé, hogy a védelmi szféra működésfolytonossági kérdéseit kizárólag önmagukban vizsgáljuk, tárgyalásukkor vele együtt a polgári szféra működésfolytonossági jellemzőit is érintenünk kell.

### 1.3.3 Művelet-orientált és rutinjellegű tevékenységrendszerek a védelmi szférában

A művelet fogalma általános értelmezés szerint "*egymással összefüggő, tervszerűen végrehajtott cselekmények sorozata, vagy ennek egy szakasza, mozzanata*" [26]. Jellemző példái közé a különböző értelmező szótárak, lexikonok korábban többek között a katonai műveleteket, mentési műveleteket sorolták. Napjainkban a védelmi szférában a műveletek számos fajtájával találkozhatunk: válságreagáló, béke- (békefenntartó, békeépítő, békekikényszerítő), rendfenntartó, veszélyhelyzet-kezelési,

katasztrófavédelmi, vagy humanitárius segítségnyújtó műveletek. [25]

A felsorolt példákból és az adott szakterületeken általánosan elfogadott értelmezésükből már előzetesen megállapítható, hogy a műveletek mint tevékenységrendszerek alapvető jellemzői közé többek között a következők tartoznak:

- a műveletek meghatározott, konkrét célok elérésére irányulnak;
- időben behatároltak (a művelet megkezdésétől a kitűzött cél eléréséig tartanak, amelyet természetesen megelőzhet egy felkészülési/tervezési szakasz és követhet egy befejező/lezáró szakasz);
- a művelet részét képező tevékenységek egységes elgondolás szerint, egységes irányítás alatt, összehangoltan kerülnek végrehajtásra;
- végrehajtásuk rendjét műveleti tervek szabályozzák;
- a műveletet végrehajtó erőket általában a konkrét feladattól függően hozzák létre, állítják össze.

A művelet-jellegű tevékenységrendszerek a mindennapi, ismétlődő, rutinjellegű tevékenységrendszerektől több, a működésfolytonosságot is befolyásoló szempontból különböznek. Ez utóbbiak alapvető jellemzői a következők:

- általános, a szervezeti alaprendeltetéshez kapcsolódó célok megvalósítására, vagy ezek feltételeinek biztosítására irányulnak;
- időben folyamatosan, ismétlődően kerülnek végrehajtásra;
- végrehajtásuk rendjét szervezeti és működési szabályzatok szabályozzák;
- az adott feladat folyamatos végrehajtására létrehozott szervezeti munkakörök, szervezeti egységek valósítják meg.

Minden szervezet működésében vannak rutinjellegű és művelet-jellegű tevékenységek. A különböző rendeltetésű szervezetek működésében azonban ezek eltérő arányban játszanak szerepet. A polgári szférabeli szervezetek jelentős része (igazgatási, adminisztratív, termelő, szolgáltató, oktatási, tudományos, stb.) alapvetően, de nem kizárólagosan, rutinjellegű tevékenységet végez, míg a katonai szervezetek alaprendeltetése művelet-orientált jellegű, de a védelmi szféra más szervezeteinek életében is szerepet játszanak a műveletek. Ugyanakkor az alapvetően műveletek végrehajtására létrehozott fegyveres erőkben is folyik a haderő fejlesztése, fenntartása

és felkészítése, amely tevékenységek mindennapi, rutinjellegű tulajdonságokkal rendelkeznek.

### 1.3.4 Katonai műveletek és jellemzőik

A katonai alkalmazásban a művelet kifejezés számos alapvető fogalom részét képezi. A katonai művelet átfogó fogalma magában foglalja a fegyveres küzdelemre épülő háborús katonai műveleteket és a válságreagáló műveleteket (nem háborús katonai műveleteket), illetve az összetettségük alapján megkülönböztetett háborúkat, hadjáratokat, hadászati műveleteket, hadműveleteket, ütközeteket és harcokat. [25] A válságreagáló műveletek közé tartoznak a háborús küszöb alatti konfliktusok kezelése, a veszélyhelyzet kezelés és humanitárius segítségnyújtás, valamint a honi területen kívüli béketámogató műveletek. [27]

Az érvényben lévő NATO fogalomjegyzék szerint a művelet "*egy katonai tevékenység, egy hadászati, harcászati, kiszolgáló, kiképzési, vagy igazgatási feladat végrehajtása; a harc megvívásának folyamata, beleértve az ütközet, vagy hadjárat céljai eléréséhez szükséges felvonulást, utánpótlást, támadást, védelmet és manővereket*" [28]. Az alapvető magyar doktrínális dokumentum szerint a hadművelet "*egy meghatározott területen és időkeretek között a haderőnemek által önállóan végrehajtott vagy együttes cél, feladat, hely és idő szerint összehangolt, egyidejű vagy egymást követő ütközeteinek, harcainak összessége a hadműveleti vezetés és irányítás megvalósulása mellett, a hadműveleti támogatással és a harccal kapcsolatos tevékenységekkel együtt*" [27].

Katonai művelet végrehajtható egy adott állam, egy szövetség (például a NATO), a művelet végrehajtására létrehozott koalíció, vagy egy nemzetközi biztonságpolitikai szervezet (ENSZ, EBESZ, stb.) vezetésével. Napjaink katonai műveleteit egyre inkább a holisztikus megközelítés, körük, jellegük kibővülése, összetettségük, más – információs, gazdasági, társadalmi, jogi, diplomáciai stb. – tevékenységekkel fennálló kapcsolatrendszerük megnövekedése, illetve a műveleteket végrehajtó erők összetételének megváltozása, az együttműködési kör kibővülése, a multilaterális jelleg uralkodóvá válása jellemzi. [29] A katonai műveletek időtartama a ritkábban előforduló néhány hetes humanitárius műveletektől, az általában több hónapos, vagy néhány éves béketámogató műveletekig terjed.

A nemzeti haderők által végrehajtott műveletek kivételével korunk katonai műveletei jellemzően többnemzetiségű (szövetségi, sőt leggyakrabban az adott feladatra

létrehozott, a résztvevő nemzetek eseti felajánlásaira épülő koalíciós) keretekben kerülnek végrehajtásra. Emellett a műveleteket végrehajtó csoportosításokban egyre gyakrabban jelennek meg más – nemzetközi, kormányzati, nem-kormányzati és civil – szervezetek is [29]. A fentiekből következik, hogy a műveletek végrehajtására kijelölt erők egymással korábban szervezeti kapcsolatban nem álló, sőt esetenként a művelet végrehajtása során is változó összetevőkből épülnek fel.

A katonai műveletek sajátossága, hogy végrehajtásukra az állandó elhelyezéstől eltérő, általában terepi és veszélyeztetett környezetben kerül sor. A szembenálló, vagy a műveletekben érintett további felek általi veszélyeztetettség háborús műveletekben teljes körű, de bizonyos mértékig a válságreagáló műveletekben is fennáll (többek között éppen ezért van szükség katonai erő alkalmazására). Emellett a természeti környezet veszélyeztető hatásai is erőteljesebben érvényesülnek, mint állandó elhelyezési körülmények között.

A biztonságpolitikai helyzetelemzések megállapításai szerint a Magyar Honvédség esetében a honi területen végrehajtott védelmi műveletek valószínűsége rendkívül alacsony. A NATO csatlakozás óta a Magyar Köztársaság biztonságát már nemcsak közvetlen környezete, hanem a távolabbi térségek eseményei is befolyásolják. Mindez a Magyar Honvédség számára mindenekelőtt a honi területen kívüli válságreagáló, béketámogató és humanitárius műveletekben történő szerepvállalást tesz szükségessé.

A Magyar Honvédség a különböző műveletekben jellemzően század és zászlóalj méretű harci támogató, logisztikai támogató, vagy egészségügyi kontingensekkel vesz részt. A távoli műveleti területen történő alkalmazás és a működtetési erőforrás-korlátok következménye, hogy a művelet végrehajtásában résztvevő erők támogatása (híradó és informatikai, logisztikai működési feltételeinek biztosítása) is alapvetően távolról, a honi területről történik.

A katonai műveletek további sajátossága, hogy alapvető tevékenységeik jelentős része (például a támadó és védelmi tevékenységek) a felkészülési időszakban valós körülmények között nem, vagy nem teljes körűen gyakorolhatók. Ez azzal a következménnyel jár, hogy a katonai műveletekben alkalmazásra kerülő új, vagy továbbfejlesztett technikai eszközök, rendszerek sem tesztelhetőek és alkalmazásuk sem gyakorolható teljes mértékben valósághű körülmények között.

### 1.3.5 Műveletek jellemzői a tágabb értelemben vett védelmi szférában

A tágabb értelemben vett védelmi szférában (ezen belül kiemelten a rendvédelemben, határvédelemben és katasztrófavédelemben) is jelentős szerepet játszanak a konkrét célok elérésére irányuló, a célok eléréséig tartó műveletek. Ezen jellegzetes művelet-típusok közé a veszélyhelyzet-kezelési (katasztrófavédelmi, humanitárius), a rendőri és a határőr műveletek tartoznak. [25]

A katonai alkalmazással szemben viszont a felsorolt alkalmazási területeken a művelet-orientált tevékenységek mellett hasonlóan jelentős szerepet töltenek be a rutinjellegű, például igazgatási, hatósági, rendészeti feladatok és tevékenységek is. A veszélyhelyzet-kezelési[12], szűkebb értelemben katasztrófavédelmi[13] műveletek célja a társadalom rendeltetésszerű működését, az emberi életeket, anyagi javakat, vagy a természeti környezetet jelentős mértékben veszélyeztető körülmények megszüntetése, a káros következmények csökkentése és felszámolása, valamint az eredeti működőképesség, vagy helyzet lehetőségek szerinti helyreállítása.

A veszélyhelyzetek közé tartoznak többek között a természeti katasztrófák (földrengések, tengerrengések, vulkánkitörések, földcsuszamlások, viharok, árvizek, aszályok, természetben bekövetkező tüzek), az ipari, közlekedési (nukleáris, vegyi, biológiai) katasztrófák, valamint az erőszakos tömegmegmozdulások. Korunk új sajátossága, hogy a különböző veszélyhelyzeteket előidézhetik terrorista támadások is.

Veszélyhelyzet-kezelési műveletekre olyan esetekben kerül sor, amikor a káros következmények megelőzése, elhárítása és felszámolása meghaladja az e célra rendelt szervezetek előírt együttműködési rendben történő védekezési lehetőségeit. Így ezeket a műveleteket már nemzeti szinten is a feladat végrehajtására ideiglenesen létrehozott, különböző kormányzati és nem-kormányzati szervezetektől igénybevett erők egységes irányítás alatt hajtják végre. Különösen igaz ez a több nemzetet érintő, vagy a nemzeti képességeket meghaladó veszélyhelyzetek kezelésére, ahol a katasztrófavédelmi, vagy humanitárius műveletek végrehajtásában ENSZ, vagy nemzeti irányítás alatt különböző nemzetek felajánlott erői vesznek részt.

A veszélyhelyzet-kezelési műveleteket végrehajtó csoportosítások nemzeti és nemzet-közi műveletek esetében is a védekezésben, elhárításban résztvevő helyi erőkből és a megerősítő, illetve speciális képességekkel rendelkező központi, vagy más helyről

[12] Az angol nyelvű szakirodalomban erre szokásosan az emergency response kifejezést használják.
[13] Az angol nyelvű szakirodalomban erre szokásosan az disaster relief kifejezést használják.

érkező erőkből állnak. Így a veszélyhelyzetek különböző helyszíneken történő bekövetkezése miatt a műveletek végrehajtásában érintett erők általában műveletenként eltérő összetételben, eltérő partnerekkel együttműködve tevékenykednek.

A veszélyhelyzet-kezelési műveletek számos sajátosságukban a katonai műveletekhez hasonlítanak (sok esetben egyenesen katonai műveletek formájában kerülnek végrehajtásra). Ezek közé tartozik, hogy a művelet végrehajtására a résztvevő erők állandó elhelyezési körleteitől távol (sok esetben jelentős távolságra, más országban, sőt földrészen), terepi körülmények között és a veszélyhelyzet következményei által fenyegetett környezetben kerül sor. A távoli, veszélyes körzetben történő alkalmazás így általában a rendelkezésre álló technikai (köztük informatikai) rendszerek, eszközök korlátozását is jelenti. A műveletek időtartama általában több naptól néhány hétig, pár hónapig terjed.

A speciálisan rendőri műveletek közé tartoznak többek között az élet- és vagyonbiztonságot tömegesen veszélyeztető erőszakos cselekmények megakadályozására; súlyos bűncselekményt elkövető, szökésben lévő fegyveres személyek elfogására; terrorcselekmények megakadályozására, túszok kiszabadítására; eltűnt személyek felkutatására; tömegrendezvények rendjének biztosítására; védett személyek, veszélyes szállítmányok őrzésére, védelmére irányuló tevékenységek. Ezeket a feladatokat a rendőrség általában csapaterő alkalmazásával oldja meg.

A rendőri műveletek mérete és időtartama a katonai és veszélyhelyzet-kezelési műveleteknél általában kisebb, illetve rövidebb, jellemzően egy, vagy néhány nap. Végrehajtásukra általában az érintett helyi, illetve szükség esetén speciális képességű központi erőkkel kerül sor. Nagyobb méretű, hosszabb időtartamú műveletek esetében a végrehajtásba általában más helyi erők, vagy más szervezetek (például honvédség, határőrség) erői is bevonásra kerülnek. Az alkalmazásra a rendőri műveletek esetében is épületen kívüli, egyes esetekben terepi körülmények között kerül sor.

A speciálisan határőr műveletek közé elsősorban a veszélyeztetett határszakaszon az országot ért fegyveres támadás, vagy külső fegyveres csoportok váratlan betörésének elhárítása; illetve az államhatár közelében bekövetkezett veszélyhelyzet esetén a szomszéd állam területéről menekülők kezelése (átléptetése, összegyűjtése, elsődleges elhelyezése, stb.) tartozik. A határőr műveleteket végrehajtó erők általában egy adott területi szerv (határőr igazgatóság) alárendeltségébe tartoznak, a migrációt kezelő

műveletek időtartama néhány hét, esetleg pár hónap lehet. A műveletek tipikusan veszélyhelyzetben, terepi körülmények között kerülnek végrehajtásra.

### 1.3.6 Művelet-orientált és rutinjellegű tevékenységek a polgári szférában, illetve a kritikus infrastruktúra védelem területén

A meghatározott cél elérésére irányuló, egységes elgondolás alapján végrehajtott tevékenységrendszer, azaz a művelet-orientált tevékenység fogalma nem csak a védelmi szférában létezik, a polgári szférában, ennek megfelelően a kritikus infrastruktúra védelem területén ezt a tartalmat a projekt kifejezés jelöli. [25]

A projekt egy konkrét, egyedi feladatra létrehozott, költségkerettel, kezdő és befejezési időponttal rendelkező üzleti eseménylánc. Olyan komplex (jelentős méretű) feladatot, összehangolt tevékenység együttest jelent, amelynek jól definiált célja van, egyedi, jelentős méretű idő, költség és erőforrás keretekkel rendelkezik [30]. A projekt "*olyan tevékenység, amely egy szervezet számára egyszeri és komplex feladatot jelent, amelynek teljesítési időtartama (kezdete és befejezése), valamint teljesítésének költségei (erőforrások) meghatározottak és egy definiált cél (eredmény) elérésére irányul*" [31].

Napjainkban a projekt a polgári szférában, illetve a kritikus infrastruktúra védelem területén egyaránt megjelenik a költségvetési és a gazdálkodó szervezetek tevékenységében, azonban szerepe a különböző gazdálkodó szervezetek működésében nagyobb jelentőségű. Ennek oka az, hogy a tapasztalatok szerint a rutinszerű, csak a tevékenység (termék) minőségének javítására, illetve a hatékonyság növelésére koncentráló szervezet hosszabb távon elveszíti versenyképességét. A versenyképesség megőrzésének, a versenyelőny realizálásának feltételét kizárólag a folyamatos innováció jelentheti (a tudásra és tudományra épülő, magas gyártástechnikai színvonalat képviselő információs ipari termelési korszakban az előállított termékek és kifejlesztett szolgáltatások 80%-a szellemi, és csak 20%-a anyagi és energia összetevő [5]), amely állandó változást, ennél fogva projektszerű működést igényel.

A projekt akkor tekinthető sikeresnek, ha az elvárt eredmény a tervezett határidőn belül, a számára rendelkezésre bocsátott erőforrás kereteket nem átlépve jön létre. A komplexitás, a jelentős méret miatt a sikertelen projekt mindenképpen számottevő (nemcsak közvetlen anyagi, hanem például presztízs) veszteséget okoz. Gyakran előfordul, hogy a projekt lezárása után nem triviális feladat annak eldöntése, hogy az sikeres vagy sikertelen volt. Előfordulhat ugyanis, hogy a projekt ugyan látszólag elérte

deklarált célját, ugyanakkor az elért cél mégsem biztosítja az elvárt eredményeket. Például a projekt célja lehet egy informatikai alkalmazás bevezetése, amely sikeresen meg is valósul, azonban később kiderül, hogy az illető alkalmazás a gazdálkodó szervezet működése szempontjából fölöslegesnek bizonyult. Az egyedi (egyszeri) jelleg jelentős mértékben megnöveli a projekt sikertelenségének kockázatát, hiszen az egyszeri végrehajtás miatt a begyakorolt módszerek, a bevált gyakorlat pontos, készségszintű alkalmazása ez esetben szóba sem kerülhet.

A projektek tipikusan jellegük szerint csoportosíthatók. A projekt jellege szerint beruházási, kutatási-fejlesztési, illetve oktatási projektekről beszélhetünk. Az egyes típusok között nem feltétlenül húzható éles választóvonal, a gyakorlatban gyakran előfordul, hogy egyetlen projekt egyszerre többféle jelleggel is rendelkezik. Például egy informatikai rendszer bevezetésekor az üzemeltetésére vonatkozó felkészítés is fontos összetevőként jelenik meg.

A projekt végrehajtását az erre a célra létrehozott projektszervezet végzi. A projekt-szervezet egy hierarchikus szervezet, az egyes pozíciókhoz jól definiált felelősségek, hatáskörök és erőforrások tartoznak. Előfordulhat, hogy a projektszervezetben megvalósuló hierarchia eltér a normál, rutinjellegű, mindennapi tevékenységrendszerekben alkalmazottól, az alá- és fölérendeltségi viszonyok akár meg is fordulhatnak. A projektszervezetben, a projektvezetésen és az operatív tevékenységeket végző munkacsoportokon (teameken), illetve a projektadminisztráción kívül gyakran megjelennek a változáskezelést, a kockázatkezelést és a minőségbiztosítást végző szerepek is.

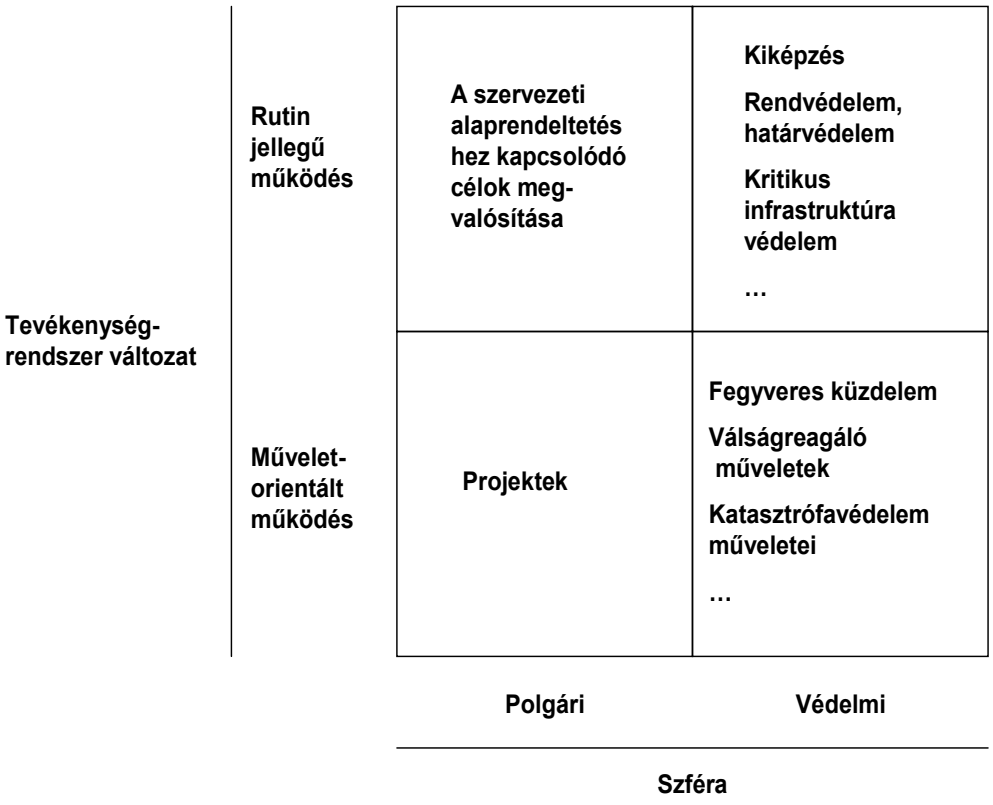
Gyakori, hogy egy projektben több szervezet működik együtt. Például egy informatikai alkalmazás bevezetésekor a megrendelő, a szállító és a független minőségbiztosító tipikusan különböző szervezethez tartozik. Ez esetben gyakori, hogy a különböző szervezetek által kijelölt projektvezetők tevékenységét egy erre a célra létrehozott projekt irányító bizottság fogja össze.

A projektek lebonyolítását különböző projektmenedzsment módszertanok segítik, ezek széles körben ismertek és elterjedtek. A projektmenedzsment módszertanok egy-egy meghatározott projekt lebonyolítására adnak iránymutatást, azonban gyakran előfordul, hogy egy-egy területen, egy-egy szervezetnél azonos időben több projekt is folyamatban van. Ebben az esetben felmerülhetnek olyan problémák is (tipikusan az erőforrások korlátozottsága miatt), amelyek kifejezetten az egyidejű projektek miatt

következnek be. Például előfordulhat, hogy egy rendelkezésre álló beléptető rendszert vagy rakodási területet a több projekt a maximális kapacitását meghaladó mértékben kívánja igénybe venni annak ellenére, hogy egyik projekt sem lép fel a rendelkezésre álló kapacitásnál nagyobb igénnyel. Ezen problémák kezelésével a multiprojekt menedzsment foglalkozik.

A mindennapi, rutinjellegű tevékenységrendszerek a projektszerűen végrehajtott tevékenységrendszerektől sok szempontból különböznek. A rutinjellegű tevékenységrendszerek alapvető jellemzői, hogy általános, a szervezeti alaprendeltetéshez kapcsolódó célok megvalósítására, vagy ezek feltételeinek biztosítására irányulnak, továbbá időben folyamatosan, ismétlődően kerülnek végrehajtásra. Jellemző rájuk ezen kívül, hogy végrehajtásuk rendjét szervezeti és működési szabályzatok határozzák meg, valamint, hogy az adott feladat folyamatos végrehajtására létrehozott szervezeti munkakörök, a statikus szervezeti hierarchiában elhelyezkedő szervezeti egységek valósítják meg.

A védelmi és a polgári szférában megjelenő tevékenységrendszer változatok kapcsolatait a következő ábra mutatja be.




1/1. ábra – Tevékenységrendszer változatok a védelmi és a polgári szférában

## 1.4 A működésfolytonosság kihívásai

### 1.4.1 Közös és eltérő kihívások a védelmi és a polgári szférában

Az eddigiekből következik, hogy a védelmi és a polgári szférabeli, így a kritikus infrastruktúrák területén megvalósuló folyamatok a működésfolytonosság területén igen sok tekintetben azonos kihívásokkal szembesülnek. Léteznek azonban olyan kihívások, amelyek kifejezetten a védelmi szférában, esetleg kifejezetten a katonai szférában jelennek meg.

A két szféra viszonyához hasonlóan működésfolytonossági szempontból a mindennapi, rutinszerű és a művelet-orientált tevékenységek számos ponton azonos kihívással találkoznak. Az előzőeknek megfelelően azonban a művelet-orientált tevékenységrendszerek az informatikai rendszerekhez kapcsolódó működésfolytonossági kérdések szempontjából a mindennapi, rutinjellegű tevékenységektől több ponton eltérő sajátosságokkal rendelkeznek. Ezek a sajátosságok megnyilvánulnak a működésfolytonosságot veszélyeztető tényezők körében és szerepében, valamint a működésfolytonosság fenntartására, helyreállítására irányuló tevékenységek lehetőségeiben, rendjében és megvalósításában.

### 1.4.2 A védelmi és a polgári szféra közös működésfolytonossági kihívásai

A védelmi és a polgári szférabeli, így a kritikus infrastruktúrák működési folyamatai egyre inkább függnek az informatikai infrastruktúrától, így a működésfolytonossági kérdések is egyre inkább előtérbe kerülnek mindkét szférában. A problémák számos tekintetben azonosak és nem függnek attól, hogy polgári, védelmi vagy a kritikus infrastruktúrák területén működő szervezetről van szó.

Valamennyi esetben előfordulhat például a folyamatos valósidejű működésre vonatkozó igény kérdése, ami a működésfolytonosság szempontjából meglehetősen problematikus lehet. Mindkét szférában egyre nagyobb jelentőséget kap a logisztika, ami tipikusan valós idejű információkat igényel. A polgári szférában tipikusan a különböző folyamatirányítási rendszerekre vonatkozóan érvényes a valósidejű működés követelménye, a katonai szférában pedig a hálózatközpontú hadviselés megjelenése hozta előtérbe ezt a kérdést. Ez esetben az egyes vezetési szintek gyakorlatilag valós idejű helyzetképet látnak, ha azonban ez a kiesések miatt csak ez egyik harcoló félnél valósul meg, az számára behozhatatlan előnyt jelent.

### 1.4.3 A védelmi és a polgári és szféra eltérő működésfolytonossági kihívásai

A tágabb értelemben vett védelmi szféra működésfolytonossági kihívásai csak kisebb mértékben térnek el a polgári szféra kihívásaitól. Annál is inkább így van ez, mivel a tágabb értelemben vett védelmi szféra szervezeteinek jellemző működési folyamatai nem térnek el jelentősen a polgári szférabeli szervezetek működési folyamataitól. Ugyanez jelenthető ki a kritikus infrastruktúrákat megvalósító szervezetekre vonatkozóan is.

Nagyobb különbségek tapasztalhatók, ha a védelmi szféra értelmezését kifejezetten a katonai szférára korlátozzuk. Az információs társadalomban a polgári szférában tapasztalható informatikai támogatottsághoz hasonlóan a katonai szférában kifejezetten a hadviselés területén is egyre inkább előtérbe kerültek és kerülnek az információalapú hadviselési módok. A hálózatközpontú hadviselési koncepció kialakítása, a C4I[14] és CIS[15] rendszerek létrehozása, a kifejezetten katonai informatikai infrastruktúrák (például Force XXI Battle Command Brigade and Below), az informatikai és informatizált eszközök (például harcjárművek), valamint a testfelületi hálózatokkal ellátott harcosok védelmi szférában széles körben történő alkalmazása, mind ezt igazolják.

Mindezekből az következik, hogy az egyes szférák összehasonlításakor működésfolytonossági szempontból különbségként kell értékelnünk, hogy a védelmi szférában megjelennek a polgári szféra veszélyforrásain túlmenő, további veszélyforrások is, továbbá nyilvánvaló, hogy a tradíciók alapján kialakult szervezeti kultúra a polgári szférához képest a védelmi szférában sokkal inkább integrálta a működésfolytonosság egyes elemeit. Mindezek fokozottan érvényesek, ha a védelmi szféra szűkebb értelmezését vesszük figyelembe, azaz kifejezetten a katonai szférára korlátozzuk. Ez esetben a releváns veszélyforrásokban megmutatkozó különbségek és a működésfolytonossághoz való viszonyulást meghatározó szervezeti kultúra eltérései még inkább jelentősek.[16]

### 1.4.4 A rutinszerű és a művelet-orientált tevékenységek közös működés-folytonossági kihívásai

Az előzőekből következik, hogy a művelet-orientált tevékenységrendszer és a projekt gyakorlatilag ugyanazt a fogalmat jelöli. A különbség mindössze annyi, hogy a művelet-

[14]Command (vezetés), Controll (irányítás), Communication (híradás), Computer (informatika) Intelligence (hírszerzés)
[15]Communication and Information Sytem (Híradó és informatikai rendszerek)
[16]Lásd a 3. A működésfolytonosság biztosításának lehetőségei c. fejezetet.

orientált tevékenységrendszer elnevezést a védelmi, míg a projekt elnevezést a polgári szférában használják elterjedten. Ezért a továbbiakban a művelet-orientált tevékenységrendszer fogalmat olyan értelemben használjuk, hogy az lefedi mind a védelmi szférában használatos művelet-orientált működést, mind pedig a polgári szférában használt projekt fogalmat is azzal a kitétellel, hogy a művelet-orientált tevékenységrendszerek tipikusan a védelmi szférára jellemzők és csak kisebb jelentőséggel vannak jelen a polgári szférában.

Napjainkra általánosan jellemző, hogy mind a rutinszerű, mind a művelet-orientált tevékenységrendszerek egyre inkább összekapcsolódnak informatikai infrastruktúrákkal, gyakorlatilag szétválaszthatatlan egységet képeznek azokkal. Az információs társadalomban ugyanis nehezen képzelhető el olyan rutinszerű tevékenység vagy művelet, amelynek ne lenne informatikai vonzata vagy összetevője. Az informatikai elem egyaránt megjelenhet a tevékenység céljában, tárgyában vagy eszközrendszerében, a tevékenységek többségében tipikusan egyszerre több ponton is. Az egyre inkább szállóigévé váló mondat és megfordítása: „*The IT is the business*”, illetve „*The business is the IT*” azt fejezi ki [32] hogy a folyamatok és az IT rendszerek egymással igen szoros kölcsönhatásban állnak, szimbiózisban jelennek meg, így már nem jelenthető ki egyik összetevő elsődlegessége sem.

Mindezek alapján megállapítható, hogy mind a rutinszerű, mind a művelet-orientált működés esetében érvényes az a megállapítás, hogy egyrészről az informatikai rendszerek kulcsfontosságú összetevői a szervezet működési folyamatainak, másrészről, hogy megfelelően működő folyamatok szükségesek az informatikai rendszerek zavartalan működéséhez. A működésfolytonosságot, ennél fogva mindkét tevékenységrendszer esetén minden olyan tényező befolyásolhatja, amely az informatikai rendszerekre illetve a működési folyamatokra hatással lehet. [25]

### 1.4.5 A rutinszerű és a művelet-orientált tevékenységek eltérő működésfolytonossági kihívásai

A korábbiakban áttekintett művelet-orientált tevékenységrendszerek jellemző sajátosságai közé tartoznak többek között a következők: a műveletet végrehajtó erők feladatorientált jellege és heterogenitása; a műveleti tevékenységek sajátosságai; a művelet végrehajtás speciális körülményei; valamint a rendelkezésre álló erőforrások szűkössége. [25]

A műveleteket végrehajtó erőket gyakorlatilag minden esetben az adott feladattól függő,

a művelet előkészítése időszakában kialakított összetétel jellemzi. Ennek megfelelően a műveletet végrehajtó erők jellemzően egymással korábban együtt nem működő, a végrehajtás során is változó, különböző nemzetekhez, szervezetekhez, vagy funkcionális területekhez tartozó összetevőkből állnak. Sokszor az egyes összetevők (például a katasztrófavédelmi műveletbe bevont katonai erők) maguk is ideiglenesen létrehozott működési elemek. A műveletet végrehajtó erők heterogenitása egyben informatikai rendszereik és a működésfolytonossághoz való viszonyulásuk (elvek, követelmények, eljárások, módszerek) heterogenitását is maga után vonja. Így a teljes integráció működésfolytonosságának megvalósítása az összetevők számára viszonylagos autonómiát is biztosító, az adott műveletre specifikusan kialakított, egységes szabályozó és működési rendszert igényel. Ennek létrehozására azonban a művelet előkészítése során általában nem áll rendelkezésre elegendő idő, így az elveket, eljárásokat és módszereket előzetesen szükséges kidolgozni.

A művelet-orientált tevékenységrendszerek általános jellemzője a mindennapi, a rutin-jellegű tevékenységektől eltérő jelleg. E műveletek alapvető tevékenységei tipikusan csak műveleti körülmények között hajthatóak végre, azaz a mindennapi tevékenység során egyáltalán nem, vagy csak korlátozott mértékben gyakorolhatóak, végrehajtásuk meghatározott időtartamra korlátozódik. Mindez maga után vonja a műveleti folyamatok és az ezeket támogató informatikai rendszerek működésfolytonossági megoldásai előzetes kipróbálásának, tesztelésének, begyakorlásának és ellenőrzésének korlátozottságát. Szemben a rutinszerű tevékenységekkel, ebben az esetben a működésfolytonosság biztosításának kapcsán összegyűlt tapasztalatok alapján történő módosítások, visszacsatolások csak elvétve lehetségesek.

Művelet-orientált működés esetén a feladat végrehajtás körülményei a mindennapi tevékenységekhez képest általában problematikusabbak. A környezeti tényezők és esetenként a szembenálló, vagy a művelet végrehajtásában érintett felek által megvalósított veszélyeztetettség, a mostoha működési feltételek (minden év- és napszakban történő tevékenység, terepi körülmények, mobil feladat végrehajtás stb.) az általánosnál jóval nagyobb és eltérő jellegű működésfolytonossági veszélyforrásokat hordoznak, és jelentős hatással vannak a folytonos működés fenntartására, helyreállítására irányuló tevékenységek feltételeire és lehetőségeire is.

A műveletek végrehajtását részben a sajátos működési feltételek, részben a gazdaságos megvalósítás következtében, a műveletet közvetlenül végrehajtó erők, és a

rendelkezésükre álló erőforrások korlátozottsága jellemzi. A végrehajtó erők állományába elsősorban az alaprendeltetést megvalósító összetevők és legfontosabb eszközeik, rendszereik tartoznak. Ezzel szemben a támogatást megvalósító erők jó része eredeti elhelyezési körletében, vagy ideiglenes, de a művelet térségétől távolabbi működési körletben hajtja végre feladatait.

Mindez gyakran azt jelenti, hogy az informatikai rendszerek működésfolytonosságát biztosító erők (szervezeti elemek, személyek) általában csak korlátozott mértékben, vagy egyáltalán nem kerülnek a műveletet végrehajtó erők állományába. Így a működésfolytonossághoz kapcsolódó feladatokat jellemzően "távolról", a helyszínen végrehajtandó teendőket pedig ideiglenes feladatszabással realizálva lehet megvalósítani, ami értelemszerűen sajátos eljárásokat és módszereket igényel.

## 1.5 A működésfolytonosság helye a szakterületek között

A működésfolytonosság az 1/2. ábrának megfelelően számos ponton szorosan kapcsolódik más szakterületekhez. A kapcsolódás nem korlátozódik kizárólag az ábrán feltüntetett esetekre, azonban ezek a kapcsolatok jelennek meg legmarkánsabban. Nyilvánvaló, hogy a felsorolt szakterületekhez való kapcsolódás mértéke sem azonos: a működésfolytonosság legszorosabb kötődése az informatikai biztonsággal, illetve az információtechnológiával alkotott kapcsolatban valósul meg.


1/2. ábra – A működésfolytonosság kapcsolódása más szakterületekhez

Az informatikai biztonság és a működésfolytonosság kapcsolata leginkább az informatikai rendszerek rendelkezésre állásának kérdésében jelenik meg: a működésfolytonosság szükséges feltétele, hogy a működési folyamatokat támogató informatikai rendszerek megfelelőképpen rendelkezésre álljanak. Ez egyúttal az információtechnológiához való szoros kapcsolódást is jelenti, hiszen a rendelkezésre állás biztosítása megfelelő architekturális felépítésű és minőségű informatikai

rendszerek meglétét és megfelelő színvonalú üzemeltetését igényli.

A jogtudományhoz való kapcsolódás a különböző releváns jogszabályok, törvényi előírások, nemzetközi megállapodások (például a 2000. évi IV. törvény, „*Az információ biztonságáról szóló, Brüsszelben, 1997. március 6-án kelt NATO megállapodás megerősítéséről és kihirdetéséről*") figyelembe vételében nyilvánul meg.

A működésfolytonosság a szervezetek szervezeti rendjének belső szabályozási rendszerének megfelelő kialakítását is feltételezi, ez pedig egyrészről szintén a jogtudományhoz, másrészről a vezetési és szervezési szakterületekhez való kapcsolódást jelzi. Utóbbi az informatikai rendszerek megfelelő minőségű üzemeltetéséhez is kapcsolódik, ez ugyanis megfelelő színvonalú irányítást is feltételez.

