

Muha Lajos

**A MAGYAR KÖZTÁRSASÁG**  
**KRITIKUS INFORMÁCIÓS INRASTRUKTÚRÁINAK**  
**VÉDELME**

című doktori (PhD) értekezés  
szerzői ismertetője és hivatalos bírálatai

**Tudományos vezető:**  
Dr. Kovács László mérnök őrnagy, PhD  
egyetemi docens

Budapest, 2007.

## A tudományos probléma

A modern gazdasági berendezkedés mellett a társadalom nincs felkészülve arra, hogy a kiesett infrastruktúrák, eszközök vagy szolgáltatások nélkül működjön, így ezeket – egyértelműen – védeni kell. A különböző infrastruktúrák, eszközök és szolgáltatások túlnyomó többségének működése az informatikai és kommunikációs rendszereken alapszik, ezeknek a rendszereknek a kiesése már önmagában is katasztrófahelyzetet idézhet elő.

Az infokommunikációs rendszerek nem csak a fizikai veszélyeknek vannak kitéve, hanem más, a kibertérből érkező támadásokkal szemben is nehezen védhetők, e rendszerek támadásával – azaz a kritikus információs infrastruktúrák működésének időleges vagy teljes működésképtelenségével – az infrastruktúráink nagy része megbénítható. Ezt a problémát felismerve a kritikus infrastruktúrák védelmén belül megjelent egy más megközelítést igénylő védelmi feladat, a kritikus információs infrastruktúrák védelme.

Hazánkban a kritikus információs infrastruktúrák védelme sajátos helyzetben van. Szövetségi rendszereink, az Európai Unió és a NATO ma már cselekvési egységben, a védelem összehangolásában gondolkodik, és ez kényszerítően visszahat a magyar biztonságpolitikára is, a szövetségi együttműködésből nem vonhatjuk ki magunkat.

**A kritikus információs infrastruktúráinkat fenyegető veszélyek feltárása, illetve az ellenük való védekezés módszereinek és eljárásainak kidolgozása** tudományos kutatást igényel, amelyet – az elmúlt években az információs rendszerek védelme területén szerzett gyakorlati tapasztalataimra is támaszkodva – jelen doktori értekezésemben bemutatok.

### **Kutatásom során az alábbi célokat tűztem ki:**

1. Nemzetközi tapasztalatok – különös tekintettel szövetségi rendszereinkre, a NATO-ra és az Európai Unióra – felhasználásával és azok hazai viszonyokra adaptálásával **meghatározni a kritikus infrastruktúra és kritikus információs infrastruktúra hazai fogalmát, tartalmát és elemeit.**
2. **Feltárni** a kritikus információs infrastruktúrákat fenyegető veszélyeket, **elemezni** a veszélyekre adható válaszokat – védelmi módszereket és eljárásokat –, valamint

a meglévő nemzetközi jogszabályok, szabványok, ajánlások alkalmazhatóságát és teljesülését.

3. **Feltárni** a hazai kritikus információs infrastruktúrák védelmi helyzetét, a meglévő jogszabályok, ajánlások teljesülését, és e vizsgálat eredménye alapján **meghatározni a Magyar Köztársaság kritikus információs infrastruktúrák védelmének elsődleges feladatait.**
4. A hazai kritikus információs infrastruktúrák védelmének egyik meghatározó területeként **javaslatot tenni a Magyar Köztársaság infokommunikációs biztonsági stratégiájára.**

### **Munkám során a következő kutatási módszereket alkalmaztam**

A széleskörű irodalomkutatásra épülő **információk és adatok összegyűjtése és rendszerezése** mellett felhasználtam a **megfigyelést** és a **kritikai adaptációt**, majd a **kutatások másodelemzésével**, az összefüggéseknek az **analízis** és **szintézis**, az **indukció** és **dedukció** módszereinek alkalmazásával törekedtem a kutatási céljaim elérésére és megvalósítására.

