ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM

HADTUDOMÁNYI KAR

Hadtudományi Doktori Iskola

Dr. Beinschróth József

Informatikai rendszerekkel támogatott folyamatok működésfolytonossági kérdései a védelmi szférában

című doktori (PhD) értekezésének szerzői ismertetője

2007.

Bevezetés

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.

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 lesz 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.

Kutatási célkitűzéseim

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.

A téma feldolgozása során alkalmazott kutatási módszereim

Az értekezés több éves kutatómunka eredményeinek felhasználásával jött létre, a jelölt a témához kapcsolódóan számos publikációt készítettem, melyek különböző tudományos folyóiratokban kerültek publikálásra.

A kidolgozás kapcsán sort kerítettem 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 kutatómunkám egyaránt kiterjedt a nyomtatott és az interneten elérhető elektronikus irodalom feldolgozására.

A témához kapcsolódó szakirodalmakat részben az Internet segítségével, részben nyomtatott cikkek, konferencia anyagok felkutatásával állítottam össze.

A kutatási módszerek alkalmazása tekintetében törekedtem az értekezés tartalmi és formai egységének megteremtésére, az egyes fejezetek logikus egymásra építésére.

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 a különböző szervezeteknél lefolytatott számos informatikai, informatikai biztonsági, illetve informatikai működésfolytonossági jellegű projekt során mint nemzetközi minősítésekkel rendelkező informatikai szakember (CISA[1], illetve ITIL[2] minősítés) szereztem.

Az értekezés tartalmába ugyancsak beépültek azok a több éves oktatás során oktatóként szerzett tapasztalataim 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 című előadássorozataiban szereztem.

A kutatási téma interdiszciplináris jellegéből következően a kutatómunka során fontos szerepet kaptak a hasonló és kapcsolódó kutatási és tudományos területen

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

tevékenykedő szakemberekkel történő konzultációk, megbeszélések, tapasztalatok és eredmények megosztása.

Az értekezés felépítése

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.

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.

Új 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 szintjének 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.

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

Budapest, 2007. október 31.

Dr. Beinschróth József