## 1.6 A működésfolytonosság szemlélete és jellemzőinek rendszerzése

### 1.6.1 Az informatikai biztonság és a működésfolytonosság kapcsolata

Az információs társadalomban megjelenő új kihívások egy részét az informatikai biztonság szakterülete[17] kezeli. Az informatikai biztonság problémaköre a működésfolytonosság problémaköréhez hasonlóan az információs társadalom kialakulásához köthető, azonban a két fogalom – bár egymással szoros kapcsolatban állnak - nem azonos. Az informatikai biztonság alapvetően az informatikai rendszerekre koncentrál, három alapvető kategóriája a bizalmasság, a sértetlenség és a rendelkezésre állás.[18] A bizalmasság azt jelenti, hogy az információ csak korlátozott kevesek számára ismerhető meg, a sértetlenség az eredeti állapotnak megfelelő, konzisztens és hiánytalan objektumot, illetve állapotot jelöl, a rendelkezésre állás pedig olyan informatikai erőforrások meglétére utal, amelyek a rendeltetésüknek megfelelő funkcionalitást képesek nyújtani egy jól definiált helyszínen és időben. [12]

A működésfolytonosság az informatikai biztonsághoz hasonlóan egy állapotot reprezentál, azonban az informatikai biztonságtól némiképpen eltérő szemléletre támaszkodik: holisztikus szemléletű, nem rendszerekben, hanem folyamatokban gondolkodik, nem az informatikai infrastruktúra, hanem a szervezet kritikus funkcionalitásának működésére, biztosítására koncentrál. Célja, hogy a működési

[17] A szakirodalomban az informatikai biztonság és az információbiztonság fogalmak használata nem mindig konzekvens. Jelen értekezésben ezeket a fogalmakat nem tekintjük azonosnak, az információbiztonságot az informatikai biztonságnál tágabb kategóriának tekintjük, amelybe nemcsak az informatikai rendszerekkel kapcsolatba hozható biztonsági kérdések, hanem többek között a papír alapú anyagok biztonsági problémái is beletartoznak.

[18] Egyes irodalmak az informatikai biztonságot öt kategóriára osztják: bizalmasság, sértetlenség, rendelkezésre állás, hitelesség, működőképesség.

folyamatok megfelelően, az előírt és elvárt jellemzőkkel, megszakadás nélkül folyjanak, illetve a kiesések ne haladják meg az egyes folyamatokra előzetesen meghatározott sebezhetőségi ablakot (az elviselhető kiesések maximális időtartamát).

A folyamatok működésfolytonosságának szükséges feltétele az őket kiszolgáló informatikai rendszerekre vonatkozó informatikai biztonság megvalósulása. A folyamatok folytonos működésére az informatikai biztonság mindhárom kategóriája befolyással van. Legszorosabban a rendelkezésre állás kategóriájához kapcsolódik, ugyanakkor nyilvánvaló, hogy közvetve mind a bizalmasság, mind a sértetlenség kategóriájának sérülése is befolyásolhatja fennállását. Bizalmas információ birtokában ugyanis a rosszindulatú támadások sikerének esélye megnő, a sérült, inkonzisztens objektumok nem, vagy csak korlátozottan használhatóak.

A működésfolytonosság kérdésköréhez az említett, főképpen az informatikai erőforrásokra vonatkozó informatikai biztonsági kategóriákon túlmenő összetevők is beletartoznak. Ide kell sorolnunk a megfelelő szabályozottságon alapuló működést, valamint az előre nem látható eseményekre történő előzetes felkészülés kérdéseit is.

### 1.6.2 A működésfolytonosság értelmezése

A működésfolytonosság általában úgy értelmezhető, mint folyamatok jellemzője, de végső soron, a legtágabb értelemben a működésfolytonosság egy szervezet, alakulat kritikus tevékenységrendszereinek, funkcionalitásának meglétére vonatkozik. A kritikus folyamatok működése biztosítja a szervezet alapvető funkcionalitásainak meglétét. A szervezet kritikus folyamatai azok a folyamatok, amelyek hiányában a szervezet nem képes az alapvető funkcionalitásait biztosítani. Ha a kritikus folyamatok működnek, a szervezet biztosítani képes az alapvető, kritikus funkcionalitásait. A szervezeten belüli megközelítés szerint az egyes kritikus folyamatok működésfolytonosságát szükséges biztosítani, de az adott szervezet funkcionalitásait igénybe vevő más személyek/szervezetek a működésfolytonosságot az illető szervezet funkcionalitásaihoz rendelik (szolgáltatás-orientált szemlélet).

A működésfolytonosság gyakorlati megvalósítása az alapvető funkcionalitásokon túlmenő erőforrások felhasználását igényli, azonban a gyakorlati esetek mindegyikében megjelenik egy olyan korlát, amely meghatározza a maximálisan felhasználható extra erőforrásokat. Ennél fogva a működésfolytonosság biztosításának elsősorban az adott szervezet kritikus folyamataira kell koncentrálnia.

A működésfolytonosság szakterülete nem terjed ki a szervezeti stratégiák, célok kezelésére. A szervezetek funkcionalitásai, folyamatai a célok elérése érdekében jönnek létre, a működésfolytonosság ezek kiesésmentes működésére fókuszál, optimalizálásuk azonban kívül esik a működésfolytonosság szakterületén. Mindezekkel összhangban a működésfolytonosság azokra az eseményekre fókuszál, amelyek kifejezetten informatikai rendszerekkel támogatott működési folyamatok kiesését okozzák, és nem tartozik tématerületéhez azoknak a lehetséges katasztrófa eseményeknek a kezelése, amelyek a működési folyamatok kiesését, illetve informatikai rendszerek károsodását messze meghaladó károkat jelentenek. Így például nem tartozik a működésfolytonosság tématerületéhez a szervezetek teljes megsemmisülését is okozó igen nagy erősségű földrengés okozta probléma megoldása, mivel ez esetben nem a működési folyamatok és informatikai rendszerek működésének újraindítása jelenti az elsődleges problémát. Mindezeken túlmenően a működésfolytonosság biztosításnak ugyancsak nem célja azon kisebb jelentőségű események, kiesések kezelése, amelyek a mindennapi normál üzemeltetés területéhez tartoznak (például egy-egy kliens gép meghibásodása).

A működésfolytonosság biztosításakor egyaránt szükséges a preventív és a reaktív megközelítés. Ez a kettős szemlélet megtalálható a védelmi szféra működését meghatározó törvényekben, ezek egyaránt tartalmaznak megelőző és reagáló jellegű előírásokat. [33], [34], [35]

A működésfolytonosság alapvetően a következő három alappillérre támaszkodik:

- Az informatikai erőforrások, az informatikai rendszerek magas színvonalú működése, amely jó minőségű technológia alkalmazásán és magas színvonalú üzemeltetésén alapszik.
- A szervezet működését meghatározó, megfelelően kialakított és betartott szabályozottság alapján történő működés, amely a releváns törvényi előírások, jogszabályok, szabványok figyelembe vételén alapszik.
- Az előre nem látható, váratlan, rendkívüli események (informatikai katasztrófa helyzet) kezelése, amelyek a katasztrófa helyzet esetén alkalmazható előzetes tervek elkészítésén alapszanak.

### 1.6.3 Informatikai erőforrások

Napjainkban mind polgári, így a kritikus infrastruktúrák területén megvalósuló, mind a

védelmi szférabeli tevékenységrendszerek, működési folyamatok erősen támaszkodnak különböző informatikai rendszerekre, ezek kiesésekor általában a működési folyamatok is leállnak. Bizonyos folyamatok kiesése azonban egyáltalán nem, vagy csak meghatározott időre engedhető meg. Ellenkező esetben a szervezet kritikus funkcionalitásait nem képes biztosítani. Az informatikai rendszerek normál működése folyamán olyan veszélyforrások (fenyegető tényezők) léphetnek fel, amelyek a biztonság ellen hatnak, esetleges érvényre jutásukkor az informatikai biztonság sérül, emiatt a folyamatos működés megszakadhat. Például a terrorista akciók tipikus célja a működésképtelenség elérése, amely többnyire az infrastruktúra rombolásán keresztül valósul meg. Tipikus példák erre *„…a közlekedési rendszerek támadása (út, vasút, légi közlekedés, vízi közlekedési rendszerek és mindezek elemei); ipari és mezőgazdasági termelési rendszerek támadása (ipari üzemek, bányák, mezőgazdasági termelő egységek); a gazdasági és pénzügyi rendszerek elleni támadás (bankok, pénzügyi szervezetek); kommunikációs rendszerek elleni támadás (Internet, telefon, TV, rádió, posta, műholdas rendszerek); közművek és energiarendszerek elleni támadás (fúrótornyok, olaj szállító rendszerek és elemei, atomerőművek, vízellátórendszerek, elektromos áram ellátó rendszerek).*” [20] Nyilvánvaló ugyanakkor, hogy mindezen infrastruktúrák nem kizárólagosan terrorista akciók következtében sérülhetnek, számos további fenyegetés veszélyezteti mindezek kiesésmentes működését.

„*Az informatikai rendszer (általában) eszközök, programok, adatok valamint a működtető személyzet információs funkciók, tevékenységek megvalósításra létrehozott rendszere.*” [36] E definícióból következik, hogy a veszélyforrások köre nem merül ki azokban, amelyek kizárólagosan a technikai eszközökre hatnak. Veszélyforrásként kell számba vennünk valamennyi olyan tényezőt, amely bármilyen egyéb módon fenyegeti az informatikai rendszer folyamatos működését (például az üzemeltető személyzet rendelkezésre állásának akadályozásával).

Fontos hangsúlyozni, hogy az informatikai rendszer kiesésmentes működését nemcsak külső fenyegetések veszélyeztetik. A nem megfelelő minőségű, az elvárt követelményeket nem teljesítő, rossz műszaki állapotban levő, nem megfelelő színvonalon üzemeltetett rendszerek önmagukban is problémát okozhatnak, emiatt a beszerzés és üzemeltetés kérdései is befolyásolhatják a működésfolytonosságot.

### 1.6.4 Szabályozott működés

Az informatikai rendszerek megfelelő rendelkezésre állása önmagában nem képes

garantálni a működésfolytonosságot, biztosításához további igényként szükség van megfelelő, jól definiált és dokumentált szabályozásokra, amelyek az adott szervezet működését meghatározzák és egyértelművé teszik.[19] Ezek hiányában ugyanis például a nem megfelelően kialakított hozzáférési jogosultság gondozási eljárásrend okozhatja bizonyos működési folyamatok megszakadást. Ez nemcsak jogosulatlan hozzáféréseket eredményezhet, hanem adat vagy funkcionalitás el nem érésében is megnyilvánulhat, ezzel akadályozva a működésfolytonosságot.

A szabályozott működés kérdéséhez számos, az adott szervezet, alakulat szervezeti kultúrájában megjelenő összetevő is hozzátartozik. Ilyenek az adott szervezetben meglevő szokások, a munkatársaktól, parancsnokoktól és beosztottaktól elvárható magatartás, a meglevő szakmai felkészültség és tapasztalat. A szervezeti kultúrának működésfolytonossági szempontból is fontos sajátossága, hogy változása, fejlődése csak nagyobb időhorizonton valósulhat meg, szemben a szabályozásokkal, amelyek elkészítéséhez és bevezetéséhez viszonylag rövidebb idő kell. A gyakorlatban is megvalósuló működésfolytonosság azonban mindenképpen feltételezi a szervezeti kultúra megfelelő színvonalát is.

### 1.6.5 Katasztrófa helyzet kezelés

Mivel nem léteznek olyan védelmi intézkedések, amelyek alkalmazásával bármilyen katasztrófa esemény (pl. technikai vagy természeti katasztrófa) garantáltan elkerülhetővé válna, a működésfolytonosság összetevői közé tartozik az előre nem látható katasztrófa eseményekre történő előzetes felkészülés is.

Az informatikai katasztrófa helyzet esetére készített akcióterveknek nem feltétlenül a kiesett informatikai rendszer működőképességének visszaállítására kell koncentrálnia, mert előfordulhat, hogy a kieső folyamat visszaállítása az őt támogató informatikai rendszer nélkül, például valamilyen átmenetileg alkalmazott manuális helyettesítő eljárással történik meg.

A katasztrófa helyzet kezelési tervek egyes akcióterveinek az egyes folyamatokhoz tartozó sebezhetőségi ablakokból (az elviselhető kiesések maximális időtartamából) kell kiindulnia. Olyan akcióterveket szükséges kidolgozni, amelyek végrehajtása garantálja, hogy az egyes kiesett folyamatok a hozzájuk tartozó sebezhetőségi ablakon belül visszaállíthatók legyenek. Mivel egy-egy működésfolytonossági probléma esetén

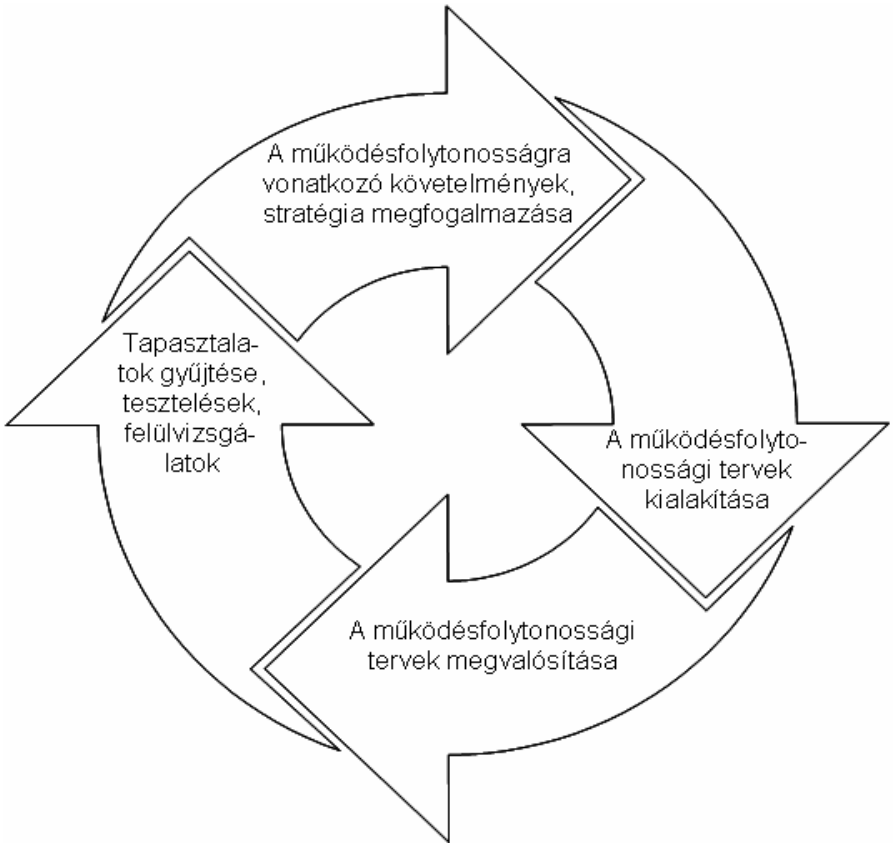
[19]Beinschróth József: Katasztrófa és üzletmenet folytonossági tervek a közigazgatásban és az üzleti szférában, előadás, Kriminálexpo, 2002.

gyakori, hogy nemcsak egyetlen folyamat esik ki, a különböző akciótervekben szükséges figyelembe venni a kiesett folyamatok között fennálló függőségeket. Előfordulhat ugyanis, hogy egy meghatározott folyamat visszaállítása csak akkor kezdődhet meg, ha egy másik már sikeresen vissza lett állítva.

### 1.6.6 A működésfolytonosság életciklusa

Egy szervezet életében a működésfolytonosság feltételeinek kialakítása nem egyszeri tevékenység, hanem folyamatosan felmerülő, ellátandó feladat.[20] Az általánosan ismert és elterjedten használt Deming ciklus, másnéven PDCA modell[21] (Plan-Do-Check-Act) alapján modellezhető a működésfolytonosság életciklusa is. (A PDCA gyakorlatilag bármilyen műveletre, tevékenységre, folyamatra, rendszerre, működtetésre, koncepcióra, elgondolásra vonatkoztatható, zárt hatásláncú, folyamatosan ismétlődő körfolyamat elv, így természetesen a működésfolytonosság témakörében is használható.)

A működésfolytonosság PDCA ciklusát a következő ábra mutatja be.




1/3. ábra – A működésfolytonosság PDCA ciklusa

[20] Az angol szakirodalomban gyakran jellezik a következőképpen: Never ending story - Soha véget nem érő történet.
[21] Magyar nyelven gyakran TVEB (Tervezés-Végrehajtás-Ellenőrzés-Beavatkozás) modellnek nevezik.

### 1.6.7 A működésfolytonossághoz kapcsolódó, létező megközelítések

Számos olyan megközelítés létezik, amely valamilyen szinten kapcsolódik a működésfolytonossághoz. [37] Ezek egy része az informatikai biztonsághoz való kapcsolódása miatt érinti a működésfolytonosságot, más részük a működésfolytonosság valamilyen részterületéhez kapcsolódik. Az informatikai biztonsághoz kapcsolódó megközelítések például a következők:

- az ITB 8. sz. ajánlásában szereplő megközelítés;
- az ITB 12. sz. ajánlásában szereplő gyakorlati szintű megközelítés;
- az ITB 12. sz. ajánlásban alkalmazott játékelméleti megközelítés;
- a folyamatszabályozási megközelítés;
- a kriptográfiai megközelítés.

A működésfolytonosság valamely részterületét érintő megközelítések például a következők:

- szervezeti diagramm;
- a COBIT kocka;
- a COBIT érettségi modell;
- az Ishikawa diagramm;
- a rendelkezésre állás modellje;
- a tervezési modell.

A felsorolt megközelítésekről megállapítható, hogy egyik sem alkalmaz olyan megközelítést, amely kifejezetten, elsődleges célként a működésfolytonosságra fókuszálna. Valamennyien csak érintőlegesen kapcsolódnak a működésfolytonossághoz, a kapcsolódás erőssége pedig tételenként eltérő.

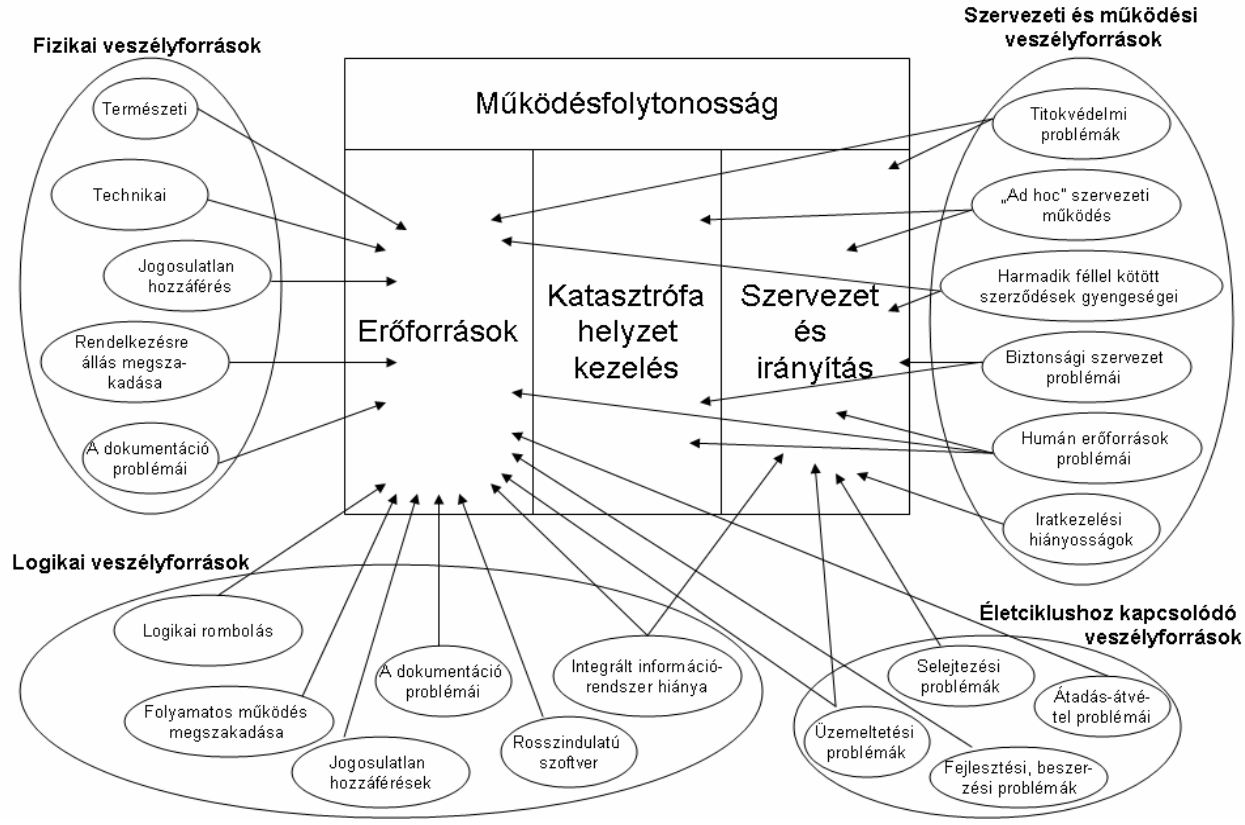
### 1.6.8 A veszélyforrásokra épülő általános megközelítés

A működésfolytonosság megfelelő szintű tárgyaláshoz olyan megközelítés szükséges, amely kifejezetten a működésfolytonosságra koncentrál. [37]

Az 1.6.2 pontban rögzítetteknek megfelelően a működésfolytonosság a következő három alappillérre támaszkodik: az informatikai erőforrások illetve magas színvonalú üzemeltetésük, megfelelő szabályozás (szervezet és irányítás), továbbá a katasztrófa

helyzetekre történő előzetes felkészülés. [38] A működésfolytonosságot különböző veszélyforrások[22], veszélyeztetik, azonban ezek nem közvetlenül okozhatják az egyes kritikus működési folyamatok megszakadását, nem közvetlenül a működésfolytonosságra hatnak, hanem valamelyik alappilléren keresztül közvetve fejthetik ki negatív hatásukat. Az egyes alappillérek azonban nem teljesen függetlenek egymástól. Nyilvánvaló például, hogy a katasztrófa helyzetekre való felkészülésnek támaszkodnia kell mind az erőforrásokra, mind pedig a szabályozási kérdésekre. Ennélfogva a katasztrófa helyzetekre való felkészülést – közvetve - mindazon veszélyforrások is veszélyeztetik, amelyek a másik két alappillérre negatív hatást fejthetnek ki. A veszélyforrások rendszerezése különböző szempontok szerint történhet.[23] Ebben a megközelítésben a fizikai, logikai, szervezeti és működési valamint az életciklushoz kapcsolódó veszélyforrás csoportokat különböztetjük meg.

A veszélyforrások és az alappillérek kapcsolatát az 1/4. ábra szemlélteti. (Az ábrán a közvetett kapcsolatok nincsenek nyilakkal reprezentálva.)




1/4. ábra – A veszélyforrások és az alappillérek kapcsolatának rendszere

Az egyes veszélyforrások pontos felsorolása nem tehető meg egzakt módon. Egyrészről

[22]Lásd a 3.3 A folyamatok működést veszélyeztető veszélyforrások és védelmi feladatok c. fejezetet
[23]A releváns irodalomban a veszélyforrások többféle szempont szerinti csoportosítása ismeretes.

azért, mert a működésfolytonosságot fenyegető veszélyforrások kisebb mértékben függnek a szervezet által végzett tevékenységrendszertől, azaz attól, hogy az illető szervezet normál, mindennapi rutinszerű vagy művelet-orientált tevékenységet folytat. Másrészről azért sem lehetséges az egzakt felsorolás, mert létezhetnek olyan veszélyforrások is, amelyek – mivel bekövetkezésükre ez ideig nem volt példa - létezése általánosan nem tudatosult[24], ugyanakkor a működési folyamatok megszakadását okozhatják. Mindezek miatt a bemutatott rendszer általános megközelítésnek tekinthető, mivel az esetek mindegyikében számba veendő veszélyforrásokat tartalmazza. Ugyanakkor a benne szereplő veszélyforrások kisebb méretű bővítésével alkalmas mind a védelmi szférabeli szervezetek, mind a kritikus infrastruktúrák szervezeteinek folyamataira, mind pedig a művelet-orientált tevékenységrendszerekre vonatkozó működésfolytonossági kérdések tárgyalására.

Ez a megközelítés az 1.6.2 pontnak megfelelően egyaránt értelmezhető a működési folyamatokra és a szervezet funkcionalitásainak meglétére, benne a veszélyforrások egyszerre kétféle csoportosításban jelennek meg. A rendszer egyrészről tartalmazza azt, hogy az egyes veszélyforrások mely veszélyforrás kategóriába tartoznak, másrészről pedig azt, hogy a működésfolytonosság alappillérei közül melyekre vonatkozóan jelentenek fenyegetést.

## 1.7 Összegzés, következtetések

Jelen fejezet az értekezés bevezetésében rögzítetteknek megfelelően a következő kutatási cél elérésére fókuszál:

*„A működésfolytonosság alapkoncepciójának kidolgozása, szemléletének megfogalmazása, jellemzőinek rendszerbe foglalása olyan módon, hogy a rendszerezett jellemzők felhasználásával a működésfolytonosság törvényszerűségei tárgyalhatók legyenek.”*[25]

A kutatási cél elérése érdekében a következő feladatokat végeztem el:

- Az információs társadalom kihívásaiból kiindulva meghatároztam és értelmeztem a működésfolytonosság jelentését.
- Rendszereztem és összevetettem a polgári és a védelmi szféra tevékenységrendszereit és ehhez kapcsolódóan meghatároztam a különböző

[24]Nem zárható ki például eddig még nem észlelt természeti jelenség bekövetkezése.
[25]Lásd 7. oldal, 1. pont.

szférákban és eltérő tevékenységrendszerekben a működésfolytonosság kihívásait.

- Megvizsgáltam, hogy a működésfolytonosság mennyiben kapcsolódik az informatikai biztonsághoz, mennyiben fed át más szakterületeket és mennyiben kapcsolódik hozzájuk.
- Meghatároztam a működésfolytonosság szemléletét és rendszereztem jellemzőit.

A feladatok elvégzésével a következő eredményekre jutottam:

Megállapítottam, hogy a működésfolytonosság az elterjedten használt üzletmenet folytonosság fogalomnál általánosabb abban az értelemben, hogy nemcsak az üzleti, hanem tetszőleges szférában is használható

Összevetve a polgári és a védelmi szféra tevékenységrendszereit, arra a következtetésre jutottam, hogy a védelmi és a polgári szféra némiképpen eltérő kihívásokat produkál a működésfolytonosság biztosításának szempontjából, továbbá, hogy a normál, mindennapi rutinszerű tevékenységekhez képest rá vonatkozóan kisebb mértékben eltérő követelmények ismerhetők fel a védelmi szférára különösen jellemző művelet-orientált tevékenység rendszer esetén. Az összevetésből azt a következtetést is levontam, hogy a polgári és védelmi szféra egyre szorosabb kapcsolódása, egymástól való függősége nem teszi lehetővé, hogy a védelmi szféra működésfolytonossági kérdéseit kizárólag önmagukban vizsgáljuk, tárgyalásukkor vele együtt a polgári szféra működésfolytonossági jellemzőit is érintenünk kell.

Megvizsgálva a működésfolytonosság kapcsolódását más szakterületekhez, azt állapítottam meg, hogy az átfedés elsősorban az informatikai biztonság egyik részterületén, informatikai rendszerek rendelkezésre állásának tekintetében van jelen, ugyanakkor a működésfolytonosságnak vannak olyan összetevői, amelyek közvetlenül nem tartoznak az informatikai biztonság kérdéseihez. Ezen túlmenően felismertem, hogy a működésfolytonosság az informatikai biztonságon túlmenően további szakterületekhez is kapcsolódik. Mindezekből azt a következtetést vontam le, hogy a működésfolytonosság nem tárgyalható az informatikai biztonság részeként.

Elemezve a működésfolytonosság szemléletét azt a következtetést vontam le, hogy a működésfolytonosság alapvetően a következő három alappillérre támaszkodik: informatikai erőforrások kezelése, szervezeti és irányítási kérdések, illetve a katasztrófa helyzetek kezelése. Ezekhez kapcsolódóan megállapítottam, hogy a

működésfolytonosság biztosítása nem egyszeri, befejezhető tevékenység, hanem folyamatos tevékenységet igényel, az ismert PDCA életciklusnak megfelelő megközelítésben.

Rendszerbe foglaltam a működésfolytonosság jellemző tulajdonságait úgy, hogy a létrehozott rendszer alapján a működésfolytonosság viszonylag egyszerűen tárgyalhatóvá vált. A kialakított rendszer tartalmazza a működésfolytonosság alappilléreit és megfelelő csoportosítással a kihívást jelentő veszélyforrásokat. Arra a következtetésre jutottam, hogy a bemutatott rendszer egyaránt használható a védelmi és a polgári szférában, így a kritikus infrastruktúravédelem területén is, mind a mindennapi folyamatos, mind pedig a művelet-orientált tevékenységek esetén.

# 2 A releváns hazai és nemzetközi, polgári és védelmi szféra specifikus ajánlások

*" A haditudomány arra tanít bennünket, ne abban bízzunk, hogy az ellenség nem fog jönni, hanem abban, hogy mi készen állunk a fogadásra; sem annak az eshetőségében, hogy nem fog támadni, hanem inkább abban a tényben, hogy pozícióinkat bevehetetlenné tettük."*

*Szun Ce: A háború művészete*

## 2.1 A működésfolytonosság biztosításához támpontot adó ajánlások felhasználása a védelmi szférában

A különböző szervezetek meghatározott szintű üzemeltetői, döntéshozói, parancsnokai részéről természetes elvárás, hogy a kompetencia körükbe tartozó informatikai rendszerekkel támogatott folyamatok megfelelően szabályozott, kiesésmentes működtetésének biztosításához szabványok, illetve ajánlások formájában segítséget kapjanak. Nem lehető fel azonban sem a hazai, sem a nemzetközi ajánlások között olyan, amely kifejezetten a működésfolytonosság biztosítására koncentrálna, kifejezetten erre vonatkozóan tartalmazna előírásokat.

Az előző fejezet szerint a működésfolytonosság az informatikai biztonság, illetve az információtechnológia szakterületéhez kapcsolódik legszorosabban. Mind az informatikai biztonság, mind az információtechnológia témaköreit számos ajánlás tárgyalja, az utóbbi esetében az informatikai rendszerek üzemeltetésnek szakterülete az, amire vonatkozóan fellelhetők a működésfolytonossághoz is kapcsolódó ajánlások.

Mivel a különböző szervezetek működési folyamatai mind a normál, mindennapi, rutinszerű, mind a művelet-orientált tevékenységrendszer esetén nagymértékben támaszkodnak az általuk alkalmazott informatikai rendszerekre, ezek megbízható, kiesésmentes működésére, az informatikai biztonságot és az informatikai rendszerek üzemeltetést tárgyaló ajánlások egyaránt adhatnak támpontokat a működésfolytonosság tekintetében is.

A továbbiakban áttekintem, összehasonlítom és értékelem a leginkább ismert és elterjedten használt, az informatikai biztonsághoz és informatikai rendszerek üzemeltetésének témaköreihez leginkább kapcsolódó ajánlásokat azzal a céllal, hogy megvizsgáljam, hogy mi az alapvető céljuk, mennyiben tekinthetők mérvadónak működésfolytonossági kérdésekben, illetve, hogy tartalmaznak-e a működésfolytonosságra vonatkozó összetevőket, továbbá, hogy mennyiben vannak

jelen, és mennyiben alkalmazhatóak a védelmi szférában.

## 2.2 Az informatikai rendszerek biztonságára vonatkozó követelményeket tárgyaló ajánlások értékelése, különös tekintettel a védelmi szférára

### 2.2.1 A vizsgált ajánlások

Az utóbbi években, évtizedekben az informatikai biztonságot tárgyaló, különböző szintű ajánlások, szabályozások jelentek meg mind a polgári, mind a védelmi szférában. [39] (Olyan szabvány, ajánlás azonban, amely kifejezetten a kritikus infrastruktúra védelemre fókuszálna, nem lelhető fel.) Ezen ajánlások és szabályozások azonban többnyire rendszerekben gondolkodnak, technológiai szemléletűek, egymással nem, vagy csak többé-kevésbé konzisztensek. Adott körülmények között a relevánsak kiválasztása és következetes alkalmazásuk általában nehézségekbe ütközik, mivel informatikai rendszerek biztonságára vonatkozó követelményeket számos szabvány tartalmaz.

Az informatikai biztonság témakörét a védelmi szférában már hosszú ideje nagy jelentőségűnek tekintik. Ezt többek között az is bizonyítja, hogy a világon az első ilyen, kifejezetten az informatikai biztonságra vonatkozó szabvány védelmi szférabeli kezdeményezés eredményeként jött létre 1985-ben és az USA Védelmi Minisztériuma (DoD – Department of Defence) által megfogalmazott informatikai biztonsági követelményeket tartalmazta. Ezen túlmenően további informatikai biztonsági követelményeket tartalmazó szabványok is születtek a védelmi szférában, például az INFOSEC (Information Security – információ biztonság) a NATO és az EU informatikai biztonságra vonatkozó megközelítést tartalmazza.

Az első magyarországi informatikai biztonsághoz némiképpen kapcsolódó szabályozás is kötődik a védelmi szférához: az 1/1981 BM rendelet, az államigazgatás területén és az állami nagyvállalatok számára volt kötelező, tűz- és vagyonvédelemmel foglalkozott, az ennek végrehajtására kiadott KSH utasítás a számítóközpontok titokvédelmét is tárgyalta.

A polgári szférában is megjelent számos különböző, az informatikai biztonságra vonatkozó szabvány, így kijelenthető, hogy meglehetősen nagy számú, az informatikai biztonságot tárgyaló dokumentum létezik, amelyek eltérő ismertséggel, különböző elterjedtséggel, különböző szemlélettel rendelkeznek. A továbbiakban azokat a szabványokat értékeljük, amelyek a leginkább ismertnek tekinthetők. Az értékelésben a

következő dokumentumok, ajánlások vesznek részt:

- TCSEC (Trusted Computer System Evalution Criteria - Biztonságos Számítógéprendszerek Értékelési Kritériumai);
- ITSEC (Information Technology Security Evaluation Criteria - Információtechnológia Biztonsági Értékelési Kritériumok);
- CC (Common Criteria for Information Technology Security for Evaluation - Az informatikai termékek és rendszerek biztonsági értékelésének módszertana);
- NATO INFOSEC (Information Security – Informatikai Biztonság);
- MEH ITB (Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság) 12. sz. ajánlás;
- A PSZÁF (Pénzügyi Szervezetek Állami Felügyelete) 10/2001. számú ajánlása;
- MSZ ISO/IEC 17799.

### 2.2.2 TCSEC

A TCSEC időrendben az elsőnek tekinthető informatikai biztonságra vonatkozó ajánlás, amelyet az USA Védelmi Minisztériuma dolgozott ki 1985-ben.[26] Fő jellemzője, hogy a rendszerek logikai védelmére koncentrálva különböző követelményeket előíró biztonsági csoportokat definiál, amelyek teljesítésével főképpen szoftver termékek minősíthetők. Például a Microsoft Windows NT Workstation Version 4.0, illetve Windows NT Server Version 4.0 operációs rendszerek a TCSEC C2 biztonsági csoportba lettek besorolva 1999-ben.

Megállapítható, hogy a TCSEC az informatikai rendszerek logikai védelmével, a biztonság funkcionális és minősítési követelményeivel foglakozik, és nem tárgyalja az adminisztratív és a fizikai védelem területeit, a szervezeti, személyi és fizikai biztonság kérdéseit, előírásai az 1.6.2 pontban megadott alappillérek közül az „*Erőforrások*” összetevőbe sorolhatók be. Főképpen az informatikai termékek gyártóinak ad támogatást azzal, hogy lehetőséget teremt a kereskedelembe kerülő informatikai termékek biztonsági minősítésére. Ez természetesen egyúttal azt is lehetővé teszi, hogy a felhasználók a piacon jelenlevő termékeket biztonsági szempontok alapján képesek legyenek összevetni és azok közül az igényeiknek megfelelő biztonsági követelményeket kielégíthető termékeket kiválasztani.

[26] Trusted Computer System Evalution Criteria (TCSEC), Department of Defence, USA, 1985.

Ugyanakkor elmondható, hogy a TCSEC nem tartalmaz az informatikai rendszerek üzemeltetésére, a szervezet folyamataira vonatkozóan megfelelő, részletesen kidolgozott követelményeket. Az informatikai rendszereket üzemeltető, felhasználó szervezetek számára, az informatikai biztonság lefedett területének tekintetében azonban egyaránt relevánsnak tekinthető mind a védelmi, mind a polgári szférában, így a kritikus infrastruktúrák területén is. A működésfolytonosság kérdését explicite nem érinti, működésfolytonosság szempontjából mindössze annyiban tekinthető hasznosnak, amennyiben az elvárt követelményeket kielégítő, minősített termékek felhasználása azt támogatja.