### **Az elvégzett vizsgálatok**

**A kitűzött célok elérése érdekében vizsgálataimat – fejezetek szerint – az alábbi felépítésű értekezésben foglaltam össze:**

#### **1. fejezet**

Megvizsgáltam az Európai Unió, a NATO és több ország, köztük a Magyar Köztársaság kritikus infrastruktúra, kritikus információs infrastruktúra fogalmát, illetve elemeinek meghatározását.

**Megállapítottam, hogy először a fogalomrendszert kell rögzíteni.** Az elemek meghatározása során nem alkalmazhatók szabadon más országok meghatározásai, az adott nemzet vonatkozásában **konkrétan kell meghatározni a kritikus infrastruktúra, kritikus információs infrastruktúra elemeit.**

**Megállapítottam, hogy valamennyi meghatározás kritikus infrastruktúraként tekint az infokommunikációs (informatikai és kommunikációs) rendszerekre.** Elgondolásom, hogy a kritikus információs infrastruktúrák védelmében az intradependencia miatt **a kritikus infrastruktúra infokommunikációs rendszerei**

**biztonságának megteremtése és fenntartása felértékelődik**, a védelem egyik alapvető elemévé válik.

**Kutatásom során megállapítottam, hogy a fegyveres erőket**, a fegyveres erők infrastruktúráit általában **nem sorolják be a kritikus infrastruktúrák közé**, mert békeidőszakban nem lehet katonai feladat – védelmi célokat közvetlenül nem ellátó – polgári létesítmények védelme, szolgáltatások felügyelete. Kutatásaim alátámasztják azt a véleményemet, hogy **a kritikus infrastruktúrák védelme nem katonai feladat**, de az ország védelmi tevékenységének tervezése, koordinációja elképzelhetetlen a fegyveres erők részvétele nélkül, és ezen túlmenően a védelmi felkészülés irányításában, a felkészülésben és felkészítésben, különösen a kérdéskör tudományos kutatásában számos feladatban szükséges a bevonásuk.

E fejezetben mindezek alapján **meghatároztam a Magyar Köztársaság kritikus infrastruktúra fogalmát, a kritikus infrastruktúrák alágazatait és felelőseit, valamint a Magyar Köztársaság kritikus információs infrastruktúra fogalmát és azok alágazatait.**

## 2. fejezet

Megvizsgáltam és elemeztem a kritikus információs infrastruktúrákat fenyegető veszélyeket. **Arra a megállapításra jutottam, hogy a kritikus információs infrastruktúrákat az információs dimenzióból a nehezen védhető fenyegetések érik.** A legtöbb támadás megvalósítása is áttevődött az internetre, és ez lehetővé teszi a nagy távolságokról történő, gyakori támadásokat, ugyanakkor számos más lehetőséget is biztosít a kapcsolódott rendszerek támadására.

Bemutattam a 2007 tavaszán bekövetkezett észt-orosz konfliktust, amely alapján azt a következtetést vonom le, hogy egy az információs dimenzióból érkező támadás komoly károkat okozhat egy fejlett infrastruktúrával rendelkező országnak. A bemutatott példa jól rávilágít arra a tényre, hogy **a védelem terén elengedhetetlenül fontos a megelőzés, a jogszabályoknak, szabványoknak, ajánlásoknak megfelelően felépített, megfelelő tartalékolással rendelkező biztonságos rendszerek kialakítása.**

Az Európai Unió és az európai országok gyakorlatát, dokumentumai feldolgozva **arra a következtetésre jutottam, hogy a kritikus információs infrastruktúrák védelme tekintetében komoly előrelépések történtek**, megteremtették a szükséges jogszabályi háttérrel a védelem érdekében. E témában széles körű tudományos kutatások

folynak, és az érintett tulajdonosi kör, az állammal együttműködve részt vállal a kritikus információs infrastruktúrák védelmében. Az információs infrastruktúrák védelme tekintetében az infokommunikációs rendszerek biztonsági szabványainak bevezetésére nagy hangsúlyt fektetnek.

A nemzetközi tapasztalatok alapján **az önszerveződő, társadalmi alapokon (is) működő hálózatbiztonsági szervezetek egyre nagyobb szerepet kell, hogy kapjanak a kritikus információs infrastruktúrák védelmében**, különösen a monitorozás és az információ-megosztás területén.