### 2.2.3 ITSEC

Az ITSEC gyakorlatilag a TCSEC európai megfelelője.[27] Kidolgozása Anglia, Franciaország, Hollandia és Németország együttműködésével történt meg 1989-ben. Alapelveiben, követelményeiben a TCSEC-kel alapvetően megegyezik, ennek megfelelően fő jellemzője, hogy a rendszerek logikai védelmére koncentrálva különböző követelményeket előíró biztonsági csoportokat definiál, amelyek teljesítésével főképpen szoftver termékek minősíthetők. Például a Sun Microsystems Inc. terméke, a Sun Solaris 2.6 operációs rendszer az ITSEC E3 biztonsági csoportba lett besorolva 1999-ben.

A TCSEC-ben alkalmazott szemlélettel megegyezően az ITSEC az informatikai rendszerek logikai védelmével foglalkozik, a biztonság funkcionális és minősítési követelményeit tárgyalja, de nem foglalkozik az adminisztratív és a fizikai védelem támasztotta igényekkel, a szervezeti, személyi és fizikai biztonság kérdéseivel. Előírásai a TCSEC-hez hasonlóan az 1.6.2 pontban megadott alappillérek közül az „*Erőforrások*” összetevőbe sorolhatók be. A TCSEC-hez hasonlóan az informatikai termékek gyártóit azzal támogatja, hogy lehetőséget teremt a kereskedelembe kerülő informatikai termékek biztonsági minősítésére, a felhasználókat pedig azzal, hogy a piacon jelenlevő termékeket biztonsági szempontok alapján képesek legyenek összevetni. Mindezek miatt az általa lefedett informatikai biztonsági területek tekintetében mind a polgári mind a védelmi szférában, így a kritikus infrastruktúrák területén is relevánsnak tekinthető.

Az ITSEC a TCSEC-hez hasonlóan a működésfolytonosság kérdését explicite nem érinti.

[27] Information Technology Security Evaluation Criteria (ITSEC), Európai Közösség, 1991

### 2.2.4 CC

Az Európai Közösség valamint az amerikai és kanadai kormányok támogatásával jött létre, 1998. évi, 2.1-es változata ISO/IEC 15408 szabványként is megjelent. Magyar szabványként is elfogadott: a MEH ITB (Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság) 16. sz. ajánlása a CC 1.0 verziójának magyar feldolgozásaként jött létre.[28] Létrehozásának célja elsősorban az volt, hogy a korábbi ajánlások technikai eltérései összhangba kerüljenek. A CC a TCSEC-hez és az ITSEC-hez hasonlóan biztonsági osztályokat definiál, a végleges követelmények azonban a korábbiakban megfogalmazottaknál árnyaltabbak lettek. Alkalmazása lehetőség ad kifejezetten biztonsági termékek (pl. tűzfal) alaposabb biztonsági minősítésére. Ennek megfelelően például a Cisco Secure PIX Firewall a CC EAL4 biztonsági osztályba lett besorolva 2001-ben.

Az előzőekhez hasonlóan kijelenthető, hogy előírásai az 1.6.2 pontban megadott alappillérek közül az „*Erőforrások*” összetevőbe sorolhatók be, továbbá, hogy az általa tárgyalt informatikai biztonsági kérdések tekintetében használatának nincs akadálya sem a védelmi, sem pedig a polgári szférában, így a kritikus infrastruktúrák területén sem. Ugyanakkor elmondható, hogy a TCSEC-hez és az ITSEC-hez hasonlóan ez esetben is a termék van a központban, az üzemeltetéshez tartozó adminisztratív, fizikai, szervezeti stb. kérdéseket a CC nem tárgyalja, így a működésfolytonosság kérdése is csak közvetve és csak részben érintett.

### 2.2.5 INFOSEC

Az INFOSEC a NATO és az EU informatikai biztonságra vonatkozó megközelítést tartalmazza.[29] „*Az INFOSEC biztonsági intézkedések alkalmazását jelenti a kommunikációs, informatikai vagy más elektronikus rendszerben feldolgozott, tárolt illetve továbbított információk védelme érdekében, melyek biztosítják a rendszerben az információ bizalmasságának, integritásának és rendelkezésre állásának védelmét, valamint a rendszerek által nyújtott szolgáltatások integritásának és rendelkezésre állásának folyamatos fenntartását, függetlenül attól, hogy a káresemény szándékosan vagy véletlenszerűen következik-e be. Annak érdekében, hogy a kommunikációs, informatikai vagy más elektronikus rendszerben feldolgozott, tárolt, illetve továbbított információk bizalmasságának, integritására és rendelkezésre állására vonatkozó*

[28]Common Criteria for Information Technology Security Evaluation 2.0, ISO/IEC 15408, 1999.
[29]Information Security, NATO Security Comittee

*biztonsági célkitűzéseit meg lehessen valósítani, egy sor egymást kiegészítő intézkedést (fizikai, személyi, információ biztonsági és INFOSEC) kell foganatosítani, hogy olyan védett környezet jöjjön létre, melyben a kommunikációs, informatikai és más elektronikus rendszerek működtetése megvalósulhat.*" [40]

Az INFOSEC alapvetően két részből áll, a kommunikáció biztonságára (COMSEC - Communication Security) és a számítógépes rendszerek biztonságára (COMPUSEC – Computer Security) vonatkozó részből. A kommunikáció biztonságára vonatkozó rész elsősorban a továbbított adatok védelmére fókuszál, és elsősorban a kriptográfiai megoldásokat tárgyalja. Ezen túlmenően foglalkozik az elektromágneses kisugárzás okozta biztonsági problémákkal is. A számítógépes rendszerek biztonságával foglalkozó rész a bizalmasság, sértetlenség, rendelkezésre állás fogalmaknak megfelelő megközelítésben tárgyalja a hardver, a szoftver és a firmware biztonságot.

Az előzőekhez hasonlóan kijelenthető, hogy előírásai az 1.6.2 pontban megadott alappillérek közül az „*Erőforrások*" összetevőbe sorolhatók be, továbbá, hogy korlátai figyelembe vételével felhasználhatósága a védelmi szférában nyilvánvaló, de használatának az előzőekhez hasonlóan a polgári szférabeli, így a kritikus infrastruktúrák területén történő használatának sincs akadálya. Megközelítése működésfolytonossági kérdéseket közvetlenül nem érint, legfeljebb annyiban, amennyiben a rendelkezésre állás a működésfolytonosság szükséges feltétele.

### 2.2.6 MEH ITB 12. sz. ajánlás

A MeH ITB 12. sz. ajánlás 1996-ban jelent meg és jelentősen túllépett a kizárólag a termékek biztonsági minősítését követő szemléleten. [41] Az informatikai rendszerek elemei (hardver, szoftver, hálózatok) esetében az ITSEC-et adaptálta, ugyanakkor részletes követelményeket és védelmi intézkedéseket tartalmaz az informatikai biztonság adminisztratív és a fizikai védelem területeire, a szervezeti, személyi és fizikai biztonság kérdéseire is. Ennek megfelelően bevezetésre kerültek az „*információvédelem*" és „*megbízható működés*" kategóriák, amelyek mindegyikében alap, fokozott és kiemelt biztonsági osztályokat definiáltak.

Mindegyik biztonsági osztályhoz részletes követelményrendszer tartozik (infrastruktúra, hardver, szoftver, adathordozók, dokumentáció, adatok, kommunikáció, személyek stb. tekintetében). Az ajánlás útmutatást ad arra vonatkozóan, hogy az egyes rendszereket, illetve rendszertípusokat melyik biztonsági osztályba szükséges besorolni. Például az IV-F (információvédelem - fokozott) biztonsági osztály a „*szolgálati titok, valamint a nem*

*minősített adatok közül a különleges személyes adatok, nagy tömegű személyes adatok, banktitkok, közepes értékű üzleti titkok feldolgozására, tárolására is alkalmas rendszer biztonsági osztálya*".

Az ajánlásról kijelenthető, hogy előírásai az 1.6.2 pontban megadott alappillérek közül az „*Erőforrások*", illetve „*Szervezet és irányítás*" összetevőkbe sorolhatók be. Felhasználhatóságának nincsenek korlátai sem a védelmi, sem a polgári szférában, így a kritikus infrastruktúrák területén sem. Bár ez az ajánlás sem tárgyalja közvetlenül a működésfolytonossági kérdéseket, mégis az előzőeknél lényegesen több támpontot ad ezen a területen. Ez egyrészt azzal valósul meg, hogy itt – bár nem teljes körűen - megjelennek az üzemeltetéshez tartozó adminisztratív, fizikai, szervezeti stb. kérdések is, másrészről pedig azzal, hogy a megbízható működés kategóriában a logikai rendelkezésre állás tekintetében időadatokat határoz meg.

### 2.2.7 A PSZÁF 10/2001. számú ajánlása

Ez az ajánlás a pénzügyi szervezetekre vonatkozik és e körben alkalmazása az eddigiektől eltérően kötelező jellegű. Nem közvetlenül az informatikai biztonsággal, hanem a pénzügyi szervezetek működésének biztonsági feltételeivel foglalkozik, ennél fogva érinti az informatikai biztonságot, sőt kisebb mértékben a működésfolytonosság kérdését is. [43] Konkrétumokat nem, csak általános irányelveket fogalmaz meg, szemlélete a folyamatszemlélethez közelít. Előírásai az 1.6.2 pontban megadott alappillérek közül az „*Erőforrások*", „*Katasztrófa helyzet kezelés*", illetve „*Szervezet és irányítás*" összetevőkben jelennek meg.

Mivel a banki és pénzügyi infrastruktúra a kritikus infrastruktúrákhoz tartozik, így védelme az 1.3.2 pontban rögzítettek szerint kapcsolódik a védelmi szféra feladataihoz, ennél fogva ez az ajánlás tulajdonképpen egy specifikus védelmi szférabeli ajánlásnak tekinthető. A pénzügyi szférában előírt kötelező alkalmazása miatt alkalmazhatósága egyértelmű, szemléletének átvétele azonban a nem pénzügyi szervezetek számára is hasznos lehet.

Az ajánlásban a működésfolytonosság szemlélete is megjelenik. Bár a működésfolytonosság teljes tárgyalását nem tartalmazza, hozzá kapcsolódóan használja az „*üzleti szolgáltatások folytonosságát biztosító tartalék berendezések*", a „*támogató informatikai rendszerek folyamatos és biztonságos működése*", továbbá az „*üzleti szolgáltatásai folyamatosságát akadályozó rendkívüli események*" kategóriákat.

### 2.2.8 MSZ ISO/IEC 17799

A Brit Szabványügyi Hivatal által 1995-ben kiadott BS 7799 szabvány első része a teljes szervezetre vonatkozó, az összes rendszerelem csoportot átölelő informatikai biztonsági követelményeket és védelmi intézkedéseket tartalmaz. A BS 7799 első részét 2000-ben ISO/IEC 17799 néven nemzetközi szabványként fogadták el, mely szabvány 2002-ben MSZ ISO/IEC 17799:2002 néven magyarul, magyar szabványként is megjelent. [12] Jelenleg érvényben levő változata az MSZ ISO/IEC 17799:2006, az előző változattól szemléletmódjában gyakorlatilag nem tér el, a két változat között elsősorban szerkezeti, szóhasználatbeli különbségek vannak.

Jellemzője, hogy nem kifejezetten az informatikai termékekhez köthető biztonsági, hanem sokkal inkább az üzemeltetési környezethez kapcsolódó kérdésekre koncentrál, a teljes szervezetet és minden rendszerelemet átfogó informatikai biztonságmenedzsment rendszer megvalósítására és ellenőrzésére a vonatkozó követelményrendszer kidolgozásával. Ez a szabvány már alapot nyújt arra is, hogy a megfelelő akkreditálás és tanúsítási eljárások alkalmazásával lehetővé váljon a felhasználói rendszer – akár egyenkénti, akár szervezeti szintű – minősítése, tanúsítása a szabványnak megfelelően[30].

A szabványt következő főbb összetevők alkotják:

- Kockázatfelmérés és kockázatjavítás;
- Biztonságpolitika;
- Az információbiztonság szervezete;
- Vagyontárgyak kezelése;
- Emberi erőforrások biztonsága;
- Fizikai és környezeti biztonság;
- A kommunikáció és az üzemeltetés irányítása;
- Hozzáférés ellenőrzés;
- Információs rendszerek beszerzése, fejlesztése és karbantartása;
- Az információbiztonsági incidensek kezelése

[30] A tanúsítás az MSZ ISO/IEC 27001:2006 szabvány alapján történhet.

- A működés folytonosságának irányítása;
- Megfelelőség.

A szabvány „*A működés folytonosságának irányítása*” fejezetében a következő alfejezeteket tartalmazza:

- A információbiztonság befoglalása a működésfolytonosság irányításának folyamatába;
- Működésfolytonosság és kockázatfelmérés;
- Az információbiztonságot magukba foglaló működésfolytonossági tervek kidolgozása és megvalósítása;
- A működés folytonosságának tervezési keretrendszere;
- A működésfolytonossági tervek vizsgálata, fenntartása és újrafelmérése.

Mindezek alapján megállapítható, hogy – bár nem ez az elsődleges célja - ez a szabvány az, amely az informatikai biztonságra vonatkozó szabványok közül a működésfolytonosság tekintetében a leginkább relevánsnak tekinthető. Előírásai az 1.6.2 pontban megadott alappillérek közül „*Erőforrások*”, „*Katasztrófa helyzet kezelés*”, illetve „*Szervezet és irányítás*” összetevők mindegyikében megjelennek.

A védelmi és a polgári szférában is, ennél fogva a kritikus infrastruktúrák területén is felhasználható, ugyanakkor a biztonságmenedzsment teljes körű tárgyalására irányuló törekvés és a viszonylag rövid terjedelem miatt a tárgyalás meglehetősen nagyvonalú, gyakran nem ad konkrét támpontokat. Például csak az információ osztályozására vonatkozó alapelveket ad meg, de konkrét osztályokat nem definiál.

A szabványt, illetve előző változatát meglehetősen széles körűen használják, a multinacionális cégek döntő többsége informatikai biztonságának menedzseléshez ezt a szabványt tekinti relevánsnak. A kritikus infrastruktúrák területén, például a pénzügyi, banki szférában hasonlóképpen elterjedtnek tekinthető. Többféle konkrét követelményrendszernek is alapját képezi.[31]

### 2.2.9 A vizsgált ajánlások fő jellemzői

A vizsgált ajánlások fő jellemzőit a következő táblázat foglalja össze.

[31]Például az Informatikai és Hírközlési Minisztérium kezdeményezésére 2004-ben kidolgozott IBIK (Az Informatikai Biztonság Irányításának Követelményrendszere) is erre a szabványra épül. http://www.halozatbiztonsag.hu/documents/MIBIK/IBIK_v095.pdf

| | **A működésfolyonosság érintettsége** | **A rendszer érintett alappillérei** | **Megjegyzés** |
|---|---|---|---|
| TCSEC | Explicite nem érintett | Erőforrások | Elsősorban a gyártókat támogatja |
| ITSEC | Explicite nem érintett | Erőforrások | Elsősorban a gyártókat támogatja |
| Common Criteria | Explicite nem érintett | Erőforrások | Magyar nyelven, magyar szabványként is fellelhető |
| NATO INFOSEC | Explicite nem érintett | Erőforrások | |
| MEH ITB 12. sz. ajánlás | Részben érintett | Erőforrások Szervezet és irányítás | Magyar nyelven, magyar szabványként is fellelhető |
| FSZÁF 10/2001. számú ajánlása | Részben érintett | Erőforrások Katasztrófa helyzet kezelés Szervezet és irányítás | Kötelező érvényű, magyar nyelven, magyar szabványként is fellelhető |
| MSZ ISO/IEC 17799:2006 | Nagy mértékben érintett | Erőforrások Katasztrófa helyzet kezelés Szervezet és irányítás | Magyar nyelven, magyar szabványként is fellelhető |

2/1. táblázat - Az informatikai rendszerek biztonságára vonatkozó ajánlások

Összefoglalásként megállapítható hogy az áttekintett informatikai biztonságra vonatkozó szabványok és ajánlások között nem lelhető fel olyan, amely kifejezetten a működésfolytonossági kérdésekre koncentrál. E kérdéskörben felmerülnek olyan kérdések is, amelyek az értékelt dokumentumok egyikében sem tárgyaltak. Az ajánlások előírásai hozzárendelhetők az 1.6.2 pontban megadott alappillérek egyes összetevőihez, azonban közülük teljes mértékben egyiket sem fedik le.

## 2.3 Az informatikai rendszerek üzemeltetésére vonatkozó követelményeket tartalmazó ajánlások értékelése különös tekintettel a védelmi szférára

### 2.3.1 A vizsgált ajánlások

Mint korábban megállapítottuk, kifejezetten a működésfolytonosság biztosítására vonatkozó ajánlások nem léteznek sem a polgári, sem a védelmi szférában, azonban az informatikai biztonságra vonatkozó ajánlások egy része azonban rendelkezik olyan összetevőkkel, amelyek érintik a működésfolytonosság kérdését. Ezeken túlmenően léteznek olyan – elsősorban a polgári szférában kidolgozott – ajánlások, amelyek az

informatikai rendszerek üzemeltetésére vonatkozóan tartalmaznak előírásokat abból a célból, hogy az informatikai rendszerek optimális üzemeltetését támogassák. [44]

Céljuk összhangban van azzal, hogy a szervezetek elsődleges célja az informatikai rendszereik biztonságos, költséghatékony üzemeltetése és a működési folyamataik megszakadás nélküli, folyamatos működtetése. Ezen ajánlások nem rendszer-, hanem folyamatszemléletűek, így közelebb állnak a működésfolytonossághoz, mint az informatikai biztonságra vonatkozó ajánlások többsége. Céljuk, hogy a folyamatok megfelelően, az előírt és elvárt jellemzőkkel, megszakadás nélkül menjenek végbe, illetve a kiesések ne haladják meg az egyes folyamatokra meghatározott sebezhetőségi ablakot.

A továbbiakban azokat az ajánlásokat értékeljük és vetjük össze, amelyek a leginkább ismertnek tekinthetők. Az értékelésben a következő dokumentumok, ajánlások vesznek részt:

- ITIL (IT Infrastructure Library – Informatikaszolgáltatás-irányítás könyvtár);
- Az ITIL-re épülő gyártófüggő megoldások;
- COBIT (Control Objectives for Information and Releated Technology – Kontroll irányelvek az információ-technológia irányításához, kontrolljához és ellenőrzéséhez).

### 2.3.2 ITIL

Az ITIL angol kormányzati kezdeményezésre és támogatással jött létre a 80-as években: a CCTA (Central Computer and Telecommunication Agency – Központi Számítógép és Távközlési Ügynökség) programjának célkitűzése szerint egységes szerkezetben és terminológiával kívánták összefoglalni az informatikai rendszerek üzemeltetésére vonatkozó jó és bevált gyakorlatokat (best practices). [45] A munka eredményeképpen több mint 40 könyvből álló könyvsorozat jött létre, ezek képezték az alapját és váltak névadójává a módszertannak. Jelenleg az ITIL-nek megfelelő informatikaszolgáltatás irányítás mellett elkötelezett legfontosabb szervezet az itSMF (IT Szolgáltatás Menedzsment Fórum). Független, nonprofit szervezetként legfőbb törekvése, hogy partnerként együttműködjön a kormányzati és szabványosítási testületek széles körével.

Az ITIL a szolgáltatásirányítás nyilvános, mindenki számára hozzáférhető, modellként működő, folyamatorientált szemléletű módszertana, amely az informatikai rendszerek

működtetésének, irányításának bevált gyakorlatát írja le. Új informatikaszolgáltatási kultúrát feltételez, amelyben az informatikai folyamatok minden szereplőjének tisztában kell lennie azzal, hogy munkájának végső célja az, hogy szolgáltatást nyújtson a szervezet alapfolyamatai számára.

Az ITIL heterogén környezetben működő, gyártófüggetlen keretrendszer, mely az informatikai szolgáltatásmenedzsment koncepcióra épül [79]. Eszerint az egymással együttműködő informatikai folyamatok alapvető feladata, hogy jól definiált és mérhető szolgáltatási szinteken biztosítsák az IT szolgáltatások minőségét. Ennek elősegítéséhez két definiált folyamatcsoport, illetve az ezekbe sorolt kulcsfolyamatok kerültek meghatározásra. Ezek a kulcsfolyamatok végzik az informatikai folyamatok biztosítását és támogatását. A definiált folyamatcsoportok és kulcsfolyamatok a következők (az eredeti angol nyelvű kifejezések és rövidítéseik a zárójelben találhatók):

- Szolgáltatásbiztosítás (Service Delivery)
    - Szolgáltatásszint biztosítás (Service Level Management -SLM);
    - Rendelkezésre állás biztosítás (Availability Management - AM);
    - Informatikaszolgáltatás-folytonosságbiztosítás (IT Service Continuity Management - ITSCM);
    - Kapacitásbiztosítás (Capacity Management - CM)
    - Informatikaszolgáltatás pénzügyi irányítása (Financial Management FM);
- Szolgáltatástámogatás (Service Support);
    - Ügyfélszolgálat (Szervezeti egység: Service Desk);
    - Incidenskezelés (Incident Management);
    - Problémakezelés (Problem Management);
    - Változáskezelés (Change Management);
    - Konfigurációkezelés (Configuration Management);
    - Kiadáskezelés (Release Management).

(Megjegyzés: Az ITIL-ben a konfigurációkezelés és a kiadáskezelés kifejezéseket sajátos értelemben használják. A konfigurációkezelés annak a folyamatnak a neve, amely magában foglalja az összes vonatkozó informatikai komponens rögzítését és felügyeletét a konfigurációkezelés adatbázisán keresztül. A kiadáskezelés ugyanakkor az a folyamat, melynek során a kiadási egységek például jóváhagyott hardver és szoftver változatok telepítése megtörténik.)

Látható, hogy a működésfolytonosság kérdése két kulcsfolyamattal is érintett: mind az Informatikaszolgáltatás-folytonosságbiztosítás (ITSCM) mind a Rendelkezésre állás

biztosítás (AM) kulcsfolyamatokhoz kapcsolódik.

A Rendelkezésre állás biztosítása az ITIL szerint az informatikaszolgáltatás informatikai folyamataihoz kapcsolódó azon tervezési, implementálási és irányítási tevékenységeiből áll, amelyek a rendszerek és szolgáltatások rendelkezésre állásának olyan magas szintjét biztosítják, amely a szervezet alaptevékenységei által támasztott igényeknek megfelel. Az ajánlás az informatikai folyamatok és rendszerek rendelkezésre állását több kategórián keresztül tárgyalja, ilyenek például a következők:

- A kiesési, illetve a definiált szolgáltatási idő hányadosa;
- A meghibásodás nélküli átlagos működési idő (Mean Time Between Failures - MTBF);
- A hiba előfordulások közötti átlagos időtartam (Mean Time Between Service/System Incident - MTBSI);
- A javítások átlagos időtartama (Mean Time To Repair/Restore - MTTR);

Az ajánlás a Rendelkezésre állás kulcs-folyamathoz kapcsolódóan az informatikai rendszerek és folyamatok jellemzőinek javítására vonatkozó módszereket is javasol:

- Kockázatkezelés;
- Redundanciák alkalmazása (tartalék alkatrészek, duplikált elérhetőségi útvonalak, hibatűrő diszk alrendszerek, automatikus detektálás és korrekció, csökkentett szinten történő futtatás);
- Komponens meghibásodások hatáselemzése (Component Failure Impact Analysis - CFIA);
- Meghibásodási eseménylánc elemzése (Fault Tree Analysis - FTA);
- Megfelelő tervezés (Szemlélet, amely szerint a rendelkezésre állási képességek javítása leginkább a tervezés kezdeti szakaszában lehetséges, így a rendelkezésre állási követelményeket a tervezési kritériumok között kell figyelembe venni.);

Az ITIL-beli Informatikaszolgáltatás-folytonosságbiztosítás kulcsfolyamat az informatikai rendszereket érintő katasztrófákkal kapcsolatos kockázatok és az azokkal szembeni sérülékenység kezelésével foglalkozik. Megfelelő intézkedéseket határoz meg az alaptevékenység folytonosságának biztosítására. Mindezek érdekében egyaránt támaszkodik mind az üzleti hatáselemzés, mind pedig a kockázatkezelés módszereire.

Az ajánlás az Informatikaszolgáltatás-folytonosságbiztosításához kapcsolódóan a következő visszaállítási lehetőségeket sorolja fel:

- Nem készülünk a kiesésekre (Ritkán használt módszer, kizárólag a vezetés felelős döntésén alapulhat.);
- Papír alapú, manuális eljárás használata (Általában csak részleges és időleges megoldást jelenthet.);
- Viszontmegállapodások, Kölcsönösségi szerződések (Túlhaladott megközelítés, a nagygépes technológiák esetén jelenthetett használható megoldást.);
- „Erőd módszer” (A sérülékenység minimalizálása.);
- Fokozatos helyreállítás (Hideg tartalék alkalmazása.);
- Közbenső helyreállítás (Meleg tartalék alkalmazása.);
- Azonnali helyreállítás (Forró tartalék alkalmazása.);
- „Alvó szerződések” (Berendezések rendelkezésre álláson tartása.);
- Kockázatáthárítás (Biztosítások kötése.).

Az ajánlás javasolja, hogy dokumentált, írásbeli folytonossági tervet kell elkészíteni, amely tartalmazza a helyreállítási tevékenységeket, a szerepeket, az elérhetőségeket, kapcsolatokat stb. A tervet folyamatosan aktualizálni kell és a példányokat alternatív helyszíneken kell tárolni. A tervhez kapcsolódó fontos követelmény az időről-időre történő tesztelés.

Mindezek alapján megállapítható, hogy az ITIL használatának nincs akadálya sem a védelmi, sem a polgári szférában, így a kritikus infrastruktúrák területén sem, továbbá, hogy – bár nem ez az elsődleges célja – az ITIL foglalkozik a működésfolytonossággal, kezelését folyamatai között, más folyamatokkal azonos súllyal tárgyalja. Működésfolytonossági kérdéseket érintő előírásai az 1.6.2 pontban megadott alappillérek közül az „*Erőforrások*”, „*Katasztrófa helyzet kezelés*”, illetve „*Szervezet és irányítás*” összetevők mindegyikében megjelennek. Ezzel összhangban kijelenthető, hogy az ITIL működésfolytonossági szempontból mindenképpen relevánsnak tekinthető, szemléletmódja, definiált folyamatai illeszkednek a működésfolytonossági kérdésekhez. (Ugyanakkor megállapítható, hogy az ITIL-ben használt terminológia a működésfolytonosságot tárgyaló irodalomban használttól némiképpen eltér.)

### 2.3.3 Az ITIL-re épülő gyártófüggő megoldások és termékek

Az ITIL mára de facto nemzetközi szabvánnyá vált. Konzisztens, integrált megközelítést és terminológiát nyújt, ennél fogva számos multinacionális vállalat is elfogadta, és saját gyakorlatába beépítette a terminológiát és megközelítést. [46] Saját ITIL-re épülő

ajánlásokat több multinacionális cég is kidolgozott. Ilyenek például a következők:

- HP: ITSM (IT Service Management)
- IBM: IT Service Processes
- Microsoft: MOF (Microsoft Office Framework)

Mivel ezen vállalatok ajánlásai gyakorlatilag teljes mértékben az ITIL-re épülnek és átvették annak szemléletét, kijelenthető, hogy az ITIL kapcsán megfogalmazott megállapítások ezekre is érvényesek.

Érdemes megjegyezni, hogy az ITIL-szerű működés támogatására több konkrét szoftver eszközt is kifejlesztettek. Ilyenek például a következők:

- Computer Associates: Allfusion, Unicenter
- HP-Compaq: Openview
- IBM: Tivoli
- Intraware (Janus technologies): Argis
- MainControl: MC/Empower
- Marval: Marval Service Management
- Network Associates: Magic Solutions
- Novadigm: Radia Inventory Manager
- Peregrine: Assetcenter, Servicecenter
- PS'Soft: Qualiparc
- Remedy (BMC, Peregrine): Remedy
- Tally System: TS.Center
- Synergon: ACTS

### 2.3.4 COBIT

Az ISACA (Information Systems Audit and Control Association - Információrendszer Ellenőrök Egyesülete) és az ISACF (Information Systems Audit and Control Fundation – Információrendszer Ellenőrök Alapítványa) együttes támogatásával jött létre az IT Governance Institute (IT Irányítási Intézet), amely 1996-ban létrehozta a COBIT nyílt szabványt [48], az IT szabványok, módszerek, élenjáró gyakorlatok egységes rendszerbe foglalt módszertani eszközét. [47]

A COBIT gyártófüggetlen, általánosan alkalmazható, nemzetközileg elfogadott keretrendszer, amely elsősorban az IT rendszerek átvilágítási/auditálási szempontjait vizsgálja. [49] Alapelve a következő: Az információtechnológiát az üzleti célok elérése

érdekében alkalmazzuk, ennek során az IT erőforrások IT folyamatokat hajtanak végre, ezek eredményei hozzájárulnak az üzleti célok eléréséhez. A folyamatok működését különböző veszélyforrások akadályozzák, amelyek különböző kockázatokat jelentenek. Megfelelő kontrollok alkalmazásával ezek elfogadható szintre csökkenthetők.

A COBIT megközelítés az IT infrastruktúrát négy főterületre (az informatikai életciklus négy szakasza) való felosztás szerint vizsgálja. Ezek a következők:

- Tervezés és szervezet;
- Beszerzés és bevezetés;
- Informatikai szolgáltatás és támogatás;
- Felügyelet.

Az Informatika szolgáltatás és támogatás a következő pontokból áll:

- Szolgáltatási szintek meghatározása;
- Külső szolgáltatások kezelése;
- Teljesítmény és kapacitás kezelése;
- Folyamatos működés biztosítása;
- Rendszer biztonságának biztosítása;
- Költségek megállapítása és felosztása;
- Felhasználók képzése;
- Informatikai felhasználók segítése;
- Konfiguráció kezelése;
- Problémák és rendkívüli események kezelése;
- Adatok kezelése;
- Létesítmény kezelése;
- Üzemeltetés irányítása.

Látható, hogy a működésfolytonosság kérdése a Folyamatos működés biztosítása pontban nevesítetten megjelenik. Ez az összetevő a következőknek megfelelően alpontokra van bontva:

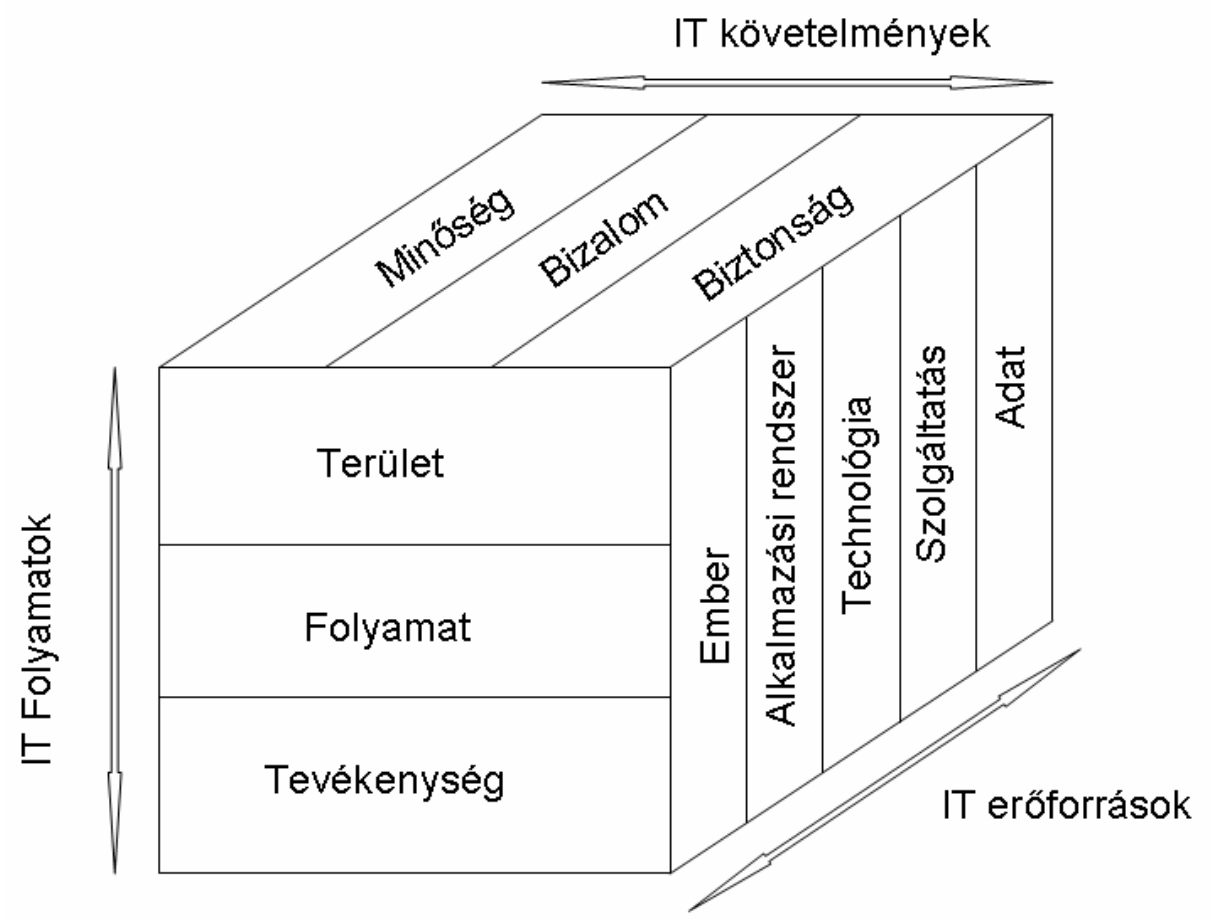
- Informatikai folyamatossági keretrendszer;
- Informatikai folyamatossági keretrendszer, stratégia és filozófia;
- Informatikai folyamatossági terv tartalma;
- Az informatikai folyamatossági követelmények minimalizálása;
- Az informatikai folyamatossági terv aktualizálása;

- Az informatikai folyamatossági terv tesztelése;
- Az informatikai folyamatossági tervhez kapcsolódó képzés;
- Az informatikai folyamatossági terv szétosztása;
- A felhasználó osztály által kialakított alternatív munkafolyamatok, helyettesítő eljárások;
- Kritikus fontosságú informatikai erőforrások;
- Tartalék telephely és hardverek;
- Külső (off-site) tartalék adattárolás;
- Tervmódosítási eljárás.

Valamennyi ponthoz részletes kontroll irányelvek tartoznak, figyelembe véve az informatikai kritériumokat (eredményesség, hatékonyság, bizalmasság, sértetlenség, hozzáférhetőség, szabályosság, megbízhatóság) és a szükséges informatikai erőforrásokat (emberi erőforrások, alkalmazások, technológia, technikai környezet, adatok).

A COBIT megközelítés szerint egy-egy szervezet különböző beosztású menedzserei más-más szempontok alapján értékelik az alkalmazott információtechnológiát. Így a felsővezetők az informatikához kapcsolódó üzleti követelményeket, az informatikai vezetők az általuk menedzselt IT erőforrásokat, a felhasználók pedig az IT folyamatokat helyezik előtérbe.

A COBIT ezt a hármas nézőpont rendszert modellezi az ún. COBIT kockával, amit a következő ábra mutat be.




2/1. ábra – A COBIT kocka

Mindezek alapján megállapítható, hogy a COBIT – bár nem ez az elsődleges célja - foglalkozik a működésfolytonossággal, kezelését folyamatai között, más folyamatokkal azonos súllyal tárgyalja. Ezzel összhangban kijelenthető, hogy a COBIT működésfolytonossági szempontból mindenképpen relevánsnak tekinthető, szemléletmódja, definiált folyamatai illeszkednek a működésfolytonossági kérdésekhez. Működésfolytonossági kérdéseket érintő előírásai az 1.6.2 pontban megadott alappillérek közül az „*Erőforrások*”, „*Katasztrófa helyzet kezelés*”, illetve „*Szervezet és irányítás*” összetevők mindegyikében megjelennek. Megállapítható továbbá, hogy az COBIT használatának nincs akadálya sem a védelmi, sem a polgári szférában így a kritikus infrastruktúrák területén sem.