### 3. fejezet

A harmadik fejezetben megvizsgáltam a kritikus információs infrastruktúrák védelmének hazai megvalósítását. A releváns nemzetközi és hazai előírások és ajánlások áttekintése során **jelentős lemaradásokat állapítottam meg, alapvető intézkedések is hiányoznak a kritikus információs infrastruktúrák védelméhez.**

Tekintettel arra, hogy a kritikus infrastruktúrák védelmének biztosítása egyaránt állami és üzemeltetői érdek, ezért arra a következtetésre jutottam, hogy hazánkban is **fel kell készülni az európai uniós források felhasználására, és meg kell teremteni a védelmi intézkedések finanszírozásában a magánszféra bevonását.**

A hiányos, ellentmondó szabályozás a terület elhanyagoltságát mutatja. Bár a kisszámú szakember-gárda a maga részéről mindent megtesz a feladatainak szakszerű és maradéktalan ellátása érdekében, ez a politikai vezetés támogatása nélkül kevés eredménnyel kecsegtet, **hiányzik az egyértelmű és következetes állami-politikai akarat és így a támogatás is.**

**Megállapítottam ,hogy a kritikus információs infrastruktúrák védelme érdekében egy nemzeti program keretében törvényben és alacsonyabb szintű jogszabályban rögzíteni kell a kritikus infrastruktúrák védelmével kapcsolatos feladatokat** (ideértve a titokvédelemi hiányosságok, vagy a nemzeti biztonsági stratégia részstratégiáinak pótlását is) **és felelőségeket, meg kell teremteni az érintett szereplők együttműködési lehetőségét és kényszerét. A kormányzati, védelmi, gazdasági és társadalmi szervezetek közötti megfelelő – gazdasági és jogszabályi alapon történő – együttműködést ki kell alakítani.**

**Az EU és a NATO ajánlásait és dokumentumait, az infokommunikációs rendszerek biztonságával kapcsolatos ajánlásokat alkalmazni kell. Meg kell teremteni a kritikus információs infrastruktúrák védelme négy pillérét: a**

**megelőzés és korai figyelmeztetés, az észlelés, a reagálás és a krízismenedzsment egységes, államilag támogatott és koordinált működtetését.**

Mindezek alapján, a feltárt hiányosságok egy részének a megszüntetése érdekében javaslatot tettem a legfontosabb állami szintű szabályozási feladatokra, és ezek egyikét, a Magyar Köztársaság infokommunikációs biztonsági stratégiáját kidolgoztam.

### **Összegzett következtetések**

1. Az Európai Unió, a NATO és több ország, köztük a Magyar Köztársaság kritikus infrastruktúra, kritikus információs infrastruktúra fogalma, illetve elemeinek meghatározása alapján megállapítottam, hogy a kritikus információs infrastruktúra elemeinek jó meghatározásához **először a fogalomrendszert kell rögzíteni.** A kritikus infrastruktúra elemeinek meghatározása során **az egyes országok fejlettségét, gazdasági és kulturális strukturáltságát, értékrendjét, gondolkodás módját is vizsgálni kell.**
2. Megvizsgáltam az Európai Unió, a NATO valamint néhány fejlett infrastruktúrával rendelkező ország kritikus infrastruktúrákra és kritikus információs infrastruktúrákra vonatkozó fogalmi meghatározásait. Ezek elemzése, illetve a hazai meghatározásokkal való összehasonlítása után **azt a következtetést vontam le, hogy a hazai kritikus infrastruktúra és kritikus információs infrastruktúra fogalmak nem megfelelőek. Ezért meghatároztam a Magyar Köztársaság kritikus infrastruktúra fogalmát, a kritikus infrastruktúrák alágazatait és felelőseit, valamint a Magyar Köztársaság kritikus információs infrastruktúra fogalmát és azok alágazatait.**
3. Megvizsgáltam és elemeztem a kritikus információs infrastruktúrákat fenyegető veszélyeket. Külön vizsgáltam a fizikai dimenzióból, és külön az információs dimenzióból érkező lehetséges fenyegetéseket. **Ezek alapján megállapítottam a kritikus információs infrastruktúrákat az információs dimenzióból fenyegető veszélyeket.**
4. Megvizsgáltam az Európai Unió, a NATO és néhány fejlett ország e téren megvalósított védelmi gyakorlatát. Az EU határozatait, irányelveit és javaslatait feldolgozva arra a **következtetésre jutottam, hogy a kritikus információs infrastruktúrák védelme tekintetében komoly előrelépések történtek.** A nemzetközi