### 2.3.5 Az ITIL és a COBIT összevetése

Az előzőek alapján megállapítható, hogy a COBIT és az ITIL között több ponton is lényeges hasonlóság van. A COBIT szélesebb területet fed le, ugyanakkor több pontban

is megfeleltethetők egymásnak. Az ITIL kulcsfolyamatai gyakorlatilag lefedik a következő COBIT összetevőket:

- Tervezés és szervezet
  - Kockázatok értékelése;
- Beszerzés és bevezetés
  - Rendszerek installálása (üzembe helyezése) és jóváhagyása;
  - Változások kezelése;
- Informatikai szolgáltatás és támogatás
  - Szolgáltatási szintek meghatározása;
  - Külső szolgáltatások kezelése;
  - Teljesítmény és kapacitás kezelése;
  - Folyamatos működés biztosítása;
  - Rendszer biztonságának biztosítása;
  - Költségek megállapítása és felosztása;
  - Informatikai felhasználók segítése;
  - Konfiguráció kezelése;
  - Problémák és rendkívüli események kezelése;
- Felügyelet
  - Eljárások felügyelete.

Az ITIL és a COBIT leginkább alkalmazási körben különböznek. Míg ugyanis az ITIL kizárólag az informatika üzemeltetési és üzemeltetés-szervezési kérdéseivel foglalkozik, addig a COBIT kiterjed az informatika előkészítési/tervezési és megvalósítási (beszerzés/fejlesztés), valamint felügyeleti területeire is.

Mindkét modell abból indul ki, hogy hogyan teremthető meg a kapcsolat az üzleti igények és az informatikai megoldások között. Eltérésként értékelhető azonban, hogy míg az alkalmazáshoz szükséges befektetéseket a COBIT esetén elsősorban a nagy és fejlett informatikával rendelkező vállalatok tudják megindokolni és megvalósítani, addig az ITIL-t - kompaktságának és áttekinthetőségének köszönhetően - az üzemeltetés fejlesztésében még csak kezdeti lépéseket tévő szervezetek is hatékonyan tudják alkalmazni.

### 2.3.6 A vizsgált ajánlások fő jellemzői

A vizsgált ajánlások fő jellemzőit a következő táblázat foglalja össze.

| Ajánlás | A működésfolyonosság érintettsége | A rendszer érintett alappillérei | Megjegyzés |
|---|---|---|---|
| ITIL | Szorosan kapcsolódik | Erőforrások<br>Katasztrófa helyzet kezelés<br>Szervezet és irányítás | Alapja a gyártófüggő változatoknak |
| IT Service Processes | Szorosan kapcsolódik | Erőforrások<br>Katasztrófa helyzet kezelés<br>Szervezet és irányítás | Az ITIL-re épül, IBM termék |
| ITSM | Szorosan kapcsolódik | Erőforrások<br>Katasztrófa helyzet kezelés<br>Szervezet és irányítás | Az ITIL-re épül, HP termék |
| MOF | Szorosan kapcsolódik | Erőforrások<br>Katasztrófa helyzet kezelés<br>Szervezet és irányítás | Az ITIL-re épül, Microsoft termék |
| COBIT | A legszorosabban kapcsolódik | Erőforrások<br>Katasztrófa helyzet kezelés<br>Szervezet és irányítás | Magyar nyelven is fellelhető |

2/2. táblázat - Az informatikai rendszerek üzemeltetésére vonatkozó ajánlások

Összefoglalásként megállapítható, hogy az áttekintett szabványok és ajánlások szorosan kapcsolódnak a működésfolytonossági kérdésekhez. Mindegyikük keretrendszer, szemléletmódjuk hasonló, szempontrendszereik között átfedések vannak, használatuknak nincs akadálya sem a védelmi, sem a polgári szférában így a kritikus infrastruktúrák területén sem. A vizsgált ajánlások működésfolytonosság szempontjából releváns előírásai hozzárendelhetők az 1.6.2 pontban megadott alappillérekhez.

## 2.4 Az ajánlások szerinti működés a védelmi szférában

Az eddigiekben megállapítottuk, hogy a vizsgált ajánlások döntő többségére igaz, hogy felhasználásuk lehetősége adott mind védelmi, mind pedig a polgári szférában, így a kritikus infrastruktúrák esetében is. [39] Megállapítható, hogy a gyakorlat él az ajánlások adta lehetőségekkel, és számos példa bizonyítja, hogy nemzetközi és a hazai katonai gyakorlatba is beépültek, illetve a felhasználásukra vonatkozó kezdeti lépések

megtörténtek. Mindezek nem korlátozódnak a szűkebb értelemben vett védelmi szférára: az ajánlások figyelembe vétele a védelmi szféra más területein is felismerhető.

A továbbiakban megvizsgáljuk, hogy a tárgyalt ajánlások mennyiben jelentek meg a védelmi szféra, illetve a kritikus infrastruktúrák működésének gyakorlatában. Az ismertetésre kerülő példák bizonyítják, hogy mind az informatikai biztonság ajánlásainak, mind pedig az informatikai rendszerek üzemeltetésre vonatkozó ajánlások tekintetében számos példa található arra, hogy a vizsgált ajánlások a gyakorlatban is használatosak.

Az informatikai biztonságra vonatkozó ajánlások védelmi szférabeli, illetve a kritikus infrastruktúrák működésének területén történő felhasználását a következők igazolják.

A kifejezetten védelmi szférabeli szervezet igényeit kifejező, az illető szervezet kezdeményezésére létrehozott ajánlások (TCSEC, INFOSEC) felhasználása nyilvánvaló. Kötelező jellege miatt a kritikus infrastruktúrák területéhez tartozó pénzügyi szervezetek esetében ugyancsak nyilvánvaló a PSZAF 10/2001. számú ajánlásának használata.

A 12/2004. (BK 12.) BM utasítás a hatálya alá tartozó szervezetek számára kidolgozott Informatikai Biztonsági Politika céljának megfogalmazásakor hangsúlyozza, hogy összhangban kíván lenni az MSZ ISO/IEC 15408 számú szabvánnyal (Common Criteria), az MSZ ISO/IEC 17799 számú szabvánnyal, valamint a vonatkozó ITB 8. és 12. számú ajánlásokkal. [50]

Bár szabványra nem hivatkozik, a Magyar Köztársaság Nemzeti Biztonsági Stratégiája a következőket tartalmazza: „*A technológia rohamos fejlődésének korában új feladatként jelentkezik a korszerű és biztonságos informatikai infrastruktúra kialakítása és a kormányzati információs rendszerek védelme. A kormányzati információs rendszert fel kell készíteni a kibernetikai támadások megelőzésére és kivédésére. A védelem sikere érdekében szoros koordináció szükséges mind a szövetségesekkel, mind az informatikai és távközlési szolgáltatók, valamint kutatóközpontok között.*” [51] Nyilvánvaló, hogy mindezek kizárólag szabványok alkalmazásán keresztül valósíthatók meg.

A Honvédelmi Minisztérium Elektronikai, Logisztikai és Vagyonkezelő Rt. Elektronikai Igazgatósága 2002. évben megszerezte a BS 7799-2:2002 szabvány szerinti „*Információ biztonság irányítási rendszer*”–re vonatkozó tanúsítását. [53], [54]

A 90-es években kiadott Magyar Honvédség Informatikai Szabályzata [55] ugyan közvetlenül nem hivatkozik sem informatikai biztonsági, sem üzemeltetési ajánlásra, de szemléletében azok tükröződnek, és közvetve érintett mindkét kérdéskör.

Az informatikai rendszerek üzemeltetésére vonatkozó ajánlások szerinti működés - az informatikai biztonság szabványainak felhasználásához hasonlóan - felismerhető a védelmi szférában, illetve a kritikus infrastruktúrák működésének területén. Az üzemeltetési szabványoknak megfelelő működésre való áttérés azonban a gyakorlatban csak fokozatosan valósulhat meg. Ennek egyrészről az az oka, hogy – a hosszabb távon várt üzemletetési költségek csökkenése ellenére – a bevezetés szakaszában számottevő anyagi erőforrásra van szükség, másrészről az áttérés egyfajta szemléletmódbeli, informatikai kultúrát érintő változásokat igényel, ami mindenképpen időigényes folyamat.

A védelmi és a polgári szférára általánosan jellemző, hogy az IT infrastruktúra modernizálása és az alkalmazások integrálásának megteremtése folyamatban van, de még messze nem ért véget. Az ajánlások szerinti működés bevezetésében az üzleti szféra multinacionális vállalatai jutottak legmesszebbre, ugyanakkor a közszolgálati és védelmi szférában is megtörténtek az első lépések, melyek során az COBIT, illetve ITIL folyamatok alapozó elemei részben megjelentek. Így pl. a Fővárosi Önkormányzatnál az ITIL alapú szabályozás alapjai felismerhetők. [46].

A BM Központi Adatfeldolgozó, Nyilvántartó és Választási Hivatal az államigazgatásban az ITIL szemléletet alapul véve támaszkodott az informatikai outsourcingra az országos választások és népszavazások során. [57] Bár a Magyar Kormányzat ez ideig nem deklarálta egységes szabvány használatát [58], a 12/2004. (BK 12.) BM utasítás a hatálya alá tartozó szervezetek számára kidolgozott Informatikai Biztonsági Politika céljának megfogalmazásakor hangsúlyozta, hogy az ismert informatikai biztonságra vonatkozó ajánlásokon túlmenően összhangban kíván lenni a COBIT-ban megfogalmazott előírásokkal. [59]

Figyelemre méltó, hogy jelentős védelmi szférabeli szervezetek a tárgyalt ajánlások terjesztésében érdekelt szerveződések tagszervezeteiként jelennek meg, így például a HM Elektronikai, Logisztikai és Vagyonkezelő Rt. az ISACA[32] magyar tagozatának tagszervezete. Az itSMF magyar tagozatának alapító tagszervezete a Honvédelmi Minisztérium, az utóbbi néhány év folyamán több HM munkatárs az itSMF által

[32]Information System Audit and Control Association - Információ Ellenőrök Nemzetközi Szövetségének Szervezete

szervezett ITIL tanfolyamon vett részt. [60]

A vizsgált informatikai rendszerek üzemeltetésére vonatkozó ajánlások védelmi szférában történő alkalmazására nemzetközi példák is léteznek. Így például Nagy-Britannia hadseregének gyakorlatát, a JSP 602 (Hierarchy of Directions & Guidance) dokumentumsorozat rögzíti. [61]

A dokumentumsorozat a következő területeket fedi le:

- Applications (AP - Alkalmazások);
- Information Environment (IE- Informatikai környezet);
- Information Infrastructure (II – Informatikai Infrastruktúra);
- Information Governance (IG – Informatikai irányítás);
- Managed Services (MS - Menedzselt szolgáltatások);
- Security of Information (SI – Az információ biztonsága).

A fejezetcímekből látható, hogy a JSP 602 az ITIL-nél szélesebb területet fed le. További különbség, hogy attól eltérően nem keretrendszer, hanem konkrét gyakorlatot rögzít. Mindezek ellenére megállapítható, hogy szorosan kapcsolódik az ITIL-hez, számos pontján konkrétan hivatkozik is rá, külön alfejezetben részletezi az itSMF szervezet szerepét. A legtöbb hivatkozás a Managed Services fejezet alatt található, ezen kívül előfordulnak még továbbiak az Applications fejezetben is. A JSP 602 szemléletében és terminológiájában az ITIL-re épül, nyilvánvaló, hogy kidolgozásakor – számos más ajánlás mellett – mint meghatározó tényezőt vették figyelembe.

A NATO ugyan nem használ egységes szabványt az informatikai biztonság menedzsmentjére [58], ugyanakkor a NATO Európai Parancsnoksága évek óta az ITIL-re épülő HP termékeket használja IT infrastruktúrája felügyeletére. [63] Bár részletesen nem kerül tárgyalásra, ugyanakkor a NATO C3 Technical Architecture ADatP-34 NATO dokumentum szabványként többek között megemlíti az ITIL-t. [64]

## 2.5 Összegzés, következtetések

Jelen fejezet az értekezés bevezetésben rögzítetteknek megfelelően a következő kutatási cél elérésére fókuszál:

*„Az informatikai biztonságra és az informatikai rendszerek üzemeltetésére vonatkozó ajánlások olyan megközelítésű elemzése, melynek eredményeképpen kiválaszthatók*

*közülük azok, amelyek a védelmi szférában működésfolytonosság tekintetében is relevánsnak tekinthetők."*[33]

A kutatási cél elérése érdekében a következő feladatokat végeztem el:

- Elemeztem, megvizsgáltam és összehasonlítottam a leginkább ismert és elterjedten használt, az informatikai biztonsághoz valamint az informatikai rendszerek üzemeltetéséhez leginkább kapcsolódó ajánlásokat azzal a céllal, hogy rögzítsem, hogy mi az alapvető céljuk, továbbá, hogy mennyiben tekinthetők relevánsnak működésfolytonossági kérdésekben, illetve, hogy mennyiben kapcsolhatók a működésfolytonosság fő jellemzőit összefoglaló rendszerhez.
- Megvizsgáltam, hogy az ajánlások alkalmazhatósága mennyiben tér el a védelmi és a polgári szférában, illetve a kritikus infrastruktúrák területén, továbbá, hogy az áttekintett ajánlások figyelembe vétele mennyiben valósul meg a védelmi szférában, illetve a kritikus infrastruktúrák területén.

A feladatok elvégzésével a következő eredményekre jutottam:

Az elemzés alapján megállapítottam, hogy olyan ajánlás, amely kifejezetten a működésfolytonosságra koncentrálna, nem létezik, azonban vannak közöttük olyanok, amelyek legalábbis részben tartalmaznak olyan normatívákat, amelyek működésfolytonossági kérdésekben relevánsnak tekinthetők. Ilyen ajánlások elsősorban az MSZ ISO 17799, az ITIL és a COBIT.

Az alkalmazhatóság vizsgálata során arra a következtetésre jutottam, hogy az áttekintett ajánlások alkalmazhatók a védelmi és polgári szférában, illetve a kritikus infrastruktúrák területén, alkalmazhatóságukra vonatkozóan gyakorlatilag nem állapíthatók meg különbségek. Azt a következtetést is levontam, hogy az ajánlások szerinti működés a védelmi szférában, illetve a kritikus infrastruktúrák területén teljes körűen jelenleg nem valósul meg, ugyanakkor számos példa igazolja, hogy a vizsgált területeken egyre inkább relevánsnak számítanak.

[33]Lásd 7. oldal, 2. pont.

# 3 A működésfolytonosság megvalósítása a védelmi szférában

*„Nem vállalok közösséget azzal a könnyelmű reménnyel, hogy valami véletlen majd megment bennünket."*

*Clausewitz*

## 3.1 A működésfolytonosság megvalósításának védelmi szférabeli összetevői

Az 1/4. ábrán bemutatott rendszer meghatározó összetevői a működésfolytonosság megvalósulását akadályozó, a szervezet kritikus folyamataira ható veszélyforrások. Hatásaik következtében a kritikus működési folyamatok megszakadhatnak, kiesések következhetnek be. Az egyes szervezetek azonban általában el képesek viselni kritikus folyamataik bizonyos ideig tartó kiesését, azaz nem jelent számukra elfogadhatatlan veszteséget, ha a folyamatok kiesései a sebezhetőségi ablaknak megfelelő időtartamon belül maradnak. Az elviselhető kiesési időtartamok folyamatonként általában különbözőek. (Például egy légi irányítási rendszer kritikus folyamatai csak minimális időtartamra eshetnek ki, ugyanakkor a kiképzés, felkészítés folyamatainak több napon keresztül tartó kiesése esetlegesen elfogadható lehet.) Előfordulhat az is, hogy egy-egy folyamat sebezhetőségi ablaka időszakonként más és más. A szervezet folyamatai közül a kritikus folyamatok kiválasztása és a hozzájuk tartozó sebezhetőségi ablakok kijelölése az adott szervezetre vonatkozó helyzetfeltárás alapján történhet meg. [42]

Az 1/4. ábrán bemutatott rendszernek megfelelően számos veszélyforrás létezik, melyek az általuk fenyegetett folyamatokra különbözőképpen hatnak és mindezeknek megfelelően működésfolytonossági szempontból eltérő kockázatokat jelentenek. A veszélyforrások érvényre jutásakor jelentkező negatív hatás, illetve kár értékelése gyakran azért problematikus, mert a veszélyforrások számottevő része olyan negatív hatást válthat ki, amely igen nehezen számszerűsíthető. (Például az informatikai rendszerek működésképtelensége miatt sikertelenül végződő békefenntartó művelet pénzügyi következményei nem határozhatók meg, ugyanakkor a hatás jelentősnek tekinthető.)

A működésfolytonosságot általában fenyegető veszélyforrások nem mindegyike jelenik meg egy–egy konkrét működési folyamat esetén.[34] Egy-egy konkrét esetben a körülmények pontos figyelembe vételével határozhatók meg azok a konkrét veszélyforrások, amelyek az adott esetben relevánsnak tekinthetők.

[34]Az informatikai biztonságot általában fenyegető veszélyforrásokat részletesen felsorolja az Informatikai Tárcaközi Bizottság 8. sz. ajánlása, az Informatikai biztonsági módszertani kézikönyv, Budapest, 1994. http://www.itb.hu/ajanlasok/a8/html/a8_3-3.htm

A működésfolytonosság biztosítása a szervezetek alapvető funkcionalitásait megvalósító erőforrásokon túlmenő erőforrásokat igényel. [1] Mivel általában igaz, hogy bármely védelmi, illetve polgári szférabeli, továbbá a kritikus infrastruktúrák területén működő szervezet korlátozott erőforrásokkal rendelkezik, az alkalmazható védelmi intézkedésekhez rendelhető pénzügyi erőforrások is limitáltak. Emiatt nem lehetséges valamennyi releváns veszélyforrás ellen védelmi intézkedést alkalmazni. Így a kritikus folyamatokat fenyegető releváns veszélyforrások közül ki kell választani azokat, amelyek a legnagyobb kockázatokat jelentik és ezek kezelésére kell konkrét védelmi intézkedéseket kialakítani. Ennek megfelelően kockázatelemzés alkalmazásával el kell végezni az egyes veszélyforrások priorizálását és ez alapján meg kell határozni azon veszélyforrások körét, amelyekre védelmi intézkedések megvalósíthatók. A kiválasztás az egyes veszélyforrások okozta kockázatok elemzésén keresztül történhet meg. [11]

A sebezhetőségi ablakokon túlmenő kiesések a veszélyforrások ellen alkalmazott védelmi intézkedések segítségével küszöbölhetők ki, illetve csökkenthetők egy elfogadható szintre, azaz a működésfolytonosság biztosítását megfelelő védelmi intézkedésekkel lehetséges elérni. Az e célból alkalmazott védelmi intézkedések egyrészről arra irányulhatnak, hogy csökkentsék az egyes veszélyforrások érvényre jutását, másrészről pedig arra, hogy a veszélyforrások érvényre jutásakor csökkentsék a bekövetkező kár, veszteség értékét.

Az előzőekből következik, hogy a kockázatelemezés eredményeinek figyelembe vételével végrehajtott konkrét védelmi intézkedések sem garantálhatják a folyamatos működést, így mindenképpen számolni kell megmaradó (általában kisebb jelentőségű) kockázatokkal. Mindezek miatt fel kell készülni arra, hogy a folyamatok megszakadása a megtett védelmi intézkedések ellenére mégis bekövetkezik. Az ilyen esetek, katasztrófa helyzetek bekövetkezésére előre fel kell készülni, ennek megfelelően olyan terveket kell készíteni, amelyek a kiesések esetleges bekövetkezésekor közvetlenül alkalmazhatók.

Az előzőeken túlmenően nyilvánvalóan szükséges, hogy a szervezeti egység vezetői, parancsnokai és beosztottai a számukra szükséges szinten ismerjék a működésfolytonosság biztosítása érdekében rájuk háruló feladatokat, továbbá, hogy a működésfolytonosság érdekében végrehajtott intézkedések időszakonként tesztelésre kerüljenek.

A szervezeti folyamatok, külső és belső körülmények, releváns veszélyforrások

költségek stb. folyamatosan változnak. Emiatt a fenti lépések végrehajtásával az adott szervezet működésfolytonossági kérdései nem lesznek végérvényesen megoldva. Időről-időre felülvizsgálatok elvégzése szükséges és a megváltozott körülményeknek megfelelően módosításokat kell végrehajtani.

Mindezeknek megfelelően a működésfolytonosság megfelelően kidolgozott működésfolytonossági menedzsment terv alapján valósítható meg, amelynek a következő összetevőkből kell állnia:

1. Helyzetfeltárás – a kritikus folyamatok, sebezhetőségi ablakok meghatározása.
2. A kritikus folyamatokat fenyegető releváns veszélyforrások kiválasztása.
3. Az egyes veszélyforrások okozta kockázatok elemzése és ez alapján a kezelendő veszélyforrások kiválasztása, illetve a védelmi feladatok kijelölése.
4. A kezelendő veszélyforrásokra vonatkozó konkrét védelmi intézkedések kidolgozása.
5. Katasztrófa helyzet esetén alkalmazható tervek készítése.
6. A működésfolytonossághoz kapcsolódó kiképzés, felkészítés, tesztelés, illetve folyamatos aktualizálásának folyamata.

A rögzített összetevők egyúttal megadják a működésfolytonosság gyakorlati megvalósításának lépéseit is: a lépéseket egymás után végrehajtva egy szervezet működésfolytonossági terve a gyakorlatban is kialakítható. [12]

Az egyes szervezetek kritikus működési folyamatainak fenntarthatóságát döntően befolyásolja az alkalmazott informatikai rendszerek megfelelő rendelkezésre állása és megfelelő működése. Ez a függőség egyaránt fennáll a védelmi és polgári szférában, így a kritikus infrastruktúrák területén is, mind a normál, rutinjellegű, mindennapi, gyakran ismétlődő folyamatok esetén, mind pedig művelet-orientált környezetben. Mind a védelmi szféra, mind pedig a művelet-orientált környezet rendelkezik néhány olyan sajátossággal, amelyek megnyilvánulnak a működésfolytonosság megvalósításának kérdéskörében is.

## 3.2 A helyzetfeltárás védelmi szférabeli jellemzői

A helyzetfeltárás során az adott szervezet valamennyi működési folyamatát áttekintjük, és kiválasztjuk közülük azokat, amelyek az adott szervezet alapvető funkcionalitásaink biztosításához szükségesek. [72] A folyamatok áttekintésének megfelelő

folyamatmodellezési eljáráson kell alapulnia, melyet korszerű informatikai eszközök felhasználásával célszerű elvégezni.[35]

A szervezet folyamatmodelljének kialakításához általában szemléket, bejárásokat szükséges végrehajtani, interjúkat szükséges lefolytatni kompetens személyekkel, illetve a szervezet folyamatainak szempontjából releváns dokumentumok tanulmányozására van szükség.

Egy adott szervezeti egység folyamatai közül nem feltétlenül tekinthető mindegyik kritikusnak. (Például nyilvánvalóan nem tartozik egy alakulat kritikus folyamatai közé az a folyamat, amely a beosztottak üdültetésére fókuszál.) A kialakított folyamatmodell segítségével meghatározhatók a kritikus folyamatok, ezek azok, amelyek az adott szervezet alapvető funkcionalitásainak biztosításában meghatározóak.

A helyzetfeltárás során meg kell határozni az egyes kritikus folyamatokhoz tartozó sebezhetőségi ablakokat. Ez gyakran egyértelműen következik fennálló törvényi kötelezettségekből, érvényes szerződésekből, ilyenek hiányában kompetens szakemberek szakvéleménye határozhatja meg.[36] (Az üzleti szférában a sebezhetőségi ablakot tipikusan az ebből származó költségek nagysága, illetve a versenytársak közötti versenyhelyzet határozza meg.) A sebezhetőségi ablakok meghatározásakor figyelembe kell venni, hogy a sebezhetőségi ablak nagysága és az ezzel járó költségvonzat között fordított arányosság létezik, azaz a sebezhetőségi ablak indokolatlanul rövidre való megválasztása indokolatlanul nagy költségekkel járhat.

A helyzetfeltárás alapelvei és módszerei teljesen általánosak, ebben a kérdésben sem a védelmi szféra, sem a művelet-orientált környezet nem igényel sajátos eljárásokat.

## 3.3 A védelmi szférabeli folyamatok működését veszélyeztető veszélyforrások és védelmi feladatok

### 3.3.1 A veszélyforrások és védelmi feladatok általános áttekintése

A működésfolytonosság biztosítására vonatkozó meggondolásoknak a lehetséges veszélyforrások áttekintésén kell alapulnia. [65] Az előzőeknek megfelelően, egy-egy konkrét esetben az összes elképzelhető veszélyforrás közül ki kell választani azokat, amelyek az adott folyamat szempontjából lényegesnek tekinthetők. Működésfolytonosság szempontjából veszélyforrásként kell figyelembe vennünk

[35] A szervezeti folyamatok modellezésére számos szoftvereszköz létezik, pl. az IDS Shceer AG terméke, az ARIS Smart Path.
[36] Például a DELPHI módszer alkalmazásával.

mindazon tényezőket, amelyek a kritikus működési folyamatok megszakadását okozhatják. A veszélyforrások áttekintése annál is inkább célszerű, mert a veszélyforrások számottevő részében nem feltétlenül a védelmi eljárás kidolgozása jelenti az alapproblémát, sokkal inkább a veszélyforrás létezésének tudatosulása. Tipikus, hogy egy-egy veszélyforrás felismerése automatikusan kijelöli a kiküszöbölése érdekében végrehajtandó védelmi feladatot, azaz az adott veszélyforrás kapcsán elérendő célt. (Például, ha veszélyforrásként megjelenik a hiányos, illetve nem létező dokumentáció, akkor az ellene alkalmazható védelmi feladat is nyilvánvaló: el kell készíteni a megfelelő dokumentációt.)

Az 1/4. ábrán bemutatott rendszer egy általános megközelítés abban az értelemben, hogy az esetek mindegyikében számba veendő veszélyforrásokat tartalmazza. Így alkalmas mind a védelmi szférabeli szervezetek folyamataira, értelemszerűen a kritikus infrastruktúrák területére is, mind pedig a művelet-orientált tevékenységrendszerekre vonatkozó működésfolytonossági kérések tárgyalásának támogatására. A rendszer a veszélyforrások egyfajta rendszerezését is tartalmazza azzal, hogy a következő kategóriákba sorolja őket: fizikai, logikai, szervezeti és működési valamint az életciklushoz köthető veszélyforrások.[37]

A fizikai és a logikai jellegű veszélyforrásokat és az ellenük alkalmazható védelmi módszereket számos irodalom együtt kezeli, mint technikai jellegű tényezőket. [67] Célszerű azonban ezt a kategóriát a fentiek szerint két részre osztani, ugyanis erősen elkülönülnek egymástól azok a veszélyforrások, amelyek az informatikai rendszerek fizikai, illetve logikai elemeire lehetnek hatással. A fizikai jellegű fenyegetések bekövetkezésekor tipikusan az informatikai rendszer fizikai összetevői (hardver elemek, kiszolgáló infrastruktúra stb.) semmisülnek meg vagy károsodnak, ugyanakkor a logikai jellegű fenyegetések a rendszer logikai elemeire (adatbázisok, programok stb.), illetve ezek működésre vonatkozóan válthatnak ki negatív hatást.

Az egyes veszélyforrások nem minden esetben különülnek el teljes mértékben egymástól, több veszélyforrás esetén előfordul, hogy az illető veszélyforrás nem csak egyetlen csoportba lenne sorolható. Például a nem létező, hiányos vagy használhatatlan dokumentáció egyaránt megjelenhet mint fizikai, logikai, esetleg szervezeti veszélyforrás, aszerint, hogy az informatikai rendszer fizikai, logikai elemeihez, vagy szervezeti folyamataihoz kapcsolódik.

[37] A releváns irodalom a veszélyforrásokat különböző szempontok szerint csoportosítja.

A működésfolytonosságot számos veszélyforrás fenyegeti. Ezek teljes körű felsorolására és tárgyalására azonban jelen értekezésben nem törekszünk. Ez nem is lenne lehetséges, mert léteznek olyan veszélyforrások is, amelyek – mivel bekövetkezésükre ez ideig nem volt példa - létezése általánosan nem tudatosult, ugyanakkor a működési folyamatok megszakadását okozhatják.[38]

A veszélyforrások értékelésekor mindenképpen érdemes figyelembe venni, hogy vannak olyan veszélyforrások, amelyek azzal a speciális tulajdonsággal rendelkeznek, hogy érvényre jutásukkor a negatív hatás nem azonnal jelentkezik, hanem a jelenség egy ideig észrevétlen marad, és csak később jelenik meg olyan szinten, ahol már a folyamatos működés megszakadását okozhatja.[39]

### 3.3.2 A veszélyforrások és védelmi feladatok rendszerezése

A továbbiakban az előző csoportosításnak megfelelően összefoglaljuk, és röviden értékeljük az 1/4. ábrán bemutatott rendszerben szereplő veszélyforrásokat, és kijelöljük a hozzájuk kapcsolódó védelmi feladatokat. Megvizsgáljuk továbbá, hogy melyek azok a veszélyforrások, és az érvényre jutásuk ellen alkalmazható védelmi feladatok, amelyek kifejezetten a védelmi szférabeli, illetve a kritikus infrastruktúrák területén történő működés, továbbá művelet-orientált esetben jelennek meg. Ennek megfelelően a következő kategóriákra térünk ki:

- fizikai veszélyforrások és védelmi feladatok;
- logikai veszélyforrások és védelmi feladatok;
- szervezeti és működési veszélyforrások és védelmi feladatok;
- életciklushoz kapcsolódó veszélyforrások és védelmi feladatok;
- sajátos veszélyforrások és védelmi feladatok művelet-orientált környezetben;
- sajátos veszélyforrások és védelmi feladatok a védelmi szférában.

### 3.3.3 Fizikai veszélyforrások és védelmi feladatok

A fizikai veszélyforrások az 1/4. ábrán bemutatott rendszernek megfelelően közvetlenül tipikusan az erőforrásokra fejthetik ki negatív hatásaikat, rajtuk keresztül befolyásolhatják a működésfolytonosságot. [65] Több csoportba sorolhatók: egy részük

[38] 2001. szeptember 11-e előtt valószínűleg sehol nem vették számba veszélyforrásként az objektumnak szándékosan nekivezetett nagyméretű utasszállító repülőgépet.
[39] Ezeket számos irodalom lappangó veszélyforrásoknak nevezi.

a földrajzi környezetből származik, természeti, illetve technikai katasztrófa formájában jelenik meg.

Természeti jellegű veszélyforrás például a földrengés, a földcsuszamlás, az árvíz, a vízbetörés, a szélvihar, a szélsőséges időjárás, a villámcsapás stb. Kifejezetten a katonai szférára jellemző veszélyforrásként vehető figyelembe az extrém környezeti feltételek közötti működés (pl. sivatagi környezet, szélsőséges hőmérséklet stb.).

Technikai jellegű veszélyforrás a saját, illetve a szomszédos szervezetnél történő robbanás, tűz, veszélyes gázképződés, stb. Ide tartoznak az ellenséges támadások, terrorcselekmények okozta fizikai veszteségek, a közlekedési katasztrófák és a kommunális ellátással kapcsolatos katasztrófák (pl. gázömlés, nagyfeszültségű vezeték szakadás, víznyomócső törés, informatikai, távközlési, erősáramú becsatlakozás kiesése, nukleáris és vegyi szennyezés stb.).

A földrajzi környezetből származó veszélyforrások közös jellemzője, hogy bekövetkezésükkor általában igen nagy kár következik be, továbbá, hogy az egyes szervezetek saját eszközeikkel nem, vagy csak korlátozottan képesek ellenük védekezni (például villámcsapás). Védelmi feladatként ez esetben a kárkövetkezmények mérséklésére irányuló reaktív intézkedések alkalmasak, ezeket a feladatokat tipikusan a katasztrófa tervek akciótervei fedik le, esetleg kockázatáthárítást (biztosítás) alkalmaznak.

A fizikai veszélyforrások más része jogosulatlan fizikai hozzáférésként jelentkezik. E körben aktív fizikai hozzáférésnek tekinthetők az illetéktelen (esetleg erőszakos) behatolások, a fegyveres támadások, terrorcselekmények. Az aktív fizikai hozzáféréseket olyan, ugyancsak fizikai veszélyforrások támogatják, amelyek mint a nem megfelelő fizikai védelmi intézkedések (nem megfelelő őrszolgálat, nem kielégítő mechanikai védelem, nem létező, nem működő beléptető, mozgásérzékelő, figyelő rendszer stb.) jelentkeznek. Ide sorolható az őrizetlenül hagyott munkahelyek problémája is.

Az aktív fizikai hozzáférések megakadályozása különböző védelmi feladatokat jelent. Ezek közé kell sorolnunk, az érintett objektumok helyének megfelelő megválasztását, az integrált belépés és mozgás ellenőrző, tűzvédelmi, gázvédelmi, stb. rendszerek telepítését, a különböző mechanikai védelmek kialakítását, valamint az élőerős védelem alkalmazását.

A jogosulatlan hozzáférések körében az aktív fizikai hozzáférések mellett léteznek passzív fizikai hozzáférések is. Ezek közvetve hathatnak a működésfolytonosságra: az illegálisan megszerzett információ az ellenséges támadások, terrorcselekmények, egyéb rosszhiszemű tevékenységek lehetőségét teremti meg, illetve sikerességének esélyét növeli. Passzív fizikai hozzáférések az elektromágneses és akusztikai hozzáférések és lehallgatások. Ilyenek például a telefonbeszélgetések és a számítógépes kommunikáció lehallgatását lehetővé tevő eszközök, a mikrofonpuska, a lézerpuska, a képernyők kisugárzásán alapuló eszközök, valamint a sugárzott és vezetett zavaró jelek alkalmazása. Ide sorolhatók a nem megfelelően elhelyezett, nem megfelelően védett eszközök (rálátási, lehallgatási lehetőség), illetve a felügyelet nélkül hagyott erőforrás elérési lehetőségek is.

A passzív fizikai hozzáférések megakadályozása védelmi feladatként az akusztikus és elektromágneses lehallgatás[40] elleni védelmek (például árnyékolások) alkalmazását jelöli ki. Ide tartozik az eszközök (különösen a kritikus eszközök) helyének megfelelő megválasztása és fizikai védelme (például megfelelően kialakított és beléptető rendszerrel ellátott szerverszobák, zárt kábelrendezők kialakítása stb.). Hasonlóképpen ide tartoznak azok a szabályzatok és eljárások, amelyek az objektumokban a személyek fizikai mozgását és a munkavégzés körülményeit szabályozzák.

Az előzőeken túlmenően fizikai veszélyforrásként jelenik meg a fizikai rendelkezésre állás megszakadása, amely többnyire az eszközök meghibásodásából, megrongálódásából, megsemmisüléséből, nem megbízható eszközök használatából, a nem megfelelő légállapotból, illetve a tűz bekövetkezéséből, valamint az infrastruktúra, az energiaellátás és a távközlés zavaraiból származhat.

A fizikai rendelkezésre állás megszakadása megfelelő minőségű eszközök alkalmazásával, megfelelő környezet kialakításával, illetve tartalékok képzésével akadályozható meg.

Ugyancsak fizikai veszélyforrásként vehetjük számba a fizikai összetevőkre vonatkozó dokumentáció hiányát, hibás, hiányos, nem naprakész állapotát. Az ide tartozó védelmi intézkedéseknek mindezek kiküszöbölésére kell irányulniuk.

### 3.3.4 Logikai veszélyforrások és védelmi feladatok

A logikai veszélyforrások az 1/4. ábrán bemutatott rendszernek megfelelően közvetlenül

[40] A kompromittáló kisugárzás tanulmányozására és a védelem kialakítására nemzetközileg elterjedt kifejezésként a TEMPEST kifejezés használatos.

egyaránt fenyegethetik az erőforrásokat, illetve a szervezet és irányítás megvalósulását, ezeken keresztül lehetnek negatív hatással a működésfolytonosságra. A logikai veszélyforrások leginkább jellemző kategóriái a következők: jogosulatlan logikai hozzáférések, a folyamatos működés megszakadása, az integrált információrendszer hiánya, rosszindulatú szoftver hatása, valamint a logikai rombolás és a megfelelő dokumentáció hiánya. Jellemző, hogy számottevő részük csak közvetve hat a működésfolytonosságra: az illegálisan megszerzett információ az ellenséges támadások, terrorcselekmények, egyéb rosszhiszemű tevékenységek lehetőségét teremti meg, illetve sikerességének esélyét növeli.

A jogosulatlan logikai hozzáférések veszélyforrásai a megfelelő belépés ellenőrzés (jelszó használati rendszer, biometriai azonosítás stb.) hiányaként, nem megfelelő jogosultság használataként, valamint a nem megfelelő naplózásként jelentkezik. Ide tartoznak a különböző kriptográfiai támadások is, amelyeket a titkosításhoz felhasznált gyenge algoritmusok, illetve gyenge kulcsok segítenek.