helyzet elemzése után azt a következtetést vontam le, hogy az egyes országok politikai vezetése megértette a problémát és **megteremtette a szükséges jogszabályi háttér**et a védelem érdekében.

5. A bemutatott észt-orosz konfliktust elemezve, azt a következtetést vontam le, hogy egy az információs dimenzióból érkező támadás komoly károkat okozhat egy fejlett infrastruktúrával rendelkező országnak. A bemutatott példa jól rávilágít arra a tényre, hogy a **védelem terén elengedhetetlenül fontos a megelőzés, a jogszabályoknak, szabványoknak, ajánlásoknak megfelelően felépített, megfelelő tartalékolással rendelkező biztonságos rendszerek kialakítása.**
6. A nemzetközi tapasztalatok elemzése alapján **megállapítottam**, hogy **az önszerveződő, társadalmi alapokon (is) működő hálózatbiztonsági szervezetek egyre nagyobb szerepet kell, hogy kapjanak a kritikus információs infrastruktúrák védelmében**, különösen a monitorozás és az információ-megosztás (biztonságkultúra fejlesztése) területén.
7. A Magyar Köztársaság kritikus információs infrastruktúráinak védelmét elemezve **megállapítottam**, hogy hazánkban **alapvető intézkedések is hiányoznak a kritikus információs infrastruktúrák védelméhez**. Az utóbbi években jelentősen megváltoztak a biztonsági fenyegetések, kockázatok, amelyekre nem vagyunk felkészülve, ugyanakkor megszűnt az állami irányítás és támogatás, beavatkozás a biztonság területén. Mindezeket figyelembe véve **jelentős lemaradásokat állapítottam meg** a területen.
8. Megállapítottam, hogy a hiányosságok megszüntetése, valamint a minél hatékonyabb védelem megteremtése érdekében egy **nemzeti program keretében** törvényben és alacsonyabb szintű jogszabályban **rögzíteni kell a kritikus infrastruktúrák védelmével kapcsolatos feladatokat** (ideértve a titokvédelemi hiányosságok, vagy a nemzeti biztonsági stratégia részstratégiáinak pótlását is) és **felelőségeket**, meg kell teremteni az érintett szereplők együttműködési lehetőségét (és kényszerét). A kormányzati, védelmi, gazdasági és társadalmi szervezetek közötti megfelelő – gazdasági és jogszabályi alapon történő – együttműködést ki kell alakítani.

9. Mindezek alapján, a feltárt hiányosságok megszüntetése érdekében **javaslatot tettem a legfontosabb állami szintű szabályozási feladatokra**, és ezek egyikét, a **Magyar Köztársaság infokommunikációs biztonsági stratégiáját kidolgoztam**.

### **Új tudományos eredmények**

1. Megvizsgáltam a hazai kritikus infrastruktúra és kritikus információs infrastruktúra meghatározásokat. Megállapítottam, hogy azok nem megfelelőek, ezért elemezve a különböző nemzetközi szervezetekben és országokban meglévő kritikus infrastruktúra és kritikus információs infrastruktúra fogalmakat, azokból következtetések levonva **meghatároztam a hazai kritikus infrastruktúrák és kritikus információs infrastruktúrák fogalmát, valamint mindkét esetben azok alágazatait**.
2. Megvizsgáltam, hogy milyen veszélyek fenyegetik a kritikus infrastruktúrákat és a kritikus információs infrastruktúrákat. Ezek alapján elemeztem a különböző nemzetközi szervezetek és országok e veszélyek ellen tett lépéseit, majd **mindezek alapján feltártam a nemzetközi védelmi megoldásokat**.
3. Elemeztem a hazai kritikus infrastruktúrák és kritikus információs infrastruktúrák védelmének helyzetét, amely alapján mind a fenyegető veszélyek terén, mind a nemzetközi téren tapasztalt eddigi védelmi lépésekhez képest komoly hiányosságokat és lemaradásokat állapítottam meg. Ezért **kidolgoztam a minimálisan szükséges parlamenti és kormányzati feladatokat**, amely elengedhetetlenül szükségesek a **Magyar Köztársaság kritikus információs infrastruktúrái védelmének euró-atlanti kompatibilitásához**.
4. A kritikus infrastruktúrák és kritikus információs infrastruktúrák védelme terén megállapított hazai hiányosságok megszüntetése érdekében **kidolgoztam a védelem egyik részterületére a Magyar Köztársaság infokommunikációs biztonsági stratégiáját**.