A jogosulatlan logikai hozzáférések megakadályozása érdekében preventív védelmi feladatként megfelelően kialakított logikai hozzáférési eljárások (például megfelelően használt jelszavakon alapuló hozzáférések) kialakítása, illetve az illetéktelen szoftver telepítések megakadályozása jelentkezik. Ezek közé a feladatok közé tartoznak az IDS[41] rendszer működtetése [68], valamint a kriptográfiai rendszerek alkalmazása is. Ebben a kategóriában reaktív intézkedésként értékelhető a naplózó rendszerek használata is.

A folyamatos működés megszakadását a nem megfelelő alternatív háttérmegoldás [69] alkalmazása, illetve a nem megfelelőképpen kidolgozott vagy végrehajtott mentések, esetleg a mentések hiánya okozhatja. Ugyancsak a folyamatos működés megszakadását idézheti elő, ha az erőforrások kisajátíthatók, használatuk nincs korlátozva, esetleg tervezési hiba vagy a fejlesztés elmaradása, illetve a szűkös anyagi erőforrások miatti elégtelen rendelkezésre álló kapacitás.

A folyamatok kiesésmentes működését a támogató informatikai rendszer redundáns megvalósításával lehet elősegíteni (hideg, meleg, forró, illetve katasztrófa tűrő tartalék), ugyancsak ezt alapozhatja meg az átgondolt mentési eljáráson alapuló rendszeres mentések végrehajtása is. Az erőforrások használatának megfelelő szabályozásával, korlátozásával, átgondolt tervezésekkel, fejlesztésekkel ugyancsak csökkenthető a

[41] Intruder Detection System – behatolás ellenőrző rendszer

folyamatos működés megszakadásnak valószínűsége.

Amennyiben egy szervezetben egymástól független, sziget megoldásokon keresztül valósul meg az informatikai rendszer, úgy nincs egységes informatikai szakmai irányítás, sok esetben a szigetek egymástól elkülönült szervezetek hatáskörében üzemelnek, illetve fejlesztik őket. Az egyes szigetek közötti információcsere problematikus, inkonzisztenciák léphetnek fel, továbbá ez esetben nem valósul meg az egyenszilárdság elve, azaz bizonyos szigetekre a többieknél nagyobb kockázatok lesznek jellemzők. Mindezek az adott szervezethez tartozó egységes, integrált informatikai rendszer alkalmazásával küszöbölhetők ki.

A rosszindulatú szoftvereknek többféle változata van, ezek különböző veszélyforrásokat jelenthetnek. Legfontosabb változataik a következők: vírusok, trójai faló programok, programférgek, logikai bombák, hátsó ajtók, baktériumok, betárcsázó programok valamint adathalászatra[42] alkalmas programok. A rosszindulatú programok között vannak olyanok, amelyek csak jelentéktelen károkat képesek okozni, ugyanakkor léteznek közöttük olyanok is, amelyek az érintett informatikai rendszer teljes kiesését okozhatják. Az adott szervezetnél előforduló rosszindulatú szoftverek elleni védekezés kapcsán fellépő hiányosságok annyiban jelentenek veszélyforrásokat, amennyiben a rosszindulatú szoftverek károkozásait lehetővé teszik.

A rosszindulatú szoftverek ellen preventív védelmi feladatként olyan megoldások használhatók, amelyek megakadályozzák a rosszindulatú szoftver rendszerbe való bekerülését, ezáltal károkozás nem is következhet be. Reaktív védelmi intézkedésként a rosszindulatú szoftver eltávolítására alkalmas szoftverek használata, illetve mentésből való visszaállítás, esetlegesen újratelepítés jöhet szóba.

A logikai rombolás[43] mint veszélyforrás elsősorban logikai, de esetenként hardver veszélyeztetést is jelent. Ennek során sugárzott vagy vezetett zavaró jelekkel a támadó általában a tárolt információ megrongálására törekszik, ugyanakkor előfordulhat a hardver megrongálására történő törekvés is[44]. Ez esetben védelmi feladatként a vezetett jelek és tápellátások szűrése, az elektromágneses árnyékolás, a megfelelő földelési hálózatok kialakítása, valamint a sztatikus feltöltődés elleni védekezés jöhet szóba.

[42] 2006. őszén széles körű nyilvánosságot kapott az egyik hazai bankrendszer elleni adathalászat jellegű támadás.
[43] A logikai rombolást számos irodalom elektromágneses terrorizmusnak nevezi.
[44] Mindezek miatt számos irodalom a sugárzott vagy vezetett jelekkel történő veszélyeztetéseket a fizikai veszélyforrások közé sorolja.

Ugyancsak logikai veszélyforrásként vehetjük számba a logikai összetevőkre vonatkozó dokumentáció hiányát, hibás, hiányos, nem naprakész állapotát. Az ide tartozó védelmi intézkedéseknek mindezek kiküszöbölésére kell irányulniuk.

### 3.3.5 Szervezeti és működési veszélyforrások és védelmi feladatok

A szervezeti és működési veszélyforrások az 1/4. ábrán bemutatott rendszernek megfelelően közvetlenül egyaránt fenyegethetik a működésfolytonosság mindhárom alappillérét, ezeken keresztül valósulhat meg áttételes negatív hatásuk a működésfolytonosságra. Egy részük nem közvetlenül hat a működésfolytonosságra, a közvetett hatás abban nyilvánul meg, hogy az illegálisan megszerzett információ az ellenséges támadások, terrorcselekmények, egyéb rosszhiszemű tevékenységek sikerének valószínűségét növeli.

Ezen veszélyforrások az előzőekhez hasonlóan több kategóriába sorolhatók. Ezek a következők: az „ad hoc” szervezeti működés, az integrált biztonsági szervezet hiánya és gyengeségei, a titokvédelmi hiányosságok, az iratkezelési hiányosságok, a harmadik féllel kötött szerződések gyengeségei, valamint a humán erőforrásokhoz kapcsolódó veszélyforrások. [11]

„Ad hoc” szervezeti működés esetén a szervezetre jellemző, hogy szervezeti egységekben, illetve rendszerekben gondolkodik, nem pedig működési folyamatokban. A szervezet működése nincs leképezve jól definiált folyamatokra, a működési folyamatok dokumentálása, modellezése nem történik meg, azok még a vezetés számára sem átláthatók, továbbá, hogy nincsenek jól definiált hatáskörök és felelősségek.

Az integrált biztonsági szervezet hiánya és gyengeségei közé a következő veszélyforrások tartoznak: Nem létezik integrált biztonsági szervezet, a vagyon és adatbiztonság egymástól függetlenül működik, illetve a funkciók összekeverednek, az adatvédelem és adatbiztonság nem megfelelően szétválasztott, valamint, hogy nincsenek megfelelő biztonsági ellenőrzések. Ide tartoznak továbbá a biztonsági szervezetek (pl. tűzvédelmi, polgári védelmi) hiánya, gyengeségei valamint a biztonsággal kapcsolatos dokumentumok hiánya (Biztonsági Stratégia, Biztonsági Politika, Biztonsági átvilágítás, Katasztrófaterv, Működésfolytonossági terv, Informatikai

Biztonsági Szabályzat stb.)[45], a szabályozások hiányosságai, ellentmondásai, a szabályok be nem tartása. Hasonlóképpen ide tartozó veszélyforrásnak tekinthető, ha a munkakörök és a szakmai kompetencia nem teljesen függ össze, valamint ha a munkaköri leírás és a tényleges tevékenység nem egyezik meg, a munkakörök szétválasztása nem megfelelő[46], azaz ugyanazon személy lát el egymással össze nem egyeztethető munkaköröket. Ugyancsak ide sorolható a nem megfelelő színvonalú kiképzés, felkészítés is.

Mindezen veszélyforrások ellen megfelelően kialakított szervezettel, a felelősségek és hatáskörök pontos meghatározásával, a működési folyamatok pontos definiálásával lehetséges védekezni.

A titokvédelmi hiányosságokhoz tartozó veszélyforrások abban nyilvánulhatnak meg, hogy nincsenek osztályozva titokvédelmi szempontból az adatok, alkalmazások, eszközök, helyiségek, illetve, hogy a titokvédelmi beosztott elhelyezkedése a szervezeti hierarchiában nem megfelelő.

Az iratkezelési hiányosságok annyiban jelennek meg veszélyforrásként, amennyiben nincs szabályozva az elektronikus íratok kezelése, előállítása, megsemmisítése, archiválása.

Harmadik féllel kötött szerződések gyengeségeit jelentik azok a hiányosságok, amikor a szerződések (fejlesztői, szállítói, karbantartási, üzemeltetői stb.) nem tartalmaznak biztonsági garanciákat, és a tevékenység megszakadására vonatkozóan a harmadik fél nem vállal garanciát.

A titokvédelmi és iratkezelési hiányosságok valamint a harmadik féllel kötött szerződések gyengeségei a jogszabályi környezet figyelembe vételével, a belső szabályozók megfelelő kialakításával és betartásával küszöbölhetők ki.

A humán erőforrások kétféle megközelítés szerint is veszélyforrást jelenthetnek. Egyrészről a humán erőforrások rendelkezésre állása is sérülhet (sérülés, betegség, haláleset, túszejtés, sztrájk stb.), másrészről a humán erőforrások önmagukban is megjelennek mint veszélyforrások. Ez elsősorban a nem megbízható, nem lojális, nem megfelelően képzett, nem elegendő gyakorlattal rendelkező munkaerő alkalmazásában nyilvánulhat meg. Veszélyforrást jelenthet, ha a szervezettől eltávozó dolgozók,

[45]Az Állami Számvevőszék Módszertan az informatikai rendszerek kontrolljainak megismeréséhez c. anyaga Az informatikai környezet és tevékenyég megismerése c. fejezetében (19-20.o) iránymutatást ad a szükséges dokumentumokra vonatkozóan. (http://www.asz.hu/ASZ/www.nsf/HTML/43240/$FILE/IT_ell_modsz_2004_02.pdf)

[46]Az angol nyelvű irodalomban erre vonatkozóan tipikusan a „seggregation of duties” kifejezést használják.

parancsnokok és beosztottak hozzáférései megmaradnak (belépő kártya, account, kulcs stb.) és a munkatársak, parancsnokok és beosztottak nem kapnak értesítést a távozás tényéről. Ugyancsak humán veszélyforrásnak tekinthetjük a nem megfelelő szintű biztonsági tudatosságot is.

A humán erőforrásokhoz kapcsolódó védelmi feladatok ezeknek megfelelően két kategóriába sorolhatók. Az első kategóriába azok az intézkedések tartoznak, amelyek a humán erőforrások kiesésének esetére vonatkoznak és segítségükkel a kiesett kompetencia pótolható. A másik kategóriába tartozó intézkedések arra irányulnak, hogy a rendelkezésre álló munkaerő megfelelően képzett, elegendő gyakorlattal rendelkező legyen és a szervezet iránti lojalitása is megfelelő legyen. A felvételi és elbocsátási eljárást szabályozottan kell végrehajtani és képzésekkel kell fokozni a biztonsági tudatosságot.

### 3.3.6 Az életciklushoz kapcsolódó veszélyforrások védelmi feladatai

Az életciklushoz kapcsolódó veszélyforrások az 1/4. ábrán bemutatott rendszernek megfelelően közvetlenül egyaránt fenyegethetik az erőforrásokat, illetve a szervezet és irányítás megvalósulását, ezeken keresztül befolyásolhatják a működésfolytonosságot. Az informatikai rendszerek életciklusa négy összetevőből áll.[47] Ezek a következők: fejlesztés és beszerzés, átadás-átvétel, üzemeltetés, selejtezés. Az életciklus valamennyi szakaszában felmerülhetnek olyan veszélyforrások, amelyek hatással lehetnek a működésfolytonosságra.

Fejlesztés/beszerzés szakaszban a következő veszélyforrások jelentkeznek: A fejlesztési cél nem tartalmaz a működésfolytonosságra vonatkozó követelményeket, nincs elkülönült fejlesztő rendszer és személyzet, a szállító nem nyújt megfelelő biztonsági garanciákat a szállított termék fenyegetettség mentességére vonatkozóan. Veszélyforrást jelent továbbá az elterjedt, szabványos szoftverek beszerzése és alkalmazása, mivel ezek biztonsági problémái általában széles körben ismertek, így a rendelkezésre állásuk akadályozásához felhasználható információ gyakorlatilag bárki számára elérhető.

Átadás-átvételkor veszélyforrást jelent, ha a biztonsági követelményrendszer ellenőrzése hiányzik, valamint ha a speciális hozzáférések (a programozók speciális jogosultságai, pl. hátsó ajtók) megmaradnak.

[47] A COBIT szerinti megközelítés figyelembe vételével.

Üzemeltetés alatt tipikus veszélyforrás, hogy a biztonságkritikus munkakörök nincsenek szétválasztva, illetve, hogy fejlesztések folynak az éles rendszeren továbbá, hogy a biztonsági események feltárása, értékelése nem történik meg. Ide is besorolhatók a harmadik féllel kötött szerződések gyengeségei valamint a szabályozások hiányosságai.

A selejtezési szakaszban veszélyforrásként a nem megfelelően végrehajtott selejtezési eljárások és a jól definiált selejtezési rend hiánya jelentkezhet. Mindezek közvetetten veszélyeztethetik a működésfolytonosságot: az illegálisan megszerzett információ az ellenséges támadások és más rosszhiszemű tevékenységek lehetőségét teremti meg, illetve sikerességének esélyét növeli.

Az életciklushoz kapcsolódó veszélyforrások egyértelműen kijelölik a velük szemben végrehajtandó védelmi feladatokat: a feladatoknak mindezek megszüntetésre kell irányulniuk.

### 3.3.7 A veszélyforrások és védelmi feladatok sajátosságai a védelmi szférában, illetve a kritikus infrastruktúrák területén

Bár a 1.3.2 pontban rögzítetteknek megfelelően a védelmi és a polgári szféra erős konvergenciája figyelhető meg, a működésfolytonosságot fenyegető veszélyforrások figyelembe vétele a védelmi és a polgári szférában, ennek megfelelően a kritikus infrastruktúrák területén némiképpen különböző módon valósul meg. [65] Ennek elsősorban tradicionális okai vannak. A védelmi szféra kultúrájában a fizikai, valamint a szervezeti és működési veszélyforrások figyelembe vétele hosszú idő óta fontos tényezőként szerepel. E szférában védelmi feladatként az egyes objektumok fizikai helyének megválasztása, az objektumok fizikai védelme, a szervezet kialakítása, a szabályozások megléte, a személyzet megválasztása, a személyzet biztonsági tudatosságának biztosítása szempont volt már az informatikai rendszerek megjelenése előtt is. Hasonlók mondhatók el az életciklushoz kapcsolódó veszélyforrásokról is.

A logikai veszélyforrások tekintetében jóval kisebb különbségek tapasztalhatók. Ennek elsősorban az az oka, hogy a logikai veszélyforrások túlnyomó többsége az informatikai rendszerek elterjedése kapcsán csak az utóbbi évtizedekben jelent meg. Ez a folyamat a védelmi és a polgári szférában, illetve a kritikus infrastruktúrák területén gyakorlatilag azonos időszakban zajlott le, és az azóta eltelt idő nem volt elegendő arra, hogy a kezelésükhöz szükséges kultúra megfelelő szinten kialakuljon. A logikai veszélyforrások ennél fogva új kategóriaként jelentek meg, melyekre jellemző, hogy esetükben az eredményes támadáshoz nem szükséges az objektumokat megközelíteni, nem kell oda

fizikailag behatolni.

A hálózatközpontú hadviselés megjelenésével a logikai veszélyforrások az ún. kibertérben jelennek meg. *„…az információs korban a hadviselés egy újabb hadszíntérrel, más szóhasználattal egy újabb dimenzióval bővült, a kibertérrel. Ebben a hadviselésben nincs katona és civil. Aki a kommunikációs eszközöket használja, üzemelteti, aki a hálózatok szolgáltatásait igénybe veszi, vagy a fenntartásukon dolgozik, ugyanúgy részese, célpontja, vagy végrehajtója ennek a különös harcnak, amihez nem kell már robbanóanyag, de hatásában sokkal pusztítóbb lehet.*" [10]

Ezen a területen a védelmi szférát érintő releváns veszélyforrásként értékelhető a COTS [24] (Commercial Off The Shelf - a kereskedelmi forgalomból beszerezhető "polcról levehető" és azonnal üzembe helyezhető termékek) rendszerek használata (például operációs rendszerek, GPS [73] stb.). Hasonlóképpen veszélyforrásként jelenik meg, hogy a védelmi szféra hálózatai (pl. SIPRNET[48], NIPRNET[49]) ugyanarra az internet-technológiára épülnek, amely a polgári szférában világméretű elterjedtséggel jellemezhető. Ez egyrészről azt eredményezi, hogy a rendszerek széles körben ismertek, másrészről pedig azt, hogy ezzel összefüggésben a hibáik, gyenge pontjaik is publikusak, ezáltal a rendszerek könnyebben támadhatók.

Mindezek miatt a logikai veszélyforrások kezeléséhez kapcsolódó védelmi feladatok kijelölése az általános szempontokon túlmenően nem tartalmaz speciális szempontokat.

A polgári szférához, így a kritikus infrastruktúrák területén történő működéshez képest a védelmi szférában lényeges különbség mutatkozik a kockázatáthárítás kérdésében is. A normál, mindennapi tevékenységek esetén a polgári szférában a kiesések okozta károk kezelésének legutolsó lehetősége a kockázatáthárítás, azaz megfelelő biztosítás kötése. A védelmi szférában ennek gyakorlati jelentősége nincs, a kockázatáthárítás mint védelmi tevékenység ez esetben általában nem megvalósítható. Különösen igaz ez a védelmi szférabeli művelet-orientált jellegű tevékenységekre. Nehezen képzelhető el ugyanis, hogy lenne olyan biztosító társaság, amely hajlandó lenne a művelet céljának el nem érése esetére (például egy sikertelen békekikényszerítő művelet) biztosítási konstrukciót ajánlani. Ez esetben a felhasznált erőforrásokra vonatkozó biztosítások elképzelhetők, azonban ezek pótlása általában önmagában nem feltétlenül biztosítja a kitűzött cél elérését.

[48] Secret Internet Protocol Router Network
[49] Unclassified but Sensitive Internet Protocol Router Network

A veszélyforrások védelmi szférában történő számbavételére számos példa található. A 90-es években kiadott Magyar Honvédség Informatikai Szabályzata [55] közvetlenül és közvetve érinti a működésfolytonosságot érintő veszélyforrásokat. A veszélyforrások szisztematikus felsorolása, csoportosítása ugyan nem szerepel benne, a felsorolt védelmi eljárások meghatározása azonban nyilvánvalóan a veszélyforrásokból kiindulva történt meg. A dokumentum a veszélyforrások fogalmát némiképpen más, az általános értelmezésnél szűkebb értelemben használja. Bár a fogalom pontos definíciója az anyagban nem szerepel, a 198. pontban a számítástechnikai titokvédelmi felelős jogai és kötelességei között szerepel a következő kitétel: „*a veszélyforrások körének és változásainak vizsgálata*”. A szövegkörnyezetből kitűnik, hogy itt a veszélyforrások fogalom korlátozott értelemben használt, ugyanis kifejezetten azokra a veszélyforrásokra vonatkozik, amelyek a bizalmasság kategóriáját sértik.

A dokumentumban közvetve is érintettek bizonyos veszélyforrások. Erre vonatkozóan számos példa található. Külön alfejezet foglalkozik például a számítógépes vírusok elleni védelemmel (200-201. pont), ebből következik, hogy a vírusok, mint veszélyforrások lettek figyelembe véve. A vírusokhoz hasonlóképpen a tűz is veszélyforrásként szerepel, erre utal a „Tűzvédelem” c. alfejezet (202-205. pont). Az „*Egyéb védelem*” (206-208. pont) alfejezetben több olyan kategória létezik, amely egyértelműen arra utal, hogy a kidolgozást bizonyos veszélyforrásokból kiindulva végezték el. Ilyenek például „*az elektronikai felderítés elleni védelem*”, az „*elektronikai zavarvédettség*” *valamint a „komplex füst, tűz, víz, betörés, illetéktelen személy behatolását jelző készülék telepítése*”.

A Belügyminisztérium által megfogalmazott Informatikai Biztonsági Politika ugyancsak kezeli a működési folyamatokat fenyegető veszélyforrásokat. A 12/2004. (BK 12.) BM utasítás a hatálya alá tartozó szervezetek számára kidolgozott Informatikai Biztonsági Politika [74] céljának megfogalmazásakor hangsúlyozza, hogy összhangban kíván lenni az MSZ ISO/IEC 15408 [75] számú szabvánnyal[50] az MSZ ISO/IEC 17799 számú szabvánnyal, valamint a vonatkozó ITB 8. és 12. számú ajánlásokkal. [76] Az MSZ ISO/IEC 17799:2006 szabvány „*Kockázatfelmérés és kockázatjavítás*” című fejezetében kifejezetten a kockázatok kérdésével foglalkozik. Ennek megfelelően a korábban értékelt, a Belügyminisztérium által relevánsnak tekintett szabvány alkalmazása megköveteli az informatikai rendszerekre, illetve folyamatokra vonatkozó

[50] A Common Criteria magyar szabványként kiadott változata

veszélyforrások, fenyegetések számbavételét.

### 3.3.8 A veszélyforrások és védelmi feladatok sajátosságai művelet-orientált környezetben

A működésfolytonosság a normál, rutinjellegű, mindennapi folyamatok esetén azt jelenti, hogy az illető folyamatok megszakadás nélkül folynak, vagy maximálisan csak annyi időre esnek ki, amennyit a szervezet még jelentős veszteségek nélkül képes elviselni, azaz a kiesések nem haladják meg az adott működési folyamatokhoz tartozó sebezhetőségi ablakokat. Művelet-orientált környezetben a működésfolytonosság ezzel azonos módon értelmezhető. [25] Ebből az következik, hogy művelet-orientált környezetben a működésfolytonosság nem teljesül, ha akár a tervezett cél, akár a tervezett határidő nem teljesül, illetve a felhasználni szándékozott erőforrások jelentős túllépésére kerül sor.

Mindezek miatt mindazon veszélyforrások a művelet-orientált működést is veszélyeztethetik, amelyek a mindennapi folyamatos működés esetén előfordulhatnak. Ezeken túlmenően azonban léteznek olyan, a működésfolytonosságot fenyegető veszélyforrások, amelyek kifejezetten művelet-orientált környezetben jelennek meg. Ennek megfelelően a művelet-orientált környezetben megjelenő veszélyforrások a következő két csoportba sorolhatók be:

- normál, rutinjellegű, mindennapi, illetve gyakran ismétlődő tevékenységek működésfolytonosságát veszélyeztető veszélyforrások;
- kifejezetten a művelet-orientált működés működésfolytonosságát veszélyeztető veszélyforrások.

A mindennapi, rutin tevékenységek és a művelet-orientált működés között a fizikai és logikai veszélyforrások tekintetében alapvető különbségek nem állapíthatók meg, legfeljebb annyiban tapasztalhatók eltérések, amennyiben a művelet-orientált környezet esetében tipikusan nagyobb gyakorisággal fordulnak elő az extrém fizikai környezeti feltételek (tipikusan ipari, illetve terepi környezet) közötti működés (pl. extrém hőmérséklet, sivatagi környezet stb.).

Lényeges különbség van azonban a kétféle működés között a szervezeti és működési veszélyforrások tekintetében. Művelet-orientált esetben nem az általános, a szervezeti és működési szabályzatok határozzák meg a működést, hanem kifejezetten az adott feladat végrehajtására létrehozott szabályzatok. Ezekre vonatkozóan nyilvánvaló

elvárás, hogy nem mondhatnak ellent az érvényes szervezeti és működési szabályzatoknak. Komoly, gyakran nehezen áthidalható problémát jelentenek a feladat végrehajtásában részt vevő különböző szervezetek belső szabályzatainak ellentmondásai. A tervezett határidő betartását veszélyeztetheti, ha az ellentmondások feloldása elhúzódik, emiatt az adott feladatra vonatkozó szabályok kidolgozása nem történik meg időben.

Ugyancsak fenyegetheti a működésfolytonosságot a nem megfelelő, nem mindenre kiterjedő, hibás vagy nem megfelelő szinten elfogadott szabályzat is. Művelet-orientált környezetben kritikus lehet, ha a különböző változások nem megfelelőképpen vannak kezelve. Ennél fogva a jól definiált változáskezelési mechanizmus hiánya, illetve nem hatékony működése ugyancsak veszélyforrásként értékelhető. (A változáskezelési mechanizmusnak megfelelő működés a mindennapi, rutin tevékenységek esetén is fontos, de a gyorsan fellépő változtatási igények, valamint a betartandó határidők miatt művelet-orientált környezetben ez a tényező lényegesen nagyobb jelentőséggel rendelkezik.)

Léteznek olyan veszélyforrások is, amelyek a művelet-orientált működés életciklusához kapcsolódnak. Ezen a területen megjelennek olyan veszélyforrások is, amelyek a normál, mindennapi működés során gyakorlatilag nem lépnek fel. A művelet-orientált működés egy meghatározott életciklus követését, azaz a következő egymás utáni lépések végrehajtását jelenti:

- a cél kitűzése és a feladat meghatározása;
- tervezés és szervezés;
- végrehajtás;
- lezárás, átadás;
- értékelés.

Ezen lépések közül nyilvánvalóan az első háromhoz kapcsolódhatnak olyan veszélyforrások amelyek a működésfolytonosságot veszélyeztetik. A művelet-orientált működést veszélyeztetheti a cél és a feladat nem pontos definiálása. Előfordulhat, hogy a kitűzött cél ugyan teljesül, az előírt feladat az előírt határidőn belül, a tervezett erőforrások felhasználásával elvégzésre kerül, ugyanakkor a végső probléma mégsem oldódik meg. Például a cél nem megfelelő meghatározása miatt a katonai cél teljesül, azonban a végső politikai cél nem vagy nem megfelelő szinten valósul meg.

A tervezés során leginkább a nem megfelelő tervek jelennek meg veszélyforrásként. Így

a nem megfelelően kialakított szervezet, a nem megfelelően kiépített kapcsolatok más szervezetekkel, a teljesíthetetlen határidők, a nem elegendő kapacitással rendelkező erőforrások allokálása, illetve a megfelelő tartalékok hiánya jelentkezik a működésfolytonosságot fenyegető veszélyforrásként. Ugyancsak a tervezéshez kapcsolódó veszélyforrásként jelenhet meg, hogy az adott művelet-orientált tevékenység nincs megfelelően összehangolva a normál, mindennapi működéssel, esetleg más művelet-orientált módon végrehajtott tevékenységekkel.

A végrehajtás során megjelenő veszélyforrások döntő többségükben megegyeznek a normál, mindennapi működés során fellépőkkel. E lépés során azonban jelentős további veszélyforrásként jelentkezik az, hogy a művelet-orientált működés esetén az egyszeri végrehajtás miatt nem feltétlenül alkalmazhatók közvetlenül a mindennapi működés során bevált gyakorlatok és megszerzett tapasztalatok.

Művelet-orientált környezetben, az eddigiekben felsorolt veszélyforrás kategóriákon (fizikai, logikai, szervezeti és működési valamint az életciklushoz köthető veszélyforrások) túlmenően megjelennek újabb veszélyforrás kategóriák is. A kifejezetten a művelet-orientált működés esetén fellépő veszélyforrások a következő kategóriákba sorolhatók:

- jogi jellegű veszélyforrások;
- politikai jellegű veszélyforrások;
- kulturális jellegű veszélyforrások;
- ismeretlen jellegű veszélyforrások.

Jogi jellegű veszélyforrásként vehető figyelembe, hogy a művelet-orientált működés helyszínén esetlegesen speciális jogszabályi feltételek létezhetnek, illetve, hogy a működés során a vonatkozó jogszabályok megváltozhatnak. Politikai jellegű veszélyforrást jelenthetnek maguk a politikai változások, illetve az a lehetőség, hogy a politika esetleg beleszól a művelet-orientált működés során meghozott szakmai döntésekbe. Kulturális jellegű veszélyforrásként értékelhetjük, hogy a művelet-orientált tevékenység esetén olyan különböző szervezetek, esetleg országok közötti együttműködésnek kell megvalósulnia, amelyek egymástól eltérő kultúrával (társadalmi, technológiai, informatikai, biztonsági stb.) rendelkeznek. Ide sorolhatjuk az együttműködő partnerek közötti nyelvi nehézségeket is. „*A többnemzeti kötelékek működésében a vezényleti nyelv különbözősége, a felszerelések, képességek, a doktrínák és az eljárások eltérései jelentős zavarokat okozhatnak.*” [27]

A művelet-orientált működés során számítani lehet olyan veszélyforrásokra is, amelyek a korábbiakban nem fordultak elő, így ismeretlennek kell tekintenünk őket. Bár ismeretlen veszélyforrások a mindennapi, normál működés esetén is megjelenhetnek, fellépésükre művelet-orientált környezetben fokozottan kell számítani. Ennek oka, hogy művelet-orientált esetben nem rutinszerű, az adott környezetben ismétlődő, sokszor kipróbált tevékenységekről van szó, így a tevékenység és a környezet egymásra hatása előre nem látható veszélyforrások fellépését okozhatja.

Az előzőeken túlmenően létezhetnek pénzügyi jellegű veszélyforrások is. Ezek nem újabb kategóriát jelentenek, a felsorolt kategóriákat átfedhetik, de az eddigiektől különböző megközelítéssel vehetők figyelembe. A pénzügyi jellegű veszélyforrások az anyagi erőforrások (általában) korlátozott volta miatt jelennek meg. Leginkább azért következhetnek be, mert az adott feladathoz rendelt költségvetés nem tartalmaz megfelelő tartalékokat és a művelet során az esetlegesen fellépő, előre nem várt költségek leginkább a működésfolytonosság biztosításra fordított anyagi erőforrásokat emésztik fel.

Az előzőekben megállapítottuk, hogy mindazon veszélyforrások veszélyeztethetik a művelet-orientált működést, amelyek a mindennapi, folyamatos működés esetén előfordulhatnak. Ennek megfelelően az ezekből következő negatív következmények elkerülésére a mindennapi, folyamatos működés esetén folytatott védelmi feladatok megegyeznek művelet-orientált tevékenységek esetén is alkalmazhatókkal. Különbségként kell értékelnünk azonban, hogy művelet-orientált tevékenységek esetén a kitűzött befejezési határidő miatt előfordulhat, hogy gazdaságosan javítható kieső berendezések javítási idejének kivárása nem lehetséges, a kieső berendezéseket ez esetben azonnal újakkal kell pótolni.

Mint korábban említettük, a művelet-orientált működés egy meghatározott életciklus követését jelenti. Ennek megfelelően a művelet-orientált környezetben megvalósuló működés az életciklusának első három szakaszában (a cél és a feladat definiálása, tervezés, végrehajtás) jelent védelmi feladatot. Mindhárom szakaszban szükség van ugyanis a működésfolytonosság kezelésére, menedzselésére. Mindezek miatt a művelet-orientált tevékenység céljával, folyamataival, erőforrásaival és határidejével összhangban levő, és megfelelő költségvetéssel alátámasztott működésfolytonosság menedzsment terv kidolgozása és megvalósítása is megjelenik védelmi feladatként. A művelet-orientált működés feltételezi, hogy részletesen kidolgozott és megfelelően

dokumentált, megfelelő szinten jóváhagyott tervek állnak rendelkezésre a szervezet, a felelősségek, a hatáskörök, az erőforrások, folyamatok stb. tekintetében. Ezen tervek között kell szerepelnie a működésfolytonosság menedzselésére vonatkozó tervnek is. A terv összetevőinek alapvetően meg kell egyeznie a 3.1 pontban megadott összetevőkkel. A mindennapi normál működés esetén érvényes összetevőkhöz képest csupán annyi a különbség, hogy rövid időtartamú műveletek esetén a folyamatos aktualizálás elveszíti jelentőségét.

## 3.4 A kockázatelemzés sajátosságai a védelmi szférában

### 3.4.1 A kockázatelemzés alapfogalmai

A korábbiak szerint egy-egy szervezet, alakulat működésfolytonosságát számos veszélyforrás érvényre jutása veszélyezteti. Ezek különböző bekövetkezési valószínűséggel rendelkeznek, ugyanakkor érvényre jutásuk esetén különböző méretű kárkövetkezményre lehet számítani. Mivel a védelmi intézkedések megvalósítására allokálható erőforrások általában korlátosak, a gyakorlatban nem lehetséges minden veszélyforrással szemben megfelelő védelmi intézkedést alkalmazni. [71] Ki kell választani azokat közülük, amelyek a legnagyobb kockázatot jelentik és azokat a védelmi intézkedéseket kell alkalmazni, amelyek ezek bekövetkezését akadályozzák meg, illetve esetleges bekövetkezésük esetén a lehetséges kárkövetkezményeket csökkentik. [72]

A kockázatra vonatkozóan az irodalomban számos definíció létezik [77] a továbbiakban az informatikai biztonság területén leginkább alkalmazható definíciót alkalmazzuk: A kockázat a kárnagyságrend kategóriájának és a gyakoriság kategóriának a „szorzata”, azaz meghatározott szabály szerint képzett kockázati kategória értéke. A definícióban szereplő szorzat kifejezés nem feltétlenül szó szerint értendő, amennyiben a kárértékre, illetve a bekövetkezés gyakoriságra (bekövetkezési valószínűségre) vonatkozóan nem állnak rendelkezésre számszerűsíthető értékek, úgy ezt a kifejezést a kárérték és a gyakoriság (általában táblázatos) összevetését jeleni.

A bekövetkezési valószínűségek becslése alapvetően az előfordulások relatív gyakorisága alapján végezhető el. Ez azonban meglehetősen problematikus feladat, mivel tipikus, hogy nem áll rendelkezésre elegendő hosszúságú olyan időtartam, amely alatt a bekövetkezési valószínűségek relatív gyakoriságát befolyásoló körülmények változatlanok lennének, illetve előfordulhat, hogy egy-egy szervezetnél az éppen értékelendő veszélyforrás bekövetkezésére még soha nem volt példa. (Abból például,

hogy egy szervezetnél még soha nem volt tűz, nem következtethetünk arra, hogy jövőbeli bekövetkezésének valószínűsége 0.) Ilyen esetekben a probléma megoldására az analógiák keresése (hasonló tevékenység, hasonló szervezet, hasonló erőforrások, esetleg más szervezetben, más országban stb.) nyújthat támpontot. Művelet-orientált esetben ez gyakran még inkább érvényes, mint normál, mindennapi működés esetén. Az egyszeri végbemenetel miatt a veszélyforrások egy részének bekövetkezési valószínűsége az előfordulás relatív gyakoriságából nem becsülhető, hiszen a relatív gyakoriságra vonatkozó adat a tervezés fázisában nem áll rendelkezésre.

A kockázatok azonosítását, elemzését és értékelését támogató módszertanok alkalmazása révén a szervezet képes összehasonlítani az egyes veszélyforrások okozta kockázatokat, képes összevetni az egyes veszélyforrások kárkövetkezményeit és az érvényre jutásukat megakadályozó védelmi intézkedések költségeit, továbbá a fennmaradó kockázatok ismerete lehetővé teszi a vezetés számára ezek tudatos kezelését.

Az előzőekkel összhangban kockázatelemzésre vonatkozóan léteznek kvalitatív és kvantitatív módszertanok. [78]

### 3.4.2 Kvalitatív módszertanok

A kvalitatív kockázatelemzési módszertanok szakértői becslésen alapuló eljárások, szinteket, skálákat használnak, nem számszerű adatokat. Eredményeik megbízhatóságára vonatkozóan nem adnak támpontot. Ezen eljárásokban az egyes veszélyforrásokhoz tartozó bekövetkezési valószínűséget és az érvényre jutásuk esetén bekövetkező kár nagyságát szakértői becslések alapján szintekbe sorolják. Általánosan használt ilyen eljárás a hatásrácsot[51] alkalmazó módszer. [80] A módszernek számos változata ismert, de az összes változat gyakorlatilag azonos alapelveken alapul.

Ez esetben a bekövetkezési valószínűséget és a bekövetkezés esetén létrejövő kár mértékét például egy-egy ötfokozatú skálán helyezik el a következő módon.

A bekövetkezési valószínűség lehetséges értékei a következők.[52]

- Nagyon kicsi (PVS – .Very Small);
- Kicsi (PS – Small);
- Közepes (PA – Medium);

[51] A hatásrács elnevezés szinonimájaként számos irodalom a kockázati mátrix fogalmat használja.
[52] A P (probability) betű a valószínűséget jelentő angol szó kezdőbetűje.)

- Nagy (PL – Large);
- Nagyon nagy (PVL – Very Large).

A létrejövő kár (hatás) lehetséges értékei a következők.

- Elhanyagolható (VS – Very Small);
- Kicsi (S – Small);
- Közepes (M – Medium);
- Jelentős (L – Large);
- Katasztrofális (VL – Very Large).

A módszer szerint bekövetkezés valószínűsége és a hatás összevetése adja meg a kockázatot.

A kockázat értékei a következők lehetnek.[53]

- Elhanyagolható (RVS – Very Small);
- Kicsi (RS – Small);
- Közepes (RM – Medium);
- Nagy (RL – Large);
- Igen nagy (RVL – Very Large).

Az eljárásban a bekövetkezés valószínűségének és a hatásnak az összevetése a következő táblázat, az ún. kockázati mátrix alapján történik meg.

| **P \ Hatás, kár** | **VS** | **S** | **M** | **L** | **VL** |
|---|---|---|---|---|---|
| **PVS** | RVS | RVS | RS | RM | RL |
| **PS** | RVS | RS | RM | RM | RL |
| **PM** | RVS | RS | RM | RL | RL |
| **PL** | RS | RM | RL | RL | RVL |
| **PVL** | RS | RM | RL | RVL | RVL |

3/1. táblázat – A kockázati mátrix

[53] Az R (risk) betű a kockázatot jelentő angol szó kezdőbetűje.

### 3.4.3 Kvantitatív módszertanok

A kvantitatív kockázatelemzési módszerek az egyes veszélyforrások bekövetkezési valószínűségének és a bekövetkező kárértékek számszerűen meghatározott értékeiből indulnak ki, eredményként is számszerű, tipikusan pénzügyi értékeket adnak. Ez esetben az egyes számértékeket jellemző megbízhatósági értékek is megjelennek. A kvantitatív kockázatelemzési módszerek általában igen sok bemenő adattal dolgoznak, azonban az alkalmazott modellek és függvények általában nem publikusak. Kvantitatív kockázatelemzés eredményes végrehajtására általában a nagy nemzetközi tanácsadó cégek képesek, amelyek hosszú idő alatt sok szervezet tanulmányozásával építették fel azt az adatbázist, amely a szervezeten kívüli input adatokat szolgáltatja. Mindezek miatt a kvantitatív kockázatelemzési módszerek végrehajtása általában meglehetősen költséges.

### 3.4.4 A módszerek alkalmazhatósága a védelmi szférában, illetve a kritikus infrastruktúrák területén valamint művelet-orientált környezetben

A mindennapi rutinszerű tevékenységek esetén a 3.4.1 pontban ismertetett szempontok figyelembe vételével általában becsülhetők a veszélyforrások bekövetkezési valószínűségei [42] és a bekövetkezésük okozta károk mértéke, így mind a kvantitatív, mind a kvalitatív kockázatelemzési módszerek alkalmazhatók a védelmi és a polgári szférában, illetve a kritikus infrastruktúrák területén.

Művelet-orientált környezetben azonban a kvantitatív kockázatelemzési módszerek alkalmazása a célok és tevékenységek sokfélesége miatt problematikus, hiszen alig képzelhető el hogy elvégzéséhez hasonló tevékenységek elemzése alapján felépített adatbázis és modell bárhol is rendelkezésre állna. Fokozottan érvényes ez nemzetközi szerződésekben vállalt katonai feladatok esetén. „*Minden többnemzeti katonai (had)művelet egyedi jellegű, és ebből adódóan a tervezés, a vezetés és a végrehajtás kérdései a kulcsfontosságú tényezők, amelyek a nemzetközi helyzet, a perspektívák, a motivációk, valamint a benne résztvevő államok érdekeinek megfelelően változhatnak.*” [27]

Bár a kvalitatív módszerek alkalmazását többnyire kevésbé professzionális eljárásnak tekintik, széles körben elterjedten használják őket, alkalmazásuk nem okoz nagyobb problémát művelet-orientált esetben sem. Ez esetben azonban figyelembe kell venni, hogy a tapasztalatok hiánya miatt a bekövetkezési valószínűségek és

kárkövetkezmények becslése csak nagyobb bizonytalansággal végezhető el, ennél fogva a kapott eredmények bizonytalansága is megnő.

## 3.5 A veszélyforrások hatásai ellen alkalmazható védelmi módszerek, különös tekintettel a védelmi szférára

### 3.5.1 A védelmi módszerek általános elvei

A 3.3 pont szerint általános, hogy egy-egy veszélyforrás azonosítása általában automatikusan meghatározza a veszélyforrás ellen alkalmazható védelmi feladatot. A kockázatelemzés alapján az egyes veszélyforrások prioritási sorrendbe állíthatók az általuk jelentett kockázatoknak megfelelően. Miután az egyes veszélyforrások gyakorlatilag meghatározzák az ellenük alkalmazható védelmi feladatokat, azokhoz a védelmi feladatokhoz kell konkrét védelmi intézkedéseket kidolgozni, amelyek a legnagyobb prioritással rendelkeznek. [67]

Mivel általánosságban igaz, hogy a működésfolytonosság biztosításához csak limitált anyagi erőforrások állnak rendelkezésre, nyilvánvaló, hogy a nagyobb prioritással rendelkező kockázatok kiküszöbölésére vagy csökkentésére vonatkozóan kell védelmi intézkedéseket kidolgozni, figyelembe véve azt is, hogy az egyes veszélyforrások között léteznek bizonyos dependenciák, azaz egy-egy veszélyforrás ellen kidolgozott védelmi intézkedés esetlegesen több veszélyforrás érvényre jutását is megakadályozza, vagy csökkenti az általuk okozott hatást. A polgári szféra gazdálkodó szervezeteire ez utóbbiak nem feltétlenül érvényesek. Esetükben, amennyiben kvantitatív kockázatelemzési adatok is rendelkezésre állnak, össze kell vetni a kockázat értékét az ellene alkalmazásra kerülő védelmi intézkedések költségével. Általában azt a védelmi intézkedést szükséges megvalósítani, amelynek költsége nem éri el a hiányában fellépő kockázatot. Ezzel szemben a védelmi szférában és a kritikus infrastruktúrák területén tipikus, hogy a szervezeteknek törvényi előírásoknak kell megfelelniük: ez esetben nem mérlegelhető, hogy a védelmi intézkedések költsége hogyan viszonyul az esetleges kiesések okozta költségekhez.

A legtöbb konkrét védelmi intézkedés részletes kidolgozása és végrehajtása igen összetett feladat, a legtöbb esetben tervezési, beszerzési, implementálási, tesztelési kiképzési, felkészítési, dokumentálási stb. lépéseket jelent, gyakran alternatív megoldások közötti választást tesz szükségessé.

A működésfolytonosság fenntartására irányuló tevékenységeknek tekinthetők mind-azon preventív jellegű védelmi módszerek, amelyek arra irányulnak, hogy a kritikus

folyamatok kiesése ne következzen be. Mindezek megfelelő minőségű technológia felhasználásával, megfelelő szervezet kialakításával, a humán feltételek, valamint a szabályozott működés biztosításával érhetők el.

### 3.5.2 A védelmi módszerek sajátosságai a védelmi szférában, illetve a kritikus infrastruktúrák területén, valamint művelet-orientált környezetben

Bár a konkrét módszerek között lényeges eltérések lehetnek, a védelmi módszerek általános elvei nem térnek el egymástól a védelmi és a polgári szférában, ennek megfelelően a kritikus infrastruktúrák területén.

Művelet-orientált működés esetén azonban további követelményként jelenik meg a korszerű projektmenedzsment, multiprojekt menedzsment módszertanok[54] alkalmazása is. Művelet-orientált esetben a konkrét védelmi intézkedések kialakításakor elsősorban a mindennapi, rutinszerű működéshez képest az egyszeri végbemenetel okoz problémákat. Emiatt fokozott jelentősége van a pontos, mindenre kiterjedő terveknek. Bár művelet-orientált tevékenységek esetén nyilvánvalóan nem lehetséges teljes körű teszteléseket, mindenre kiterjedő gyakorlatokat végrehajtani, fontos, hogy a lehetőségeket maximálisan kihasználva kell elvégezni az egyes összetevőkre vonatkozó és integrációs teszteket, illetve gyakorlatokat. Mivel művelet-orientált esetben egy-egy kritikus pozíciót betöltő személy lecserélése problematikus lehet, nagy jelentősége van a személyi feltételeknek és a hasonló tevékenységek végzésében szerzett tapasztalatoknak. Kritikus pozíciók esetében fontos lehet annak vizsgálata, hogy az adott pozíció betöltésére kijelölt személyt szakmai, emberi és pszichológiai kompetenciája alkalmassá teszi-e erre. Ez esetben ugyancsak nagy jelentősége van az erőforrásokra vonatkozó a különböző tartalékolási mechanizmusoknak, illetve a redundanciák kialakításának, valamint a megfelelő időtartalékok biztosításának.

## 3.6 A katasztrófa helyzet kezelés sajátosságai a védelmi szférában

### 3.6.1 A katasztrófa kezelés általános kérdései

Az anyagi erőforrások korlátozott volta miatt a működésfolytonosság teljes biztonsággal soha nem valósítható meg. Egyetlen veszélyforráshoz sem alakíthatók ki ugyanis olyan védelmi módszerek, amelyek tökéletes biztonsággal kiküszöbölnék az illető veszélyforrás negatív hatásait. „*A biztonságtechnikában egy dolog 100%-os, hogy*

[54] A módszertanok ismertéről vizsgához kötött minősítés szerezhető, pl. IPMA (International Project Management Association, illetve PMI (Project Management Institute) minősítések.

*semmi sem 100%-os.*" [67] Az előzőeknek megfelelően lehetségesek olyan veszélyforrások is, amelyek nem tudatosulnak, emiatt ezekre védelmi intézkedések sem kerülnek kidolgozásra. Ezekhez tartozó problémaként jelenik meg, hogy egy-egy tervezett védelmi intézkedés gyakorlati megvalósítása olyan erőforrásokat igényelne, amelyek allokálása meghaladná az illető veszélyforrás érvényre kerülése esetén bekövetkező károk értékét.

Mindezek miatt számítani kell arra, hogy időnként olyan veszélyforrások kerülnek érvényre, amelyek a megtett preventív jellegű védelmi intézkedések ellenére, illetve a felvállalt kockázatok következményeként a kritikus folyamatok kiesését okozzák, azaz katasztrófa helyzet következik be. Az informatikai rendszerekkel támogatott folyamatok működésfolytonossági kérdéseinek tekintetében természetesen nemcsak a természeti katasztrófák okozhatnak kieséseket, hanem számos, az előzőekben már áttekintett veszélyforrás is. Ennek megfelelően katasztrófaként jelentkezhet például egy-egy adatvesztés vagy szerver meghibásodás is. Ezek kezelése kizárólag reaktív jellegű védelmi intézkedésekkel lehetséges. Reaktív jellegű védelmi intézkedésnek tekinthetők mindazon intézkedések, amelyek arra irányulnak, hogy a kieséseket követően az előre definiált sebezhetőségi ablakokon belül a kritikus folyamatok a lehető legrövidebb időn belül újrainduljanak.

A katasztrófa helyzetek kezeléséhez az adott szervezeten belül előre felépített katasztrófa kezelő szervezetre és olyan kidolgozott akciótervekre[55] van szükség, amelyek a kiesett folyamatok vissza-, illetve helyreállítására irányulnak. Visszaállítás esetén a folyamatok a lehető legrövidebb időn belül újraindulnak egy előre definiált minimális szolgáltatási szinten (általában az eredeti jellemzőknél alacsonyabb szinten), a helyreállítás eredménye pedig az eredeti szolgáltatási szintnek megfelelő működés.

A katasztrófa helyzet esetén alkalmazott akciótervek végrehajtása legkorábban akkor kezdődhet meg, amikor a katasztrófa helyzet, általában egy elsődleges kárfelmérés után, deklarálásra kerül. Emiatt a katasztrófát kiváltó események és a katasztrófa helyzet deklarálása között általában időkülönbség van. Ekkor az erőre definiált, ún. szükséghelyzeti tervek (például tűzriadó terv, villamos energia kiesésére vonatkozó terv stb.) érvényesek, amelyek iránymutatást adnak az ezen időszakban követendő magatartásra.

A katasztrófa helyzet kezeléshez tartozó dokumentumok tárolási helyszínének

[55] Az akcióterveket folyamatként célszerű definiálni az egyes lépések pontos időzítésének megadásával.

megválasztásakor[56] figyelembe kell venni, hogy ne állhasson elő az az eset, hogy egy katasztrófa esemény bekövetkezésekor a visszaállítás folyamatát meghatározó dokumentumok is megsemmisülnek.

### 3.6.2 A katasztrófa kezelő szervezet

A katasztrófa helyzetek kezelésére megfelelően kialakított katasztrófa helyzet kezelő szervezetet[57] kell kialakítani, amely általában egy hierarchikus szervezet, a hierarchia minden pontján jól definiált pozíciókkal, amelyekhez egyértelműen elérhetőségek, feladatok, felelősségek, hatáskörök, kapcsolódási pontok és erőforrások vannak rendelve.

A katasztrófa kezelő szervezet kialakításakor figyelembe kell venni, hogy katasztrófa helyzet esetén emberi erőforrások is kieshetnek, elérhetetlenné válhatnak. Emiatt megfelelő redundanciákról, duplikálásokról is szükséges gondoskodni. (Például a katasztrófa menedzser beosztáshoz mindenképpen vele azonos szinten kiképzett helyettest kell rendelni.) A katasztrófa kezelő szervezet tipikus elemei a következők:

- Kríziskezelő csoport;
- Katasztrófa menedzser;
- Kárfelmérő csoport;
- Technikai csoport.

A kríziskezelő csoport a katasztrófa helyzet kezelés projekt szponzora. Kapcsolatot tart a felső vezetéssel, ugyanakkor közvetlen segítséget ad a katasztrófa menedzsernek. Katasztrófa helyzet kezelő központot állít fel a katasztrófa helyzet helyszínén, illetve annak közelében. Kinevezi a katasztrófa helyzet elhárításában résztvevő személyeket, gondoskodik valamennyi intézkedés dokumentálásáról, kapcsolatot tart a külső beszállító, szolgáltató szervezetekkel. Intézkedik a katasztrófa helyzet elhárításához szükséges anyagi erőforrások biztosításáról.

A katasztrófa menedzser a katasztrófa helyzet kezelés projekt menedzsere, operatív irányítója. A kárfelmérő csoport jelentése alapján deklarálja a katasztrófa helyzetet. Kapcsolatot tart a kárfelmérő, a technikai és infrastruktúra visszaállító csoportokkal és koordinálja munkájukat, gondoskodik az estleges ellentmondások feloldásáról, ellátja a

[56] A tárolási helyszín megválasztáskor természetesen figyelembe kell venni a bizalmasságra vonatkozó követelményeket is.
[57] A katasztrófa kezelő szervezet szinonimájaként számos irodalom a katasztrófa team elnevezést használja.

katasztrófa helyzet kezeléséhez szükséges információ koordinálását. Felelős az érvényben lévő katasztrófa helyzet kezelési terv karbantartásáért, teszteléséért és a hozzá kapcsolódó oktatásokért.

A kárfelmérő csoport többféle szakterületi szakértelemre alapozva részletesen meghatározza a bekövetkezett kár kiterjedését, megvizsgálja, hogy kritikus folyamatok kiesését milyen súlyú okok idézték elő, továbbá, hogy mekkora lesz a kiesések várható időtartama. A katasztrófa menedzser a kárfelmérő csoport elsődleges jelentése alapján hoz döntést a katasztrófa helyzet deklarálásáról, nagyobb súlyú katasztrófa események esetén a konkrét akciótervek a kárfelmérésére vonatkozó, a részletes kárfelmérés után indíthatók.

A technikai csoport sokféle technikai jellegű kompetenciát integrálva a szükséges technológiák vissza/helyreállítását végzi a kárt szenvedett területen az előre kidolgozott, illetve az adott helyzetre megfelelően adaptált akciótervek szerint. Azonosítja és megszerzi azokat a pótlólagos erőforrásokat, amelyek elengedhetetlenek a kritikus folyamatok vissza-, illetve helyreállításához.

A katasztrófa helyzet kezelés megkezdésének fontos feltétele, hogy a felmérésben és a visszaállításban részt vevő szakértők különösebb nehézség nélkül elérhetők legyenek. Emiatt a katasztrófa kezelő szervezet tagjainak elérhetőségét is rögzíteni kell, lehetőség szerint alternatív elérhetőségi lehetőségek felsorolásával. A rögzített elérhetőségeknek ki kell terjedniük a katasztrófa kezelő szervezet tagjain kívüli személyekre is. Ilyen módon rögzíteni szükséges a visszaállításban résztvevő operatív munkatársak, parancsnokok és beosztottak (például szerverek rendszergazdái, speciális ismeretekkel rendelkező szakértők), valamint a visszaállításban résztvevő külső partnerek/hatóságok (például beszállítók, mentők, tűzoltóság stb.) elérhetőségeit is.

### 3.6.3 Akciótervek

Az akciótervek célja, hogy a bennük szereplő lépések végrehajtása után a szolgáltatás, a kritikus folyamatok egy meghatározott időn belül visszaálljanak egy előre definiált, gyakran az eredetinél alacsonyabb szintű, minimális szolgáltatási szinten. Az akciótervek számos lehetőségre támaszkodhatnak. Így tartalmazhatják alternatív helyszínre történő áttelepülés, tartalék erőforrások használatba vétele, új erőforrások beszerzése, átmeneti áttérés manuális, papír alapú működésre stb. eseteit, illetve ezen esetekre vonatkozóan az adott szervezetre és kiesésre kidolgozott részletes terveket.

Az akciótervek elsősorban a visszaállítási folyamatokra vonatkoznak. A helyreállítási folyamatok a visszaállítási folyamatoknál többnyire lényegesen hosszabbak, időtartalékokkal rendelkeznek, emiatt tervezési fázis is szerepelhet bennük, így nem feltétlenül szükséges rájuk részletes akcióterveket kidolgozni. Ezzel szemben a visszaállítási folyamatokat általában igen szoros időkorlátok között kell végrehajtani, emiatt tervezési lépések nem szerepelhetnek bennük. Ez indokolja azt is, hogy a visszaállítási folyamatok akcióteveit részletesen ki kell dolgozni.

Az akcióterveket az előzetesen definiált visszaállítási időmátrix figyelembe vételével szükséges kialakítani. A visszaállítási időmátrix az egyes kritikus folyamatokhoz olyan, az illető folyamat sebezhetőségi ablakának megfelelő időintervallumnál nem nagyobb időtartamokat rendel, amelyek alatt az egyes folyamatok visszaállítását kell megvalósítani. Meghatározásakor nagyon fontos az egyes folyamatok közötti függőségek figyelembe vétele. Az akciótervekben a konkrét tevékenységeken túlmenően rögzíteni kell az akciók végrehajtásában résztvevő személyek feladatait, felelősségeit, hatásköreit, az általuk követendő hierarchiát és a rendelkezésükre álló erőforrásokat is.

### 3.6.4 A katasztrófa helyzet kezelés sajátosságai a védelmi szférában, illetve a kritikus infrastruktúrák területén, valamint művelet-orientált esetben

A katasztrófa helyzet kezelés általános elvei nem térnek el lényegesen egymástól a védelmi és a polgári szférában, illetve a kritikus infrastruktúrák területén, legfeljebb annyiban, hogy előfordulhat, hogy egy gazdálkodó szervezetet ért katasztrófa olyan kieséseket, veszteségeket okoz, hogy a működést nem éri meg újraindítani. Ez a védelmi szférában, illetve a kritikus infrastruktúra védelem területén, a mindennapi folyamatos tevékenységek esetén nem fordulhat elő, hiszen ott tipikusan állami, törvények által meghatározott funkcionalitás biztosítása jelenti a feladatot, emiatt az újraindítás gazdaságossági szempontjai nem mérlegelhetők. Művelet-orientált esetben eltérő helyzet alakulhat ki. Ez esetben a katasztrófa helyzet bekövetkezése a jól definiált határidők, illetve limitált erőforrások miatt akár a művelet-orientált működés sikertelen befejezését is eredményezheti.

A normál, mindennapi, rutinszerű működéshez képest, művelet-orientált működés esetén a visszaállítás és helyreállítás viszonya is eltérő lehet. A helyreállítás a visszaállításnál hosszabb időt vesz igénybe, ennek végeztével a folyamatok az eredeti

jellemzőiket biztosítva mennek ismét végbe. A mindennapi, normál, rutinszerű működés esetén a kiesés kezelése mindig a helyreállítással fejeződik be, művelet-orientált tevékenységek esetén azonban a betartandó határidők és limitált anyagi erőforrások miatt gyakran előfordul, hogy a helyreállítás elmarad, és a tevékenység befejezéséig hátralevő időben a visszaállítás biztosította szinten valósul meg a működés.

Az akciótervek végrehajtásakor általános tapasztalat, hogy egy, a valóságban bekövetkezett helyzet nem teljes mértékben azonos az akcióterv elkészítésekor vélelmezettel. Ennek ellenére a tapasztalatokkal összhangban kijelenthető, hogy az adott helyzet megoldásában az előre elkészített akciótervek kis módosítással felhasználhatók az adott helyzet kezelésére.[58] Művelet-orientált tevékenységek esetén ez fokozottan érvényes. Ennek elsősorban az egyszeri végbemenetel az oka, ami miatt az egyes kiesések körülményeinek előzetes meghatározása a tapasztalatok hiányában a normál, rutinszerű, gyakran előforduló tevékenységekhez képest csak jóval nagyobb bizonytalansággal végezhető el. Mindezek miatt a konkrét akciótervek alkalmazása esetén művelet-orientált tevékenységek során számítani kell arra, hogy egy-egy konkrét kiesés olyan körülmények között jön létre, amely az előre kidolgozott akcióterveknek csak nagyobb mértékű módosításával kezelhető.

## 3.7 A működésfolytonosság biztosításának egyéb követelményei

### 3.7.1 A működésfolytonossághoz kapcsolódó felkészítés, tesztelés, illetve aktualizálásának folyamata

A működésfolytonosság biztosítása az előzőeken túlmenően további követelményeket is támaszt. A működésfolytonosság biztosítása követelményeket támaszt a felkészítés és a tesztelés területén, valamint megjelennek az aktualitásra vonatkozó követelmények is. Ezek – bár kevésbé összetettek – az eddig ismertetetteknél nem kisebb jelentőségűek, nem kielégítő megvalósításuk a működésfolytonosság biztosításnak sikertelenségét okozhatják.

### 3.7.2 A működésfolytonosságra vonatkozó felkészítés

A működésfolytonosság biztosítása az egyes szervezeti egységek vezetői, parancsnokai és beosztottjai számára katasztrófa helyzet bekövetkezése esetén alapfeladataikon túlmenő feladatokat is jelenthet. Emiatt fontos, hogy a számukra szükséges szinten ismerjék a működésfolytonosság biztosítása érdekében rájuk háruló feladatokat, azaz a működésfolytonosság biztosításának egyik fontos összetevője a

[58]Vid Ödön: Gondolatok az üzletmenet folytonosságról c. előadása, ISACA Hungarian Chapter 2004. 04.14.

hozzá kapcsolódó felkészítés is. A felkészítésnek egyaránt ki kell terjednie általános, a működésfolytonosság tudatosságának növelését célzó és gyakorlati részekre. A különböző pozíciókat betöltő személyeknek általában különböző célú felkészítésekre van szükségük. Például a katasztrófa tervhez kötődő egyes akciótervek felelőseinek számára szükséges olyan speciális felkészítések végrehajtása, amelyen megtörténik konkrét tervekre vonatkozó oktatás. Ez esetben az érintett személyeknek pontosan tudniuk kell, hogy mi a szerepük a katasztrófát követő munkában, milyen felelősséggel és hatáskörrel rendelkeznek (ez eltérhet a normál munka során betöltött szerepektől). A oktatásnak gyakorlati összetevőket is kell tartalmaznia, amely alapján az érintett személyeknek képesnek kell lenniük arra, hogy konkrét feladataikat katasztrófa helyzetben végre tudják hajtani. A felkészítésre vonatkozóan fontos követelmény, hogy az oktatott anyag megismerésére vonatkozó (nem formális) számonkérésnek kell azt követnie.

A felkészítéseken részt kell venniük azoknak a személyeknek, akik új beosztásba kerülnek, ezen túlmenően szükséges, hogy az oktatásoknak periodikusan (az általános gyakorlat szerint évente) ismétlődjenek. Mindezeken túlmenően az adott szervezetben bekövetkező változásokat követően ugyancsak szükséges a megváltozott helyzetre vonatkozó felkészítés.

### 3.7.3 A működésfolytonosság tesztelése

A működésfolytonosság tényleges megvalósulása tesztek végrehajtásával érhető el. Teszteléseket tipikusan katasztrófa eseményekre vonatkozóan lehetséges elvégezni. Megkülönböztethetők éles, szimulációs illetve szóbeli tesztek. A leginkább megbízható eredményt nyilvánvalóan az éles tesztek szolgáltatják, a szóbeli tesztek csak az elméleti ismeretek elsajátítását tükrözhetik. [71]

A tesztek végrehajtását megelőzően szükséges az elvárt eredmények rögzítése, mert ez alapján lesz értékelhető a tesztelés eredménye. A végrehajtáshoz figyelembe kell venni, hogy a normál működéshez képest általában többlet erőforrásokra van szükség, továbbá, hogy az éles teszt önmagában mindig bizonyos kockázattal jár. Mindezek miatt a teszteléseket pontosan meg kell tervezni (beleértve az előre nem látható problémák esetén alkalmazandó normál működésre vonatkozó visszatérési eljárásokat is), és az egyes végrehajtott lépéseket pontosan dokumentálni kell.

### 3.7.4 A működésfolytonosság aktualizálásának feladata

A működésfolytonosság konkrét megvalósítására, illetve 3.1. pontban említett működésfolytonosság menedzsment tervre vonatkozóan igen fontos követelmény, hogy a szervezet folyamataival, erőforrásaival, önmagával és más dokumentumokkal összhangban legyen. Az 1.6.6 pontban ismertetett életciklus modellhez kapcsolódóan mindezek vizsgálata nemcsak a megvalósítás első fázisában szükséges, hiszen a tevékenység folyamán sokféle változásra kell felkészülni. A változáskezelés folyamatát úgy kell kialakítani, hogy a változások automatikusan érvényre kerüljenek a működésfolytonosság biztosítására létrehozott működésfolytonosság menedzsment tervben is. Mindezekkel összhangban a működésfolytonosság menedzsment terv folyamatos aktualizálása igen fontos összetevő. Magában a tervben meg kell határozni azokat a mechanizmusokat, amelyek biztosítják a folyamatos naprakészséget. Tipikus, hogy az aktualizálás folyamatát bizonyos, nagyobb jelentőségű események illetve időpontok bekövetkezése indítja el.

## 3.8 Összegzés, következtetések

Jelen fejezet az értekezés bevezetésében rögzítetteknek megfelelően a következő kutatási cél elérésére fókuszál:

*„A működésfolytonosságot veszélyeztető veszélyforrások elemzése, a működésfolytonosság biztosítását alkotó összetevők meghatározása."*[59]

A kutatási cél elérése érdekében a következő feladatokat végeztem el:

- Meghatároztam, hogy melyek a működésfolytonosság biztosításnak fő összetevői és hogy mi jellemzi ezeket.
- Megvizsgáltam hogy az egyes összetevők mennyiben rendelkeznek sajátos tulajdonságokkal a védelmi szférában illetve a kritikus infrastruktúrák területén valamint művelet-orientált működés esetén.

A feladatok elvégzésével a következő eredményekre jutottam:

A vizsgálat során megállapítottam, hogy a működésfolytonosság biztosításának fő összetevőit a következők jelentik: az adott szervezetnél elvégzett helyzetfeltárás, a releváns veszélyforrások azonosítása és értékelése, az ezek alapján végrehajtott kockázatelemzés, illetve az ennek eredményeire támaszkodó, konkrét védelmi

[59]Lásd 7. oldal, 3. pont.

intézkedések megtétele, beleértve a katasztrófa helyzetekre való felkészülést is. Mindezeken túlmenően a működésfolytonosság biztosításának további fontos összetevői a folyamatos aktualizálás, a tesztelés, valamint a hozzá tartozó megfelelő oktatás. Ezen összetevők meghatározzák a működésfolytonosság biztosítására vonatkozó, a gyakorlatban is használható terv kialakításának lépéseit is.

Azt a következtetést is levontam, hogy az informatikai rendszerekkel támogatott folyamatok működésfolytonosságának biztosítása hasonló problémákat okoz a védelmi és a polgári szférában, így a kritikus infrastruktúrák területén, a normál mindennapi, illetve művelet-orientált működés esetén is. Elsősorban tradicionális okok miatt kisebb különbségek léteznek a fizikai, a szervezeti és működési valamint az életciklushoz kapcsolódó veszélyforrások tekintetében, a logikai veszélyforrások vonatkozásban gyakorlatilag nem ismerhetők fel különbségek.

További következtetésként megállapítottam, hogy művelet-orientált környezetben megjelennek olyan veszélyforrások és ehhez kapcsolódóan védelmi feladatok is, amelyen a normál, mindennapi működés során nem lépnek fel, ugyanakkor kimutattam, hogy a kockázatáthárítás mit védelmi módszer nem lehet tipikus művelet-orientált tevékenységek esetén. Megállapítottam továbbá, hogy művelet-orientált működés esetén a kvantitatív kockázatelemzési módszerek kevésbé alkalmazhatók, illetve, hogy a katasztrófa helyzetek kezelése sajátos jellemzőkkel rendelkezik mind a védelmi szféra, mind pedig a művelet-orientált tevékenységek esetén.

# 4 A folyamatos működés értékelési, minősítési módszerei a védelmi szférában

*„Ha nem mérjük, nem is értjük."*

*Az itSMF Magyarország 3. szemináriumának mottója*

## 4.1 A mutatószám rendszerre vonatkozó elvárások

A különböző szervezetek megfelelő szintű üzemeltetői, döntéshozói, parancsnokai részéről jogos elvárás, hogy nyomon követhessék, esetleg szemléletesen ábrázolják a kompetenciájukhoz tartozó szervezet működésfolytonosságának minőségét. Értékeljék a működésfolytonosság megvalósult, aktuális szintjét, illetve arra vonatkozóan elvárásokat fogalmazhassak meg, esetlegesen összevessék a megvalósult szinteket más, hasonló szervezetek jellemzőivel. Mindezek egy megfelelően kidolgozott minősítési rendszer alapján elképzelhetők, azonban a szakterülethez tartozó irodalomban nem lelhető fel olyan mérési, minősítési eljárás, amely alapján mindezek megtehetők.

A minősítési rendszerre vonatkozóan az előzőeken túlmenően fontos követelményként jelenik meg, hogy rá építkezve lehetőség legyen arra, hogy bizonyos időhorizonton célként jelöljük meg az elérni kívánt szintet, továbbá, hogy segítséget nyújtson abban, hogy meghatározhassuk a szervezet működésfolytonosságának gyenge pontjait és a fejlesztendő területeket.

A minősítési rendszer kidolgozásakor figyelembe kell venni, hogy az egyes folyamatok működésfolytonossága dinamikus, időben változó, optimális esetben időben fokozatosan javuló minőségi jellemzőkkel rendelkezik, ennek megfelelően a minősítési rendszernek a működésfolytonosság állapotának fejlettségét, érettségét kell kifejeznie.

Mindezek a követelmények akkor teljesíthetők, ha a minősítési jellemzők konkrét, számszerű értékek, mutatószámok[60] formájában jelennek meg. A mutatószámok általában a mennyiségi jellemzők mérésére alkalmasak közvetlenül, gyakori, hogy a mennyiségi jellemzőket tükröző mutatószámok közvetlen méréssel, automatikusan jönnek létre, ugyanakkor a minőség kezelése mutatószámokkal sokkal inkább problematikus. Gyakori, hogy a minősítéshez nem elegendő egyetlen mutatószám, ez esetekben mutatószám rendszereket szükséges alkalmazni. „*A mutatószám rendszerek több mutató matematikailag vagy logikailag összekapcsolt kombinációi.*" [30]

[60] A mutatószámok szinonimájaként számos irodalom az indikátor illetve a mérőszám fogalmat használja:

A minőségi jellemzők számszerűsítésére vonatkozóan gyakori módszer, hogy verbálisan definiált minőségi szinteket alakítunk ki és az egyes szinteket számszerű jellemzőkkel reprezentáljuk. Mindezek után egy-egy konkrét esetet saját tulajdonságai alapján ezen verbális szintek valamelyikéhez rendeljük és az adott szinthez tartozó számszerű értékkel jellemezzük.[61]

A mutatószám rendszerekre vonatkozóan gyakran általános követelményként jelenik meg, hogy a jellemzőket tükröző mutatók legyenek szemléletesen ábrázolhatók. Mindezek megkönnyítik az áttekinthetőséget, és lehetővé teszik az időbeli változások gyors követését, valamint az összehasonlítások elvégzését. Ezzel összefüggésben áll az a követelmény, hogy a mutatószám rendszer ne álljon túlzottan sok mutatószámból, mivel ez esetben áttekinthetetlenné, kezelhetetlenné válhat a rendszer.

Egy-egy alakulat, szervezet fő funkcionalitásait általában számos működési folyamaton keresztül valósítja meg. Emiatt az egyes szervezetek üzemeltetői, döntéshozói, parancsnokai összhangban az 1.5.2 pontban rögzítettekkel, tipikusan nem az egyes folyamatok működésfolytonossági kérdéseire, sokkal inkább a szervezet egészének működésfolytonossági problémáira koncentrálnak. Ez összhangban van a mutatószámok limitált számosságra vonatkozó követelménnyel, ennek megfelelően a mutatószám rendszernek nem az egyes folyamatokra, hanem az egyes folyamatokat integráló szervezetre, alakulatra kell vonatkoznia.

## 4.2 Érettségi modellek

Az előzőek szerint a minősítési rendszernek a működésfolytonosság állapotának fejlettségét, érettségét kell kifejeznie. Az állapotok, folyamatok fejlettségének, érettségének jellemzése nem kizárólagosan a működésfolytonossághoz kapcsolódó probléma, számos olyan modell létezik, amely ezt a megközelítést alkalmazza. Ilyenek például a COBIT[62] érettségi modell, az Open Source Maturity Modell (Nyílt forráskód érettségi modell), a CMM (Capability Maturity Modell – Képességérettségi modell). Ezeken túlmenően a különböző projektmenedzsment módszertanokban is megtalálhatók az érettségi modellek. Ezekre a modellekre általánosan jellemző, hogy az egyes szinteket az előzőeknek megfelelően verbálisan írják le, és ezekhez rendelik a megfelelő mérőszámokat.

Az informatikai rendszerek üzemeltetésére fókuszáló, a 2.4 pontban rögzítettek szerint

[61] Tipikus példa erre a módszerre a felkészítéseket követő számonkéréseken adott osztályzat.
[62] Lásd 2.3.4 pont.

mind a polgári, mind a védelmi szférában elterjedten használt COBIT menedzsment eszközként tartalmaz egy úgynevezett érettségi modellt, amely számszerűvé, ezáltal tervezhetővé, értékelhetővé és ellenőrizhetővé teszi az informatikai rendszerek üzemeltetésének fejlettségi szintjét. A modell egy valamennyi folyamatra alkalmazható, általános hatfokozatú skálát határoz meg, amelyben az egyes fokozatok ismérvei verbálisan definiáltak[63].

## 4.3 A kialakított mutatószám rendszer

### 4.3.1 A mutatószám rendszer általános tulajdonságai

A korábbiakban rögzítettek szerint, a minősítési rendszernek a működésfolytonosság állapotának fejlettségét, érettségét kell kifejeznie, így megfelelő módosításokkal a minősítésre alkalmas a COBIT érettségi modellhez hasonló, annak koncepcióját követő minősítési rendszer.

Az 1/4. ábrán bemutatott rendszer egyaránt vonatkozhat a működési folyamatokra és a működési folyamatokat integráló szervezet funkcionalitásaira. A 4.1 pontban megfogalmazottaknak megfelelően a mutatószámok kialakításakor a szervezet funkcionalitásaira fókuszálunk. A 1.6.2 pontban megadott alappilléreknek megfelelően a működésfolytonosság három alappillérre támaszkodik. Kézenfekvő, hogy az egyes alappillérekhez egy-egy olyan mutatószámot rendeljünk, amely az illető alappillér érettségi szintjét reprezentálja. Így a mutatószám rendszer összesen három konkrét, a COBIT-ban szereplő szintek számával megegyező számú szintet reprezentáló számból áll, ami megfelel a 4.1 pontban megfogalmazott követelményeknek.

Mindezeknek megfelelően egy szervezet működésfolytonossága egy rendezett számhármassal jellemezhető, amelynek segítségével különböző szervezetek működésfolytonossági állapotai megfelelőképpen összevethetők. Egy adott szervezeten belül az egyes számértékek nyilvánvalóan időről időre változnak, így a számértékek követésével lehetővé válik a működésfolytonosság időbeli változásának követése, valamint adott időtávra vonatkozó célok rögzítése is.

Mivel az eddigiek szerint a védelmi és a polgári szféra, illetve ennek megfelelően a kritikus infrastruktúrák területén megvalósuló működés, valamint a mindennapi folyamatos rutinszerű, illetve művelet-orientált működés működésfolytonossági

[63] A verbálisan definiált szintekbe történő besorolást a gyakorlatban célszerű támogatni megfelelően kidolgozott kérdőív/űrlap rendszerrel, valamint az ezeken rögzítettekre épülő számítási eljárásokkal. (Például felmérhető egy meghatározott időszakra vonatkozóan a működésfolytonossági problémák száma, az oktatásban részt vett munkatársak és az összes munkatárs aránya stb.)

szempontból több ponton is eltérő tulajdonsággal rendelkezik, nem lehetséges, hogy valamennyi változatra azonos verbálisan megadott minőségi szinteket definiáljunk. Az eltérő tulajdonságok miatt mindenképpen meg kell különböztetnünk a mindennapi, rutinszerű, illetve művelet-orientált működésekhez tartozó minősítések alapjául szolgáló jellemzőket.

A mindennapi, rutinszerű működési folyamatok egyaránt jellemzőek lehetnek mind a védelmi, mind a polgári szférára, illetve a kritikus infrastruktúrák területén történő működésre. Bármelyik szférába tartoznak is az eddigiek szerint nincsenek közöttük akkora különbségek, hogy ne lehetne azonos, verbálisan megadott szintekhez rendelni őket. Hasonlók mondhatók el a művelet-orientált tevékenységek esetére. Ezek az eddigiek szerint akár a védelmi, akár a polgári szférába, illetve a kritikus infrastruktúrák területéhez tartoznak, csak akkora különbségekkel rendelkeznek, hogy alkalmazhatók rájuk azonos, verbálisan megadott szintek.

Mindezeknek megfelelően összesen kétféle verbálisan megadott minősítési szint rendszert szükséges kialakítani, az egyik a normál mindennapi folyamatos működéhez, a másik pedig a művelet-orientált működéshez alkalmazható.

### 4.3.2 A normál, mindennapi folyamatos működéshez tartozó mutatószám rendszer

A normál, mindennapi folyamatos működés típusú tevékenységek esetére az egyes alappillérek minősítéséhez a következő szintek illetve verbális jellemzők alkalmazhatók. [38]

| Erőforrások beszerzése és üzemeltetése | |
|---|---|
| **0 Nem létező** | A szervezetben nem lelhető fel az a felismerés, hogy az erőforrások beszerzése és üzemeltetése összefüggésben van a működésfolytonossággal. Teljesen hiányzik az erőforrások beszerzésére és üzemeltetésére vonatkozó bármiféle koncepció. Beszerzések esetén működésfolytonossági szempontok nem merülnek fel, az informatikai üzemeltetés kizárólag reaktív jellegű, a kiesések megelőzését az üzemeltetés nem tekinti feladatának. |
| **1 Ad hoc jellegű** | Bár a szervezet vezetése tudatában van annak, hogy az informatikai erőforrások beszerzéséhez és üzemeltetéséhez kapcsolódó kérdések befolyásolják a működésfolytonosságot, ezekre vonatkozóan nincsenek a működésfolytonossági szempontok figyelembe vételét támogató szempontrendszerek illetve jól definiált eljárásrendek. Az erőforrások beszerzésekor működésfolytonossági szempontok (pl. tartalékok beszerzése, magas megbízhatósággal rendelkező eszközök) csak időnként, és csak ad hoc módon vannak figyelembe véve. Az üzemeltetés többnyire reaktív jellegű, a kiesések megelőzését az üzemeltetés általában nem tekinti feladatának. |
| **2 Ötlet-szerű** | A szervezet általános szinten tisztában van azzal, hogy az informatikai erőforrások beszerzése és üzemeltetése befolyásolja a működésfolytonosságot. Az erőforrások beszerzésekor működésfolytonossági szempontok többnyire figyelembe vannak véve, de mindez csak ad hoc módon történik, ugyanis ezekre vonatkozóan nem létezik jól definiált szempontrendszer. Az üzemeltetés során bizonyos kérdésekben felismerhető a proaktív jelleg, előfordulnak a meghibásodások megelőzésének céljából végrehajtott karbantartások, továbbá olyan alkalmazások (pl. vírusvédelmi megoldások), illetve redundanciák (pl. hibatűrő diszk alrendszerek), amelyek a kifejezetten a kiesések elkerülését támogatják. Mindezek azonban csak ötletszerűen valósulnak meg, a beszerzésekre és az üzemeltetésre vonatkozó a teljes problémakört lefedő szempontrendszer nem lett kialakítva. |
| **3 Hiányos** | Az informatikai erőforrások beszerzésének és üzemeltetésnek összefüggése a működésfolytonossággal ismert és elfogadott a szervezetben. Folyamatban van az erőforrások beszerzésére vonatkozó általános, működésfolytonossági szempontrendszert is tartalmazó szabályzatok kidolgozása, de a szempontrendszer nem tekinthető teljes körűnek. Az üzemeltetés folyamán érvényesül a proaktív szemlélet, az üzemeltetés a kiesések megelőzését fontos feladatának tekinti, de erre vonatkozóan nem rendelkezik általános koncepcióval. Az üzemeltetés színvonalának mérésére vonatkozóan nem működik egységes értékelési eljárás, az üzemeltetés ellenőrzésére csupán utólagos jelleggel kerül sor olyan esetek kapcsán, amelyek nyomán veszteségek keletkeztek, illetve amelyek zavart okoztak a szervezet működésében. |

| | |
|---|---|
| **4 Megfelelő** | A szervezet legtöbb szintjén teljes mértékben tisztában vannak azzal, hogy az informatikai erőforrások beszerzése és üzemeltetése összefüggésben van a működésfolytonossággal. A felsővezetés általánosságban ismeri, hogy az informatikai erőforrások megfelelő működése milyen értékekkel járul hozzá a szervezettől elvárt kritikus funkcionalitásokhoz, illetve azzal, hogy a kiesések számottevő veszteségeket okozhatnak. Az informatikai erőforrások beszerzéséhez a működésfolytonossági szempontokat is tartalmazó kidolgozott szempontrendszer áll rendelkezésre, amelyet minden beszerzéskor kötelezően figyelembe is vesznek. Az informatikai erőforrások üzemeltetésének eljárásai szabványosítottak és dokumentáltak, azonban bizonyos vezetői pozícióban levő személyek saját szakmai tapasztalataik alapján határozzák meg az informatikai rendszerek üzemeltetésének irányítási módját, e kérdésben nem követnek szabványokat. A szabványosított eljárások elsajátításának érdekében megfelelő képzési formákat alakítottak ki. Az üzemeltetés színvonalára vonatkozóan méréseket nem, vagy csak korlátozottan végeznek, de a mérési adatokat többnyire nem használják semmire. |
| **5 Optimális** | A szervezet minden szintjén teljes mértékben tisztában vannak azzal, hogy az informatikai erőforrások beszerzése és üzemeltetése összefüggésben van a működésfolytonossággal. A felsővezetés teljes mértékben tudatában van annak, hogy az informatikai erőforrások megfelelő működése milyen értékekkel járul hozzá a szervezettől elvárt kritikus funkcionalitásokhoz, illetve, hogy a kiesések milyen veszteségekkel járnak. A beszerzési és üzemeltetési eljárásokat külső normák alapján alakítják, a folyamatos fejlesztések és a más szervezetekhez viszonyított érettségi modellek eredményei alapján. A beszerzések az informatikai stratégiából vannak levezetve, megvalósításuk az általános beruházási eljárásoknak megfelelően történik, a konkrét beszerzési eljárásokhoz kötelezően alkalmazandó, működésfolytonossági szempontokat is tartalmazó kidolgozott szempontrendszer áll rendelkezésre. Az üzemeltetés ismert és általánosan elfogadott szabványokon alapul (pl. ITIL [79], Information Technology Infrastructure Library). Az üzemeltetést végző személyzet számára a képzettségre vonatkozóan előírások léteznek, az üzemeltetők továbbképzése rendszeresen megtörténik. Az üzemeltetésre vonatkozóan mérési eljárásokat alakítottak ki, a mérési adatokat nyilvántartják és elemzik, a fejlesztések során ezeket figyelembe veszik. |

4/1 táblázat – A mindennapi folyamatos működéshez tartozó mutatószám rendszer - Erőforrások beszerzése és üzemeltetése

| Szabályozások (szervezet és irányítás) | |
|---|---|
| **0 Nem létező** | Az informatikai erőforrásokhoz és folyamatokhoz kapcsolódó dokumentált, formális szabályozások egyáltalán nem léteznek. A vezetés fel sem ismerte, hogy a működésfolytonosság egyik feltétele a megfelelő szabályozottságok alapján történő működés. A szervezeten belül informatikai szervezet egyáltalán nem létezik. |
| **1 Kezdeti/ Formális** | A szervezet általánosságban felismerte, hogy többek között a működésfolytonosság biztosításának érdekében szükség van az informatikai működés szabályozására. A szabályzatok egy részének első változata kidolgozás alatt van, vagy már elkészült, de csak formálisan. A formálisnak tekinthető szabályzatok hiányosak, nem terjednek ki minden részletre, konkrétumokat nem, csak általánosságokat tartalmaznak, vagy egy másik szervezet számára készített szabályzat adaptálásával jöttek létre és a gyakorlatban nyilvánvalóan használhatatlanok. A szabályzat készítésén/elkészítésén túlmenően a gyakorlatban való használhatóságot elősegítő semmiféle erőfeszítés nem történt, a szabályzatok megfelelő kommunikálása, a rájuk vonatkozó felkészítés nem történt meg. A szabályzatokat nem ismerik azok, akikre vonatkoznak, az informatikai működés nem is ezek szerint folyik. Informatikai szervezet nem létezik, de bizonyos pozíciókhoz informatikai üzemeltetési feladatok (is) vannak rendelve. |
| **2 Ötlet-szerű** | A szervezet általános szinten tisztában van azzal, hogy a működésfolytonosság egyik feltétele a szabályok alapján történő működés. Az informatikai működésnek azonban csak egy része szabályozott (pl. csak a rendszerek egy részére létezik rendszerszintű informatikai biztonsági szabályzat), fontos szabályzatok egyáltalán nem léteznek. Az elkészített szabályzatokra vonatkozó felkészítés megtörténik, a munkatársak, parancsnok és beosztottak többnyire ismerik a rájuk vonatkozó szabályokat. A szabályozott területeken a működés többé-kevésbé a szabályzatok szerint folyik, de a szabályzatok betartásra vonatkozóan ellenőrzések nem léteznek. A szabályzatok felülvizsgálata legfeljebb csak ötletszerűen történik. Kezdetleges informatikai szervezet került kialakításra, de ebben a felelősségek, hatáskörök, hierarchia stb. nem egyértelmű. |
| **3 Ellent-mondá-sos/Hi-ányos** | Tudott és elfogadott a szervezetnél hogy a működésfolytonosság egyik feltétele a szabályok alapján történő működés. Emiatt az informatikai működés legtöbb összetevője szabályozott, azonban az egyes szabályozások között ellentmondások léteznek, illetve maradnak szabályozatlan területek. Az elkészített szabályzatokra vonatkozó felkészítés megtörténik, a szabályozott területeken a működés általában a szabályzatok szerint folyik. Bár a munkatársak, parancsnokok és beosztottak többnyire ismerik a rájuk vonatkozó szabályokat, az ellentmondások és hiányosságok miatt előfordul, hogy a működés a gyakorlatban nem a szabályzatok szerint folyik. A szabályzatok betartásra vonatkozóan ellenőrzések nem jellemzőek. Az informatikai szervezetben levő pozíciók feladatai, hatáskörei, a hozzájuk rendelt erőforrások nem pontosan meghatározottak, az informatikai szervezet nem megfelelően épül be a szervezeti hierarchiába, több irányból, egymásnak ellentmondó feladatokat kaphat. |

| | |
|---|---|
| **4 Megvalósított** | A szervezet legtöbb szintjén teljes mértékben tisztában vannak azzal, hogy az informatikai működés szabályozása összefüggésben van a működésfolytonossággal. Az informatikai működés minden összetevője szabályozott, a szabályzatok kialakítása ismert és elfogadott szabványok alapján történik. Az informatikai szervezetben levő pozíciók feladatai, hatáskörei, a hozzájuk rendelt erőforrások többnyire jól definiáltak, az informatikai szervezet szervezeti hierarchiába való tagozódása egyértelmű. Az elkészített szabályzatokra vonatkozó felkészítés megtörténik, azonban ez nem terjed ki az egész szervezetre. A beosztottak többnyire ismerik a rájuk vonatkozó szabályokat, a működés a kialakított szabályzatoknak megfelelően folyik. A szabályzatok betartására vonatkozóan rendszeresek az ellenőrzések, eltérések esetén szankcionálások léteznek. Az ellenőrzések tapasztalatai beépülnek a szabályozások újabb változataiba. |
| **5 Optimális** | A szervezet minden szintjén teljes mértékben tisztában vannak azzal, hogy az informatikai működés szabályozása összefüggésben van a működésfolytonossággal. Folyamatosan fejlesztik és összehangolják a szabályozásokat. A szabályzatok kialakításakor és fejlesztésekor az ismert és elfogadott szabványok előírásain túlmenően figyelembe veszik a saját működésben szerzett tapasztalatokat, más szervezetek tapasztalatait és a legújabb kutatási eredményeket. A felkészítés kiterjed az egész szervezetre, minden munkatárs, parancsnok és beosztott részesül felkészítésben, az oktatásokhoz hozzátartozik az ismeretek számonkérése is. A munkatársak, parancsnokok és beosztottak teljes mértékben ismerik a rájuk vonatkozó szabályokat, a működés a kialakított szabályzatoknak megfelelően folyik. A szabályzatok betartására vonatkozóan folyamatos ellenőrzések vannak végrehajtva, eltérések esetén formalizált eljárásokon alapuló szankcionálások léteznek. Az ellenőrzések tapasztalatai beépülnek a szabályozások újabb változataiba. |

4/2. táblázat – A mindennapi folyamatos működéshez tartozó mutatószám rendszer - Szabályozások (szervezet és irányítás)

| Katasztrófa helyzet kezelés | |
|---|---|
| **0 Nem létező** | Teljesen hiányzik az informatikai katasztrófa helyzetek kezelésére utaló bármilyen eljárás, illetve elképzelés. A szervezet nem ismerte fel még azt sem, hogy foglalkozni kellene ezzel a kérdéssel. |
| **1 Kezdeti/ Formális** | A szervezet általánosságban felismerte, hogy a működésfolytonosság biztosításának érdekében szükség van az informatikai katasztrófa helyzet esetén alkalmazható tervre. A terv első változata kidolgozás alatt van, vagy már elkészült, de csak formálisan. A formálisnak tekinthető terv hiányos (tipikusan üres vagy hiányos táblázatok fordulnak elő benne), konkrétumokat nem, csak általánosságokat tartalmaz, vagy egy másik szervezet számára készített terv adaptálásával jött létre és a gyakorlatban nyilvánvalóan használhatatlan. A terv készítésén/elkészítésén túlmenően a gyakorlatban való használhatóságot elősegítő semmiféle erőfeszítés nem történt, a szükséges felkészítés, a tesztelések kérdése szóba sem került. |
| **2 Túlhala-dott/Hi-bás** | A szervezet tudatában van annak, hogy a működésfolytonosság egyik feltétele az informatikai katasztrófa helyzetek esetén alkalmazható terv készítés. Létezik ugyan katasztrófa terv, de elkészítése óta már hosszabb idő (több év) telt el és a szükséges frissítések nem lettek végrehajtva. A terv készítéséhez alkalmazott módszertan túlhaladott vagy hibás, elkészítését nem előzte meg kockázatelemzés, a tervből fontos összetevők, illetve adatok hiányoznak, a konkrét adatok nem aktualizáltak. Nincs kialakítva megfelelő katasztrófa kezelő szervezet. A megnevezett szervezeti egységek, objektumok, folyamatok, pozíciók nem felelnek meg a gyakorlatban megvalósulóknak. Nyilvánvalóan nagy valószínűséggel bekövetkező katasztrófa eseményekre nincsenek kidolgozott akciótervek. A tervben szereplő felelősök nincsenek tisztában azzal, hogy katasztrófa helyzet esetén a katasztrófa kezelő eljárásban érintettek. A katasztrófa helyzet kezelésére vonatkozóan felkészítés nem volt, a terv működésére vonatkozóan tesztek nem lettek végrehajtva. |
| **3 Kezdet-leges** | A szervezet tudatában van és elfogadja, hogy a működésfolytonosság egyik feltétele az informatikai katasztrófa helyzetekre való megfelelő felkészülés. Kvalitatív kockázatelemzésen alapuló katasztrófa terv létezik, amely bizonyos katasztrófa események esetén a gyakorlatban is használható. A katasztrófa terv ismert és általánosan elfogadott módszertan alapján készült, nyilvánvaló hibákat nem tartalmaz, a benne rögzített adatok döntő többsége megfelel a gyakorlatban megvalósuló helyzetnek. A terv fejlesztése, a változások követése ötletszerűen történik, hozzá tartozóan nincsenek jól definiált változáskövetési eljárások. A tervben szereplő felelősök részben ismerik az informatikai katasztrófa helyzetben előálló feladataikat, felelősségeiket, a rendelkezésükre álló erőforrásokat és helyüket a katasztrófa kezelő szervezetben. A katasztrófa helyzetre való felkészülésre vonatkozóan időnként léteznek oktatások, ezek azonban többnyire csak a gyakorlatban nem használható általánosságokat tartalmaznak. A felkészítés nem terjed ki az egész szervezetre, bizonyos munkatársak, parancsnokok és beosztottak a felkészítésből kimaradnak (pl. új beosztottak). A katasztrófa tervben megfogalmazott akciótervek tesztelése nem vagy csak formálisan történik meg. |

| | |
|---|---|
| **4 Hasz-nálható** | A szervezet minden szintjén tisztában vannak azzal, hogy a működésfolytonosság egyik feltétele az informatikai katasztrófa helyzetekre való megfelelő felkészülés. Kockázatelemzésen alapuló katasztrófa terv létezik, amely katasztrófa események többségének bekövetkezése esetén a gyakorlatban is használható. A katasztrófa terv ismert és általánosan elfogadott módszertan alapján készült, nyilvánvaló hibákat nem tartalmaz, a benne rögzített adatok döntő többsége megfelel a gyakorlatban megvalósuló helyzetnek. A terv fejlesztése, a változások követése időben periódikusan (pl. évente) megtörténik. A tervben szereplő felelősök teljes mértékben ismerik az informatikai katasztrófa helyzetben előálló feladataikat, felelősségeiket, a rendelkezésükre álló erőforrásokat és helyüket a katasztrófa kezelő szervezetben. A katasztrófa helyzetre való felkészülésre vonatkozóan jól definiált ütemezés szerint léteznek felkészítések, amelyek az általános ismereteken túlmenően a felelősök számára a konkrét ismereteket is tartalmazzák. A felkészítés kiterjed az egész szervezetre, minden munkatárs, parancsnok és beosztott részesül felkészítésben, az egyes akciótervekben szereplő felelősök felkészítéséhez számonkérés is tartozik. A katasztrófa tervben megfogalmazott akciótervek tesztelése időnként megtörténik, a tesztelések eredményei kiértékelésre kerülnek. |
| **5 Optimá-lis** | A szervezet nemcsak annak van tudatában, hogy a működésfolytonosság egyik feltétele az informatikai katasztrófa helyzetekre való megfelelő felkészülés, hanem azzal is, hogy a kérdéskör menedzselésének egy jól definiált folyamat keretében kell megvalósulnia. Kvantitatív kockázatelemzésen alapuló katasztrófa terv létezik, melynek elkészítésekor és folyamatos aktualizálásakor nemcsak a saját, hanem a hasonló szervezetek tapasztalatait és a legújabb kutatások eredményeit is figyelembe veszik. A terv a katasztrófa események döntő többsége esetén a gyakorlatban is használható. Ismert és általánosan elfogadott módszertan alapján készült, a benne előforduló hibák száma minimális, a rögzített adatok kivétel nélkül megfelelnek a gyakorlatban megvalósuló helyzetnek. A terv fejlesztése, a változások követése időben periodikusan (pl. évente), valamint a tervet érintő változások (pl. személyi vagy szervezeti változások) esetén haladéktalanul megtörténik. A tervben szereplő felelősök teljes mértékben ismerik az informatikai katasztrófa helyzetben előálló feladataikat, felelősségeiket, a rendelkezésükre álló erőforrásokat és helyüket a katasztrófa kezelő szervezetben. A katasztrófa helyzetre való felkészülésre vonatkozóan jól definiált ütemezés szerint illetve a változásokhoz kapcsolódóan léteznek felkészítések, amelyek az általános ismereteken túlmenően a felelősök számára a konkrét ismereteket is tartalmazzák. A felkészítés kiterjed az egész szervezetre, minden munkatárs, parancsnok és beosztott részesül felkészítésben, az egyes akciótervekben szereplő felelősök felkészítéshez számonkérés is tartozik. A katasztrófa tervben megfogalmazott akciótervek tesztelése jól definiált időközönként és a változásokhoz kapcsolódóan megtörténik, a tesztelések eredményei kiértékelésre kerülnek, szükség esetén automatikusan javítást eredményező lépések (pl. újabb felkészítések vagy beszerzések) indulnak. |

4/3 táblázat – A mindennapi folyamatos működéshez tartozó mutatószám rendszer - Katasztrófa helyzet kezelés

### 4.3.3 A művelet-orientált működéshez tartozó mutatószám rendszer

A művelet-orientált működés típusú tevékenységek esetére az egyes alappillérek minősítéséhez a következő szintek, illetve verbális jellemzők alkalmazhatók.

| Erőforrások beszerzése és üzemeltetése | |
|---|---|
| **0 Nem létező** | A művelet-orientált működés tervezésekor és a működés folyamán hiányzik az a felismerés, hogy az erőforrások biztosítása és üzemeltetése összefüggésben van a működésfolytonossággal. Teljesen hiányzik az erőforrások biztosítására és üzemeltetésére vonatkozó bármiféle koncepció. A tervezés alatt és az erőforrások biztosítása, beszerzése esetén működésfolytonossági szempontok nem merülnek fel, tartalékok, redundanciák nem léteznek, az informatikai üzemeletetés kizárólag reaktív jellegű, a kiesések megelőzését az üzemeltetés nem tekinti feladatának. |
| **1 Ad hoc jellegű** | Bár a művelet-orientált tevékenység vezetése tudatában van annak, hogy az informatikai erőforrások biztosításához és üzemeltetéséhez kapcsolódó kérdések befolyásolják a működésfolytonosságot, a kitűzött célok határidőre való elérését, erre vonatkozóan a tervezés folyamán nincsenek a működésfolytonossági szempontok figyelembe vételét támogató szempontrendszerek definiálva. Az erőforrások művelet-orientált tevékenységhez való rendelésekor, illetve beszerzésekor működésfolytonossági szempontok (pl. tartalékok beszerzése, magas megbízhatósággal rendelkező eszközök) csak időnként, és csak ad hoc módon vannak figyelembe véve. Gyakori konfliktusokat, esetlegesen kieséseket okoz, hogy az erőforrások használata nincs összehangolva más művelet-orientált tevékenységgel, illetve a normál mindennapi működéssel. Az üzemeltetés többnyire reaktív jellegű, a kiesések megelőzését az üzemeltetés általában nem tekinti feladatának. |
| **2 Ötlet-szerű** | A művelet-orientált tevékenység vezetése általános szinten tisztában van azzal, hogy az informatikai erőforrások biztosítása és üzemeltetése befolyásolja a működésfolytonosságot, döntően hozzájárul a kitűzött célok határidőre történő eléréséhez. Az erőforrások biztosításakor működésfolytonossági szempontok többnyire figyelembe vannak véve, tartalékok, redundanciák többnyire léteznek, de mindez jól definiált szempontrendszer hiányában csak ad hoc módon történik. Az üzemeltetés során bizonyos kérdésekben felismerhető a proaktív jelleg, előfordulnak a meghibásodások megelőzésének céljából végrehajtott karbantartások, továbbá olyan alkalmazások (pl. vírusvédelmi megoldások) illetve redundanciák (pl. hibatűrő diszk alrendszerek), amelyek kifejezetten a kiesések elkerülését támogatják. Mindezek azonban csak ötletszerűen valósulnak meg, a beszerzésekre és az üzemeltetésre vonatkozó, a teljes problémakört lefedő szempontrendszer nem lett kialakítva. Előfordul, hogy konfliktusokat okoz, hogy az erőforrások használata nincs összehangolva más művelet-orientált tevékenységgel, illetve a normál mindennapi működéssel. A működés során fellépő, előre nem látott erőforrás igények tipikusan a működésfolytonosság biztosításra allokált tartalékok rovására vannak kielégítve. |

| | |
|---|---|
| **3 Hiányos** | Az informatikai erőforrások beszerzésének és üzemeltetésének összefüggése a működésfolytonossággal ismert és elfogadott a tervezés során és a művelet-orientált tevékenységet megvalósító alakulatban, szervezetben. A tervezés során megtörténik az erőforrások beszerzésére, illetve biztosítására vonatkozó általános, működésfolytonossági szempontrendszert is tartalmazó beszerzési terv kidolgozása, de a szempontrendszer nem tekinthető teljes körűnek. Az üzemeltetés folyamán érvényesül a proaktív szemlélet, az üzemeltetés a kiesések megelőzését fontos feladatának tekinti, de erre vonatkozóan nem rendelkezik általános koncepcióval. Az üzemeltetés színvonalának mérésére vonatkozóan nem működik egységes értékelési eljárás, az üzemeltetés ellenőrzésére csupán utólagos jelleggel kerül sor olyan esetek kapcsán, amelyek nyomán kiesések keletkeztek, illetve amelyek zavart okoztak a működésében. Gyakori, hogy a működés során fellépő, előre nem látott erőforrás igények tipikusan a működésfolytonosság biztosítására allokált tartalékok rovására vannak kielégítve. |
| **4 Megfelelő** | A tervezés során és a művelet-orientált tevékenységet megvalósító alakulatban, szervezetben legtöbb szinten teljes mértékben tisztában vannak azzal, hogy az informatikai erőforrások biztosítása és üzemeltetése összefüggésben van a működésfolytonossággal, feltétele a kitűzött célok határidőre történő elérésének. A művelet-orientált tevékenység vezetése általánosságban ismeri, hogy az informatikai erőforrások megfelelő működése milyen értékekkel járul hozzá az elérendő célokhoz és határidőkhöz. Az informatikai erőforrások biztosításához működésfolytonossági szempontokat is tartalmazó kidolgozott szempontrendszer áll rendelkezésre, amelyet kötelezően figyelembe is vesznek. Az informatikai erőforrások üzemeltetésének eljárásai pontosan definiáltak és dokumentáltak. Előfordul azonban, hogy bizonyos vezetői pozícióban levő személyek saját szakmai tapasztalataik alapján határozzák meg az informatikai rendszerek üzemeltetésének irányítási módját, e kérdésben nem követik az előre definiált eljárásokat. Az előre definiált üzemeltetési eljárásokhoz megfelelő felkészítési formákat alakítottak ki. Az üzemeltetés színvonalára vonatkozóan méréseket nem vagy csak korlátozottan végeznek, de a mérési adatokat többnyire nem használják semmire. Előfordul, hogy a működés során fellépő, előre nem látott erőforrás igények a működésfolytonosság biztosításra allokált tartalékok rovására vannak kielégítve. |

| | |
|---|---|
| **5 Optimá-lis** | A tervezés során és a művelet-orientált tevékenységet megvalósító alakulat, szervezet minden szintjén teljes mértékben tisztában vannak azzal, hogy az informatikai erőforrások biztosítása és üzemeltetése összefüggésben van a működésfolytonossággal, alapvetően meghatározza a kitűzött célok határidőre történő elérését. A művelet-orientált tevékenység vezetése teljes mértékben tudatában van annak, hogy az informatikai erőforrások megfelelő működése milyen értékekkel járul hozzá a kitűzött célok határidőre történő eléréséhez. Az erőforrások biztosításának, beszerzésének és üzemeltetésének eljárásait külső normák alapján alakítják, a folyamatos fejlesztések és a más hasonló művelet-orientált tevékenységekhez viszonyított érettségi modellek eredményei alapján. Az erőforrások biztosítása, illetve beszerzése a művelet-orientált tevékenyég céljaiból vannak levezetve, a konkrét eljárásokhoz kötelezően alkalmazandó, működésfolytonossági szempontokat is tartalmazó kidolgozott szempontrendszer áll rendelkezésre. Az üzemeltetés ismert és általánosan elfogadott szabványokon alapul (pl. ITIL [79], Information Technology Infrastructure Library). Az üzemeltetést végző pozíciókat betöltő személyek számára a képzettségre vonatkozóan előírások léteznek, az üzemeltetők továbbképzése rendszeresen megtörténik. Az üzemeltetésre vonatkozóan mérési eljárásokat alakítottak ki, a mérési adatokat nyilvántartják és elemzik. Az erőforrások használata teljes mértékben össze van hangolva más művelet-orientált tevékenységgel, illetve a normál mindennapi működéssel. Nem fordul elő, hogy a működés során fellépő, előre nem látott erőforrás igények a működésfolytonosság biztosításra allokált tartalékok rovására vannak kielégítve. |

4/4 táblázat - A művelet-orientált működéshez tartozó mutatószám rendszer - Erőforrások beszerzése és üzemeltetése

| Szabályozások (szervezet és irányítás) | |
|---|---|
| **0 Nem létező** | Az informatikai erőforrásokhoz és folyamatokhoz kapcsolódó dokumentált, formális szabályozások egyáltalán nem léteznek. A művelet-orientált tevékenység vezetése fel sem ismerte, hogy a működésfolytonosság, a kitűzött célok határidőre történő elérésének egyik feltétele a megfelelő szabályozottságok alapján történő működés. Az informatikai feladatok ellátását végző informatikai szervezet a művelet-orientált tevékenységet végrehajtó szervezeten belül nincs kialakítva. |
| **1 Kezdeti/ Formális** | A művelet-orientált tevékenységet végző alakulat, szervezet általánosságban felismerte, a tevékenység tervezés során azonban nem szerepelt szempontként, hogy többek között a működésfolytonosság biztosításának, a kitűzött célok határidőre történő elérésének érdekében szükség van az informatikai működés szabályozására. A formálisnak tekinthető szabályzatok hiányosak, nem terjednek ki minden részletre konkrétumokat nem, csak általánosságokat tartalmaznak, vagy egy másik művelet-orientált, illetve mindennapi folyamatos tevékenységre vonatkozó szabályzatok adaptálásával jöttek létre és a gyakorlatban nyilvánvalóan használhatatlanok. A szabályzatok megfelelő kommunikálása, oktatása, a szükséges felkészítések nem történtek meg. A szabályzatokat nem ismerik azok, akikre vonatkoznak, az informatikai működés nem ezek szerint folyik. Az informatikai feladatok ellátását végző informatikai szervezet a művelet-orientált tevékenységet végrehajtó szervezeten belül nincs kialakítva, azonban bizonyos pozíciókhoz informatikai üzemeltetési feladatok (is) vannak rendelve. |
| **2 Ötlet-szerű** | A művelet-orientált tevékenységet végző, tervező alakulat, szervezet általános szinten tisztában van azzal, hogy a működésfolytonosság biztosításnak, a kitűzött célok határidőre történő elérésének egyik feltétele a szabályok alapján történő működés. Az informatikai működésnek azonban csak egy része szabályozott (pl. csak a rendszerek egy részére létezik rendszerszintű informatikai biztonsági szabályzat), fontos szabályzatok egyáltalán nem léteznek, illetve az egyes szabályzatok között ellentmondások vannak. Az elkészített szabályzatok oktatása, kommunikálása, a hozzájuk tartozó felkészítés megtörténik, az egyes pozíciókat betöltő személyek többnyire ismerik a rájuk vonatkozó szabályokat. A változáskezelés egyáltalán nem szabályozott. A szabályozott területeken a működés többé-kevésbé a szabályzatok szerint folyik, de a szabályzatok betartására vonatkozóan nincsenek ellenőrzések. |

| | |
|---|---|
| **3 Ellent-mondá-sos/Hi-ányos** | Tudott és elfogadott a művelet-orientált tevékenységet végző alakulatban, szervezetben, hogy a működésfolytonosság, a kitűzött célok határidőre történő elérésének egyik feltétele a szabályok alapján történő működés. Emiatt az informatikai működés legtöbb összetevője szabályozott, azonban az egyes szabályozások között ellentmondások léteznek, illetve maradnak szabályozatlan területek. Az elkészített szabályzatokhoz kapcsolódó felkészítés megfelelő, a szabályozott területeken a működés általában a szabályzatok szerint folyik. A változáskezelés szabályozása kezdetleges szinten valósul meg. Az informatikai szervezetben levő pozíciók feladatai, hatáskörei, a hozzájuk rendelt erőforrások nem pontosan meghatározottak, más művelet-orientált tevékenységek, illetve a normál mindennapi működés feladataival gyakran ellentmondásban vannak. Bár az egyes pozíciókat betöltő személyek többnyire ismerik a rájuk vonatkozó szabályokat, az ellentmondások és hiányosságok miatt előfordul, hogy a működés a gyakorlatban nem a szabályzatok szerint folyik. A szabályzatok betartásra vonatkozóan ellenőrzések nem jellemzőek. |
| **4 Megva-lósított** | A művelet-orientált tevékenységet végző alakulat, szervezet legtöbb szintjén és a tevékenység tervezésekor teljes mértékben tisztában vannak azzal, hogy az informatikai működés szabályozása összefüggésben van a működésfolytonossággal, a kitűzött célok határidőre történő elérésének egyik feltétele a szabályok alapján történő működés. Az informatikai működés minden összetevője szabályozott, a szabályzatok kialakítása ismert és elfogadott szabványok alapján történik. A változáskezelés megfelelőképpen szabályozott. Az elkészített szabályzatokhoz kapcsolódó felkészítés megfelelőképpen megvalósul. Az informatikai szervezetben levő pozíciók feladatai, hatáskörei, a hozzájuk rendelt erőforrások többnyire jól definiáltak, az informatikai szervezet tagozódása az alakulat, szervezet hierarchiájába egyértelmű, más művelet-orientált tevékenységekkel, illetve a normál, mindennapi működéssel nincsenek ellentmondások. Az egyes pozíciókat betöltő személyek többnyire ismerik a rájuk vonatkozó szabályokat, a működés a kialakított szabályzatoknak megfelelően folyik. A szabályzatok betartására vonatkozóan rendszeres ellenőrzések vannak végrehajtva, eltérések esetén szankcionálások léteznek. |
| **5 Optimá-lis** | A művelet-orientált tevékenységet végző alakulat, szervezet minden szintjén teljes mértékben tisztában vannak azzal, hogy az informatikai működés szabályozása összefüggésben van a működésfolytonossággal, a kitűzött célok határidőre történő elérésének egyik feltétele a szabályok alapján történő működés. A szabályzatok kialakításakor és fejlesztésekor az ismert és elfogadott szabványokon előírásain túlmenően figyelembe veszik a hasonló művelet-orientált tevékenységek végrehajtásában szerzett tapasztalatokat és a legújabb kutatási eredményeket. A változáskezelés gyakorlata is zökkenőmentes. A szabályozásokhoz tartozó felkészítés kiterjed valamennyi pozícióra, a felkészítéshez hozzátartozik az ismeretek számonkérése is. Az egyes pozíciókat betöltő személyek teljes mértékben ismerik a rájuk vonatkozó szabályokat, a művelet-orientált működés a kialakított szabályzatoknak megfelelően folyik. A szabályzatok betartására vonatkozóan folyamatos ellenőrzéseket hajtanak végre, eltérések esetén formalizált eljárásokon alapuló szankcionálások léteznek. |

4/5 táblázat - A művelet-orientált működéshez tartozó mutatószám rendszer - Szabályozások (szervezet és irányítás)

| Katasztrófa helyzet kezelés | |
|---|---|
| **0 Nem létező** | Teljesen hiányzik az a művelet-orientált tevékenységeket fenyegető informatikai katasztrófa helyzetek kezelésére utaló bármilyen eljárás, illetve elképzelés. A művelet-orientált tevékenységet végző alakulat, szervezet nem ismerte fel még azt sem, hogy foglalkozni kellene ezzel a kérdéssel. |
| **1 Kezdeti/ Formális** | A művelet-orientált tevékenységet végző szervezet általánosságban felismerte, hogy a működésfolytonosság biztosításának érdekében, a kitűzött célok határidőre történő eléréséhez szükség van informatikai katasztrófa helyzet esetén alkalmazható tervre. Az erre vonatkozó terv azonban csak formális, a gyakorlatban használhatatlan, hiányos (tipikusan üres vagy hiányos táblázatok fordulnak elő benne), konkrétumokat nem, csak általánosságokat tartalmaz, vagy egy másik művelet-orientált tevékenység, illetve mindennapi folyamatos működésre vonatkozó terv adaptálásával jött létre. A terv készítésén/elkészítésén túlmenően a gyakorlatban való használhatóságot elősegítő semmiféle erőfeszítés nem történt, a tervre vonatkozóan oktatások, felkészítések nem lettek elvégezve. |
| **2 Túlhala-dott/Hi-bás** | A művelet-orientált tevékenységet végző szervezet tudatában van annak, hogy a működésfolytonosság, a kitűzött célok határidőre való elérésnek egyik feltétele az informatikai katasztrófa helyzetek esetén alkalmazható terv készítése. Létezik ugyan katasztrófa terv, de terv készítéséhez alkalmazott módszertan túlhaladott vagy hibás, elkészítését nem előzte meg kockázatelemzés, a tervből fontos összetevők illetve adatok hiányoznak. A megnevezett szervezeti egységek, objektumok, folyamatok pozíciók nem felelnek meg a gyakorlatban megvalósulónak. A terv önmagával és bizonyos külső körülményekkel nem konzisztens, ellentmondásokat tartalmaz. Nincs kialakítva megfelelő katasztrófa kezelő szervezet. Nyilvánvalóan nagy valószínűséggel bekövetkező katasztrófa eseményekre nincsenek kidolgozott akciótervek. A tervben szereplő kritikus pozíciót betöltő személyek nincsenek tisztában azzal, hogy katasztrófa helyzet esetén a katasztrófa kezelő eljárásban érintettek. A katasztrófa helyzethez kapcsolódóan nincsenek felkészítések. |
| **3 Kezdet-leges** | A művelet-orientált tevékenységet végző alakulat, szervezet tudatában van és elfogadja, hogy a működésfolytonosság, a kitűzött célok határidőre való elérésének egyik feltétele az informatikai katasztrófa helyzetekre való megfelelő felkészülés. Kockázatelemzésen alapuló katasztrófa terv létezik, amely bizonyos katasztrófa események esetén a gyakorlatban is használható. A katasztrófa terv ismert és általánosan elfogadott módszertan alapján készült, nyilvánvaló hibákat nem tartalmaz, a benne rögzített adatok döntő többsége megfelel a gyakorlatban megvalósuló helyzetnek, önmagával és a külső körülményekkel konzisztenciában van. Létezik a katasztrófa helyzetek kezelése céljából kialakított katasztrófa kezelő szervezet. A tervben szereplő pozíciót betöltő személyek részben ismerik az informatikai katasztrófa helyzetben előálló feladataikat, felelősségeiket, a rendelkezésükre álló erőforrásokat és helyüket a katasztrófa kezelő szervezetben. A katasztrófa helyzetek kezelésére vonatkozóan léteznek felkészítések, ezek azonban többnyire csak a gyakorlatban nem használható általánosságokat tartalmaznak. |

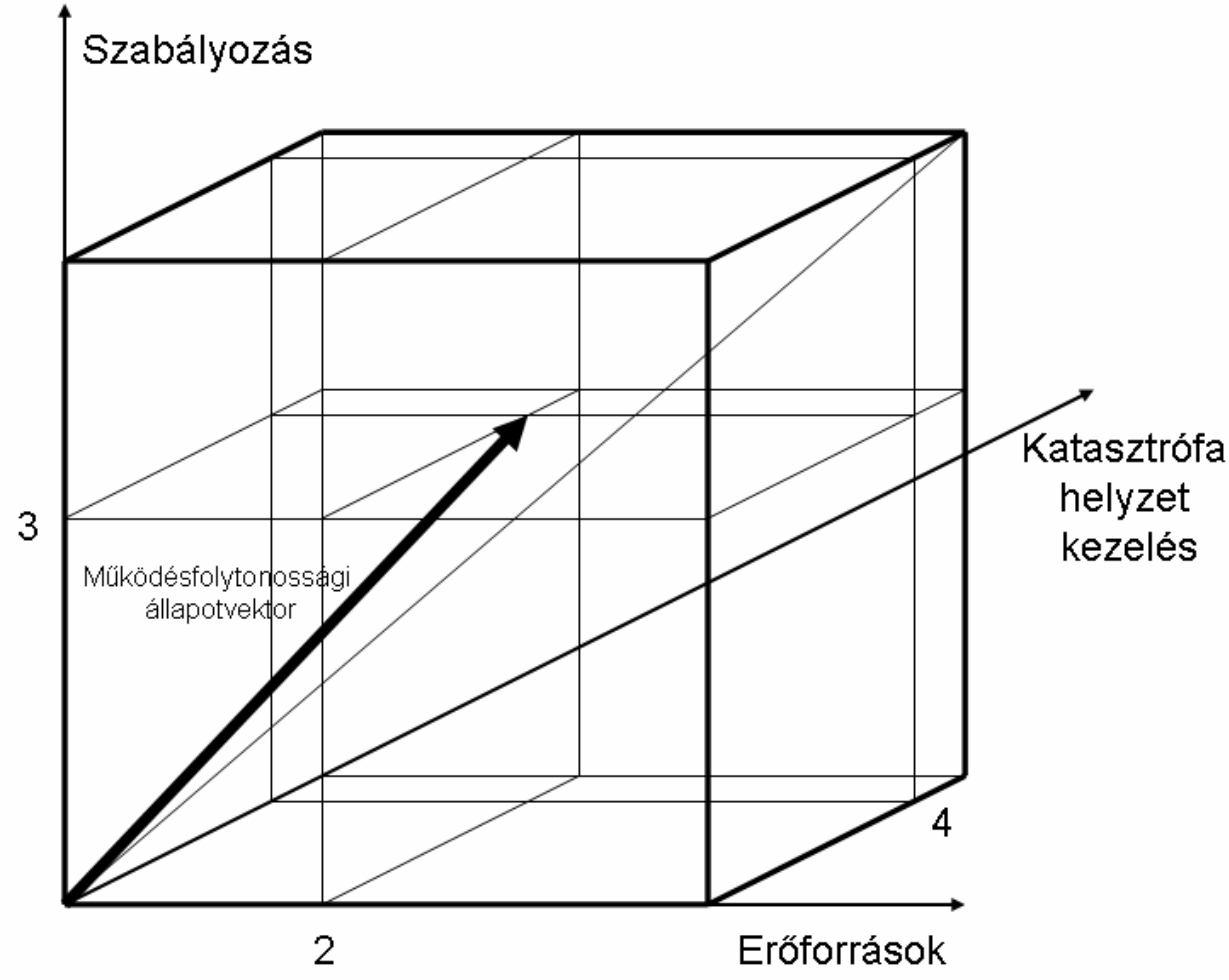
| | |
|---|---|
| **4 Hasz-nálható** | A művelet-orientált tevékenységet végző alakulat, szervezet minden szintjén tisztában vannak azzal, hogy a működésfolytonosság, a kitűzött célok határidőre való elérésnek egyik feltétele egyik feltétele az informatikai katasztrófa helyzetekre való megfelelő felkészülés. Kockázatelemzésen alapuló katasztrófa terv létezik, amely katasztrófa események többségének bekövetkezése esetén a gyakorlatban is használható. A katasztrófa terv ismert és általánosan elfogadott módszertan alapján készült, nyilvánvaló hibákat nem tartalmaz, a benne rögzített adatok döntő többsége megfelel a gyakorlatban megvalósuló helyzetnek. Jól definiált katasztrófa kezelő szervezet létezik, a szervezet minden pozíciójához pontosan hozzá vannak rendelve az elérhetőségek, felelősségek, hatáskörök és erőforrások. A tervben szereplő kritikus pozíciókat betöltő személyek teljes mértékben ismerik az informatikai katasztrófa helyzetben előálló feladataikat, felelősségeiket, a rendelkezésükre álló erőforrásokat és helyüket a katasztrófa kezelő szervezetben. A katasztrófa helyzetre vonatkozóan megfelelő felkészítések történtek a felkészítéshez számonkérés is tartozik. |
| **5 Optimá-lis** | A művelet-orientált tevékenységet végző alakulat, szervezet nemcsak annak van tudatában, hogy a működésfolytonosság, a kitűzött célok határidőre való elérésnek egyik feltétele az informatikai katasztrófa helyzetekre való megfelelő felkészülés, hanem annak is, hogy a kérdéskör menedzselésének egy jól definiált folyamat keretében kell megvalósulnia, amely végigkíséri az egész művelet-orientált tevékenységet. Kvantitatív kockázatelemzésen alapuló katasztrófa terv létezik, melynek elkészítésekor és folyamatos aktualizálásakor nemcsak a saját, hanem a hasonló művelet-orientált tevékenységek tapasztalatait és a legújabb kutatások eredményeit is figyelembe veszik. A terv a katasztrófa események döntő többsége esetén a gyakorlatban is használható. Ismert és általánosan elfogadott módszertan alapján készült, a benne előforduló hibák száma minimális, a rögzített adatok kivétel nélkül megfelelnek a gyakorlatban megvalósuló helyzetnek. A terv fejlesztése, a változások követése időben periodikusan, valamint a tervet érintő változások (pl. személyi vagy szervezeti változások) esetén haladéktalanul megtörténik. Jól definiált katasztrófa kezelő szervezet létezik, a benne szereplő kritikus pozíciókat betöltő személyek teljes mértékben ismerik az informatikai katasztrófa helyzetben előálló feladataikat, felelősségeiket, a rendelkezésükre álló erőforrásokat és helyüket a katasztrófa kezelő szervezetben. A katasztrófa helyzetre való felkészülésre vonatkozóan magas színvonalú felkészítések történnek, az egyes akciótervekben szereplő kritikus pozíciókat betöltő személyek felkészítéséhez számonkérés is tartozik. A katasztrófa tervben megfogalmazott akciótervek tesztelése jól definiált időközönként és a változásokhoz kapcsolódóan megtörténik, a tesztelések eredményei kiértékelésre kerülnek, szükség esetén automatikusan javítást eredményező lépések (pl. újabb felkészítések vagy beszerzések) indulnak. |

4/6 táblázat - A művelet-orientált működéshez tartozó mutatószám rendszer - Katasztrófa helyzet kezelés

A megadott verbális kategóriák egy-egy konkrét esetben nem feltétlenül fedik le pontosan az adott állapotot. Emiatt a nevesített diszkrét értékektől eltérő értékelések is elfogadhatók. (Például, ha egy konkrét értékelés során az állapítható meg, hogy a katasztrófa helyzet kezelés állapota valahol a 2-es és 3-as szint között helyezkedik el, és a 3-as szinthez van közelebb, akkor a numerikus értékelés lehet 2,8).

### 4.3.4 A szemléletes megjelenítés (működésfolytonossági állapotvektor)

Az előzőeknek megfelelően a működésfolytonosság egy rendezett számhármassal jellemezhető. A rendezett számhármasok szemléletessé is tehetők, azaz megjeleníthetők egy 3 dimenziós vektor formájában (működésfolytonossági állapotvektor). A vektor ábrázolható a három dimenziós koordináta rendszerben elhelyezett 5 egységnyi élű kocka belsejében a következő ábrának megfelelően.




4/1. ábra – A működésfolytonossági állapotvektor

A vektor iránya és hossza szemléletes képet ad az értékelt működésfolytonosság állapotáról. Nyilvánvaló, hogy a hosszabb vektor magasabb szintű

működésfolytonosságot reprezentál, ugyanakkor a vektor iránya is kifejező: minél inkább eltér a kocka átlójától, annál jelentősebb eltérés van az alappillérek szintjei között. (Az ábrán az erőforrások a második, a szabályozások a harmadik, a katasztrófa kezelés pedig a negyedik szintű értékelést kapta.)

A különböző szervezetek működésfolytonossági állapotai az előzőeknek felhasználásával megfelelőképpen összevethetők. Egy adott szervezeten belül a vektor hossza és iránya nyilvánvalóan időről időre változik, így felhasználásával lehetővé válik a működésfolytonosság időbeli változásának követése, valamint felhasználásával meghatározott időtávra vonatkozóan célok szemléletes kitűzése is lehetővé válik.

## 4.4 Összegzés, következtetések

Jelen fejezet az értelkezés bevezetésében rögzítetteknek megfelelően következő kutatási cél elérésére fókuszál:

*„A működésfolytonosságra vonatkozó minősítési rendszer koncepciójának kidolgozása."*[64]

A kutatási cél elérése érdekében a következő feladatokat végeztem el:

- Megvizsgáltam, hogy a működésfolytonosság aktuális állapotára vonatkozó mutatószám rendszernek milyen követelményeket kell kielégítenie.
- Meghatároztam, hogy a működésfolytonosságra vonatkozó minősítési rendszer milyen koncepcióra épülően határozható meg.

A feladatok elvégzésével a következő eredményekre jutottam:

Arra a következtetésre jutottam, hogy a működésfolytonosságot jellemző mutatószám rendszer akkor használható eredményesen, ha azon túlmenően, hogy alkalmas a működésfolytonosság aktuálisan megvalósított szintjének jellemzésére, még azt is lehetővé teszi, hogy a különböző szervezetek működésfolytonossági szintjeit összevethessük, továbbá, hogy segítségével a működésfolytonosság időbeli változásait követhessük, illetve, hogy alkalmazásával objektív célkitűzéseket fogalmazzunk meg.

Ebből kiindulva javaslatot tettem a korábbiakban ismertetett, a működésfolytonosság fő jellemzőit összefoglaló rendszerre épülő, szemléletesen ábrázolható mutatószám rendszer kialakítására, amely egy-egy szervezeten belül alkalmas a működésfolytonosság aktuális szintjének jellemzésére. Kimutattam, hogy a

[64] Lásd 7. oldal, 4. pont.

mutatószámok meghatározása a mindennapi folyamatos működés illetve művelet-orientált tevékenység egymástól eltérő kritérium rendszert igényel, ugyanakkor az a tény, hogy a tevékenység a védelmi, a polgári, illetve a kritikus infrastruktúrák területén folyik, gyakorlatilag nem befolyásolja az alkalmazható kritériumokat.

## Összefoglalás

Jelen értekezésben értelmeztem a működésfolytonosság jelentését, megállapítottam, hogy az üzletmenet folytonosság fogalmánál általánosabb, tetszőleges szférában is használható fogalom. Felismertem, hogy tárgyalása a védelmi és a polgári szféra, illetve a kritikus infrastruktúrák, valamint a normál, mindennapi rutinszerű, továbbá művelet-orientált dimenziók mentén végezhető el. Rögzítettem hogy a polgári és védelmi szféra egyre szorosabb kapcsolódása, egymástól való függősége nem teszi lehetővé, hogy a védelmi szféra működésfolytonossági kérdéseit kizárólag önmagukban vizsgáljuk, tárgyalásukkor vele együtt a polgári szféra működésfolytonossági jellemzőit is érintenünk kell. Bizonyítottam, hogy a tárgyalás során használt dimenziók mentén kisebb mértékben eltérő sajátosságok ismerhetők fel.

Rögzítettem, hogy a működésfolytonosság több más szakterülethez is kapcsolódik, illetve, hogy a legszorosabb kapcsolódás az informatikai biztonság irányában ismerhető fel. Rögzítettem továbbá, hogy a működésfolytonosság biztosítása nem egyszeri, befejezhető tevékenység, hanem folyamatos tevékenységet igényel.

Kialakítottam egy olyan rendszert, ami a működésfolytonosság viszonylag egyszerű tárgyalását és szemléltetését teszi lehetővé, tartalmazva a működésfolytonosság alappilléreit (informatikai erőforrások kezelése, szervezeti és irányítási kérdések, illetve a katasztrófa helyzetek kezelése) és megfelelő csoportosítással a kihívást jelentő veszélyforrásokat. A rendszerről megállapítottam, hogy az egyaránt használható a védelmi és a polgári szférában, így a kritikus infrastruktúravédelem területén is, mind a mindennapi folyamatos, mind pedig a művelet-orientált tevékenységek esetén.

Az informatikai biztonsághoz valamint az informatikai rendszerek üzemeltetéséhez leginkább kapcsolódó ajánlásokhoz kapcsolódóan felismertem, hogy olyan ajánlás, amely kifejezetten a működésfolytonosságra koncentrálna, nem létezik, azonban vannak közöttük olyanok, amelyek legalábbis részben tartalmaznak olyan normatívákat, amelyek működésfolytonossági kérdésekben relevánsnak tekinthetők.

Megállapítottam, hogy az ajánlások egyaránt alkalmazhatók a védelmi és polgári szférában, illetve a kritikus infrastruktúrák területén, alkalmazhatóságukra vonatkozóan gyakorlatilag nem állapíthatók meg különbségek. Megállapítottam továbbá, hogy az ajánlások szerinti működés a védelmi szférában, illetve a kritikus infrastruktúrák területén teljes körűen jelenleg nem valósul meg, ugyanakkor az ajánlások vizsgált területeken egyre inkább relevánsnak számítanak.

Rögzítettem, hogy a működésfolytonosság biztosításának fő összetevői a következők: az adott szervezetnél elvégzett helyzetfeltárás, a releváns veszélyforrások azonosítása és értékelése, az ezek alapján végrehajtott kockázatelemzés, illetve az ennek eredményeire támaszkodó, konkrét védelmi intézkedések megtétele, beleértve a katasztrófa helyzetekre való felkészülést is. Mindezeken túlmenően a működésfolytonosság biztosításának fontos további összetevői a folyamatos aktualizálás, a tesztelés valamint a hozzá tartozó megfelelő felkészítésre is.

Ezekhez kapcsolódóan megállapítottam, hogy - kisebb különbségektől eltekintve – a működésfolytonosság biztosítása hasonló problémákat okoz a védelmi és a polgári szférában, így a kritikus infrastruktúrák területén, a normál mindennapi, illetve művelet-orientált működés esetén is.

Meghatároztam, hogy a működésfolytonosság aktuális állapotára vonatkozó mutatószám rendszernek milyen követelményeket kell kielégítenie. Megállapítottam, hogy azon túlmenően, hogy alkalmasnak kell lennie a működésfolytonosság aktuálisan megvalósított szintjének jellemzésére, követelményként jelentkezik még az is, hogy alkalmas legyen a különböző szervezetek működésfolytonossági szintjeinek összevetésére, továbbá, hogy segítségével a működésfolytonosság időbeli változásait követhessük, illetve, hogy alkalmazásával objektív célkitűzéseket fogalmazzunk meg.

Javaslatot tettem a működésfolytonosság fő jellemzőit összefoglaló rendszerre épülő, szemléletesen ábrázolható mutatószám rendszer kialakítására, amely egy-egy szervezeten belül alkalmas a működésfolytonosság aktuális szintjének jellemzésére. Megállapítottam, hogy a mutatószámok meghatározása a mindennapi folyamatos működés, illetve művelet-orientált tevékenység egymástól eltérő kritérium rendszert igényel, ugyanakkor az, hogy a tevékenység a védelmi, a polgári, illetve a kritikus infrastruktúrák területén folyik, gyakorlatilag nem befolyásolja az alkalmazható kritériumokat.

## Az elért tudományos eredmények

1. A működésfolytonosság alapkoncepciójának kialakítása, szemléletének megfogalmazása, fő jellemzőinek rendszerezése.

   A rendszer a működésfolytonosság viszonylag egyszerű tárgyalását és szemléltetését teszi lehetővé, tartalmazva a működésfolytonosság alappilléreit (informatikai erőforrások kezelése, szervezeti és irányítási kérdések, illetve a katasztrófa helyzetek kezelése) és megfelelő csoportosítással a kihívást jelentő veszélyforrásokat. A rendszer fontos tulajdonsága, hogy egyaránt használható a védelmi és a polgári szférában, így a kritikus infrastruktúravédelem területén is, mind a mindennapi folyamatos, mind pedig a művelet-orientált tevékenységek esetén.

2. Az informatikai biztonságra valamint az informatikai rendszerek üzemeltetésére vonatkozó ajánlások védelmi szférában történő alkalmazhatóságának bizonyítása.

   A működésfolytonosság problémájához leginkább kapcsolódó ajánlások rendszerezésén és elemzésén keresztül rögzítésre került, hogy olyan ajánlás, amely kifejezetten a működésfolytonosságra koncentrálna, nem létezik, azonban vannak közöttük olyanok, amelyek legalábbis részben tartalmaznak olyan normatívákat, amelyek működésfolytonossági kérdésekben relevánsnak tekinthetők. Az értekezésben bizonyítást nyert, hogy a releváns ajánlások egyaránt alkalmazhatók a védelmi és polgári szférában, illetve a kritikus infrastruktúrák területén, továbbá, hogy alkalmazhatóságukra vonatkozóan gyakorlatilag nem állapíthatók meg különbségek.

3. A működésfolytonosság biztosítását lehetővé tevő fő összetevők meghatározása.

   A működésfolytonosság biztosítását lehetővé tevő fő összetevők kijelölik a működésfolytonosság biztosítására vonatkozó terv gyakorlati lépéseit. Az értekezésben bizonyítást nyert hogy - kisebb különbségektől eltekintve – a működésfolytonosság biztosítása hasonló problémákat okoz a védelmi és a polgári szférában, így a kritikus infrastruktúra védelem területén is.

4. A működésfolytonosság szintjét jellemző mutatószám rendszer koncepciójának kialakítása.

   A működésfolytonosság szintjét jellemző mutatószám rendszer szemléletesen ábrázolható és alkalmas arra, hogy segítségével egy-egy szervezeten belül a

működésfolytonosság aktuális szintje jellemzésére függetlenül attól, hogy a tevékenység a védelmi, a polgári, illetve a kritikus infrastruktúrák területén folyik. A mutatószám rendszer tartalmazza az egyes szintek kritériumait, kidolgozása megtörtént a mindennapi folyamatos működésre, illetve művelet-orientált tevékenységre vonatkozóan is.

## Ajánlások, gyakorlati felhasználhatóság

1. Az értekezés tartalmazza a működésfolytonosság fő jellemzőinek rendszerezését és alapkoncepcióját, rendszerezi és egységesíti a releváns irodalomban fellelhető, a működésfolytonossághoz kapcsolódó kiinduló gondolatokat, alapelveket, így a működésfolytonosságra vonatkozó felkészítési, oktatási anyagok készítéséhez kiinduló anyagként felhasználható.
2. Az értekezés áttekinti és értékeli az informatikai biztonságra és az informatikai rendszerek üzemeltetésére vonatkozó ajánlásokat, ezzel támogatja, hogy az egyes szervezetek működését meghatározó különböző szabályzatok a releváns ajánlásoknak megfelelőek legyenek, így közvetve elősegítheti az egyes szervezetek hatékonyabb működését.
3. Az értekezés rögzíti azokat a lépéseket, amelyeket különböző szervezeteknek a működésfolytonosság megvalósítása érdekében meg kell tenniük, így alapul szolgálhat az egyes szervezetek számára konkrét működésfolytonossági terveik kidolgozásához.
4. Az értekezés tartalmaz egy mutatószám rendszert, amely alkalmas működésfolytonosság aktuálisan megvalósított szintjének jellemzésére. Ezzel támogatja, a különböző szervezetek működésfolytonossági szintjeinek összevetését, továbbá a működésfolytonosság időbeli változásainak követését, illetve a működésfolytonosságra vonatkozó objektív célkitűzések rögzítését.

# Ábrák és táblázatok jegyzéke[65]

## Ábrák jegyzéke



## Táblázatok jegyzéke



[65] A forrásmegjelölés nélküli ábrák és táblázatok valamennyien a jelölt saját eredményei.

## Felhasznált irodalom


1. Eric V. Larson, John E. Peters: Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options (Chapter Six: Ensuring Military Capability: Continuity of Operations), RAND, Santa Monica, 2001. http://www.rand.org/pubs/monograph_reports/MR1251/MR1251.Chap6.pdf
2. Szeles Péter: Kommunikációs paradigmaváltás szükségessége a Magyar Honvédségben, Hadtudomány, XV. Évfolyam, 4. szám
3. Szárazföldi Haderő Doktrína (Army Doctrine Publication - Volume 2 – Command)
4. A Magyar Honvédség Összhaderőnemi Vezetési Doktrínája (tervezet), HM HVK Vezérkari Csoportfőnökség, 2003. április.
5. Várhegyi – Haig – Kovács: Információs műveletek, Multimédia oktatási anyag, ZMNE
6. Várhegyi-Makkai: Információs korszak, információs háború, biztonságkultúra, OMIKKK, Budapest, 2000.
7. Eric V. Larson, John E. Peters: Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options (Chapter Five:Ensuring Constitutional Authority: Continuity of Government), RAND, Santa Monica, 2001., http://www.rand.org/pubs/monograph_reports/MR1251/MR1251.Chap5.pdf
8. Continuity of Operation (COOP) in the Executive Branch: Background and Issues for Congress, CRS Report for Congress, 2004.
9. A Magyar Köztársaság Nemzeti biztonsági Stratégiája, (2073/2004 Kormány határozat), 2004. április 27.
10. Az informatikai biztonság kézikönyve, szerkesztő: Muha Lajos, Verlag Dashöfer Szakkiadó, 2000. (folyamatosan aktualizált kiadvány)
11. Az informatikai biztonság menedzselésének eljárásrendje, MSZ ISO/IEC 17799:2006.
12. Az informatikai biztonság menedzselésének eljárásrendje, MSZ ISO/IEC 17799:2002.
13. Országh László: Angol-magyar kéziszótár, Akadémiai kiadó, 1983.
14. Oxford Advanced Learners Dictionary, fourth Edition, Oxford University Press, 1989.
15. U.S. Army Continuity of Operations (COOP) Program Policy and Planning, Army Regulaion 500-3, 2006.
16. Department of Defense Defense Continuity Program (DCP), DIRECTIVE NUMBER 3020.26, 2004., www.dtic.mil/whs/directives/corres/pdf/d302026_090804/d302026p.pdf.
17. Módszertan az információs rendszerek kontrolljainak ellenőrzéséhez, 2004. www.asz.hu/ASZ/www.nsf
18. Pályázati felhívások a Tanács által szervezett általános versenyvizsgákra biztonsági, információtechnológiai és információbiztonsági területen, Az Európai Unió Hivatalos lapja, 2005. 12. 13., www.epa.hu/00800/00877/00613/pdf/hu0001s010.pdf
19. Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai, MTA SZTAKI, 2006. 05.14., www.cert.hu/dmdocuments/MTA3_online.pdf
20. Bencze – Hegedüs – Kolossa – Padányi – Praveczki – Szternák: Válságreagáló műveletek elmélete és gyakorlata a XXI. században, Egyetemi jegyzet, ZMNE, 2004.
21. Héjja – Kónya – Laczkó: Hadtudományi ismeretek, Egyetemi jegyzet, ZMNE, 2003.
22. EPCIP European Programme for Critical Infrastructure Protection

http://ec.europa.eu/justice_home/funding/epcip/funding_epcip_en.htm
23. www.isaca.hu/addons/news_1626_CIIP_GerencserAndras.pdf
24. Kassai Károly: A vezetés korszerűsítésének technikai feladatai, Hadtudomány, X. évfolyam, 1. szám
25. Munk Sándor – Beinschróth József: Informatikai rendszerek működésfolytonossági kérdéseinek sajátosságai művelet-orientált környezetben, Bolyai Szemle, 2006. IV. sz.
26. A magyar nyelv értelmező szótára, Akadémiai Kiadó, Budapest, 1996.
27. A Magyar Honvédség összhaderőnemi doktrínája, HM HVK Hadműveleti Csoportfőnökség, 2002.
28. AAP-6(2005) NATO Glossary of terms and definitions. [2-O-2.o.], JP 1-02 DoD Dictionary of Military and Associated Terms, 2005.
29. NATO Strategic Commanders: Strategic Vision: The Military Challenge, Allied Command Transformation – Allied Command Operations, NATO, 2004.
30. Controlling értelmező szótár, IFUA Horváth & Partners, Budapest, 2004.
31. Görög Mihály: Általános projektmenedzsment, Aula, 2001.
32. CIO – A Chief Information Officer Kézikönyve, Management Kiadó, 2003.
33. 2004. évi CV. törvény a honvédelemről és a Magyar Honvédségről
34. 1999. évi LXXIV. törvény a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről
35. 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról
36. Munk Sándor: Katonai informatika, egyetemi jegyzet, Zrínyi Miklós Nemzetvédelmi Egyetem, 2003.
37. Beinschróth József: A működésfolytonosság modelljei, kutatói szemináriumi tanulmány, ZMNE, 2005.
38. Beinschróth József: Informatikai rendszerekkel támogatott folyamatok működésfolytonosságának modellezése és mérése, Hadmérnök, 2006. IV. szám
39. Beinschróth József: A működésfolytonosság kérdése az informatikai biztonságra vonatkozó ajánlásokban, Kard és Toll, 2005/1.
40. C-M(2002)49 Security within the North Atlantic Treaty Organisation (NATO) 22. pont, www.nbf.hu/anyagok/anyagok/jogszabalyok/C-M(2002)49.pdf, (Magyar fordítása: Kerner Menyhért: Információvédelem a kormányzati és a védelmi szférában, az információbiztonság jogi háttere, http://old.honvedelem.hu/hirek/kiadvanyok/kutatas/doktorandusz/kerner_menyhert)
41. Informatikai rendszerek biztonsági követelményei, Miniszterelnöki Hivatal, Informatikai Koordinációs Iroda, 1996.
42. A kockázatmenedzsment gyakorlata, tanfolyami segédanyag, Kürt Kft., 2006.
43. A Pénzügyi Szervezetek Állami Felügyelete elnökének 10/2001. számú ajánlása a pénzügyi szervezetek működésének biztonsági feltételeiről
44. Beinschróth József: A működésfolytonosság kérdése az informatikai rendszerek üzemeltetésére vonatkozó ajánlásokban, Nemzetvédelmi Egyetemi Közlemények, 2005. IX évf. 2. sz.
45. IT Service Management v2.1.b ITSMF, Ltd., 2003
46. Szabó Zoltán: Infrastruktúra és IT szolgáltatás menedzsment, Szakszeminárium BKÁE, 2004.
47. COBIT – Az információtechnológia irányításához, kontrolljához és ellenőrzéséhez, A COBIT Irányító Bizottsága és az IT Governance Institute, 2000.

48. CISA Review Technical Information Manual, ISACA Inc., 2001.
49. COBIT Executive Summary, IT Governance Institute, 2000.
50. 12/2004. (BK 12.) BM utasítás a Belügyminisztérium Informatikai Biztonsági Politikája kiadásáról, www.bm.hu/proba/bmtvtev.nsf/datum/3B0A71A8B6E30855C1256EED004ABEE9
51. A Magyar Köztársaság Nemzeti Biztonsági Stratégiája, III.3.7. Információs rendszerek védelme, (2073/2004 Kormány határozat), 2004. április 27.
52. Az Informatikai Biztonság Irányításának Követelményrendszere (IBIK) http://www.halozatbiztonsag.hu/documents/MIBIK/IBIK_v095.pdf
53. www.hmei.hu
54. www.xisec.com
55. Ált/210. A Magyar Honvédség Informatikai Szabályzata, Magyar Honvédség 1993.
56. Szabó Zoltán: Az ITIL hazai alkalmazhatóságának kérdései, itSMF Magyarország elsõ szakmai szemináriuma, 2004. október 7.
57. Farkas Lajos: A népszavazás biztonsági kihívásai és tapasztalatai, LNX Security Szeminárium, 2005
58. Az IHM Informatikai Biztonság Albizottság 2003. 12.15-i ülésének jegyzőkönyve
59. 2/2004. (BK 12.) BM utasítás a Belügyminisztérium Informatikai Biztonsági Politikája kiadásáról
60. www.itsmf.hu
61. JSP 602, Hierarchy of Directions & Guidance, www.ams.mod.uk/ams/content/docs/jsp600/default.htm
62. Az IHM Informatikai Biztonság Albizottság 2003. 12.15-i ülésének jegyzőkönyve
63. www.kfki.com/hu/sajtoszoba/index_D3F09129B6934EECB51B0C09A030B129.php
64. NATO C3 Technical Architecture ADatP-34, Version 3.0, NATO OPEN Systems Working Group, 15. dec. 2001.
65. Beinschróth József: A működésfolytonosságot fenyegető veszélyforrások, Nemzetvédelmi Egyetemi Közlemények 2006. X évf. 1. sz.
66. Jozsef Beinschroth: Physical and Environmental Security, KANDO CONFERENCE 2006, XXIIIth SCIENTIFIC SESSION, 2006.
67. Horváth – Lukács- Tuzson – Vasvári: Informatikai biztonsági rendszerek, Ernst&Young, 2001.
68. Bodnár Csaba: Linux-alapú kiszolgálók alkalmazási lehetőségei az önkormányzatoknál, www.e-ware.hu/download/upload/124/html/mclx.ppt
69. Vasvári György: Háttértípusok és kiválasztásuk szempontjai a katasztrótervezéshez, A 2002. október 16-án megrendezett szakmai fórum követőkiadványa, Infoszféra Kft., 2002
70. Kassai Károly: A vezetés korszerűsítésének technikai feladatai, Hadtudomány, X. évfolyam, 1. szám
71. Halbritter Tamás: Katasztrófaterv készítés a gyakorlatban, A 2002. október 16-án megrendezett szakmai fórum követőkiadványa, Infoszféra Kft., 2002.
72. Beinschróth – Lukács: Informatikai biztonság menedzselése egy magyar középvállalatnál, Kandó Konferencia 2006.
73. Lukács Gellért: GPS háborúban és békében, http://www.navisys.hu/aeromap/articles/20010914_gps.html
74. www.bm.hu/proba/bmtvtev.nsf/datum/3B0A71A8B6E30855C1256EED004ABEE9.html
75. MSZ ISO/IEC 15408 Informatika. Biztonságtechnika. Az informatikai

biztonságértékelés közös szempontjai
76. Informatikai Tárcaközi Bizottság 8. sz. ajánlás: Informatikai biztonsági módszertani kézikönyv; Informatikai Tárcaközi Bizottság 12. sz. ajánlás: Informatikai rendszerek biztonsági követelményei
77. Az informatikai biztonság helyzete, biztonsági stratégia megvalósítása és kialakítása, tanulmány, 2002. http://www.informatika.gkm.gov.hu/data/39885/az_informatikai_biztonsag_helyzete.pdf
78. Kürt Computer Rendszerház Rt.: Informatikai rendszerek kialakítása Magyarországon, 2002., http://www.informatika.gkm.gov.hu/data/39892/informatikai_biztonsagi_rendszerek_kialakitasa.pdf
79. IT Foundation Certification – tanfolyami jegyzet, IQSOFT- John Bryce Oktatóközpont, 2005
80. Schutzbach Mártonné: Az informatikai biztonság általános koncepciója és gyakorlata a védelmi szférában, Nemzetvédelmi Egyetemi Közlemények, 2001. IV. sz.

## A kutatási területhez kapcsolódó publikációk

1. Beinschróth József: A működésfolytonosság modelljei, kutatói szemináriumi tanulmány, ZMNE, 2005.
2. Beinschróth József: A működésfolytonosság kérdése az informatikai biztonságra vonatkozó ajánlásokban, Kard és Toll, 2005/1.
3. Beinschróth József: A működésfolytonosság kérdése az informatikai rendszerek üzemeltetésére vonatkozó ajánlásokban, Nemzetvédelmi Egyetemi Közlemények, 2005. IX évf. 2. sz.
4. Munk Sándor – Beinschróth József: Informatikai rendszerek működésfolytonossági kérdéseinek sajátosságai művelet-orientált környezetben, Bolyai Szemle, 2006. IV. sz.
5. Beinschróth – Lukács: Informatikai biztonság menedzselése egy magyar középvállalatnál, Kandó Konferencia 2006.
6. Beinschróth József: A működésfolytonosságot fenyegető veszélyforrások, Nemzetvédelmi Egyetemi Közlemények 2006. X évf. 1. sz.
7. Jozsef Beinschroth: Physical and Environmental Security, KANDO CONFERENCE 2006, XXIIIth SCIENTIFIC SESSION, 2006. ISBN 963 7154 42 6
8. Beinschróth József: Informatikai rendszerekkel támogatott folyamatok működésfolytonosságának modellezése és mérése, Hadmérnök, 2006. IV. szám
9. Beinschróth József: Működésfolytonossági és katasztrófa tervek koncepcionális kérdései, Vészhelyzeti kommunikáció - tudományos konferencia, Budapesti Műszaki Főiskola, Kandó Kálmán Villamosmérnöki Kar, 2007. ISBN 978-963-7154-57-7