## **Az értekezés ajánlásai**

1. A doktori (PhD) értekezésemben megfogalmazottakat javaslom felhasználni a területre vonatkozó stratégiák, programok, jogszabályok és ajánlások megalkotásában, aktualizálásában, különös tekintettel az alábbiakra:
  - a nemzeti kritikus infrastruktúrák védelmi program megalkotása;
  - a kritikus infrastruktúrák védelmi követelményeiről szóló törvény megalkotása;
  - a honvédelmi törvényt aktualizálása;
  - a titokvédelmi törvényt aktualizálása;
  - az infokommunikációs biztonsági stratégia kiadása;
  - az infokommunikációs rendszerek biztonságával kapcsolatos ajánlások, módszertani segédanyagok aktualizálása (elkészítése).
  
2. Javaslom értekezésemet felhasználni a kritikus információs infrastruktúrák, illetve a kapcsolódó szakterületeken folyó egyetemi (főiskolai) alap, mester és doktori képzésben tananyagként.
  
3. Javaslom értekezésem – információs infrastruktúrák védelmével kapcsolatos – jogszabályokat, ajánlásokat áttekintő és összefoglaló részeit, az általam javasolt stratégiával együtt felhasználni az információbiztonsági szakemberek különböző tanfolyami képzéseiben, illetve továbbképzéseiben.

## Publikációs jegyzék

1. MUHA Lajos: *Magyar Informatikai Biztonság Irányítási Keretrendszer* – Információs Társadalom Koordinációs Tárcaközi Bizottság ajánlástervezet (<http://www.itktb.hu/Resource.aspx?ResourceID=docstorefile&f=871&t=stored>), Budapest, 2005. – 16p.
2. DÉRI Zoltán, LOBOGÓS Katalin, MUHA Lajos, NYÍRY Géza, SNEÉ Péter, VÁNCSA Julianna: *Az Informatikai Biztonság Irányításának Vizsgálata* (szerkesztő: Muha Lajos) – Információs Társadalom Koordinációs Tárcaközi Bizottság ajánlástervezet (<http://www.itktb.hu/Resource.aspx?ResourceID=docstorefile&f=834&t=stored>), Budapest, 2005. – 313p.
3. DÉRI Zoltán, LOBOGÓS Katalin, MUHA Lajos, SNEÉ Péter, VÁNCSA Julianna: *Az informatikai biztonság irányításának követelményrendszere* (szerkesztő: Muha Lajos) – Információs Társadalom Koordinációs Tárcaközi Bizottság ajánlástervezet (<http://www.itktb.hu/Resource.aspx?ResourceID=docstorefile&f=833&t=stored>), Budapest, 2004. – 207p.
4. MUHA Lajos - BODLAKI Ákos: *Az informatikai biztonság (egyetemi, főiskolai jegyzet)* – Budapest: PRO-SEC Kft. 2001. – 176p. – ISBN 963 86022 6 0
5. BODLAKI Ákos, MUHA Lajos: *Az informatikai biztonság tanúsítási és minősítési eljárásrendjének terve* – tanulmány a Miniszterelnöki Hivatal Informatikai Koordinációs Iroda részére, Budapest, 1997. – 112p.
6. BODLAKI Ákos, CSERNAY Andor, MÁTYÁS Péter, MUHA Lajos, PAPP György, VADÁSZ Dezső: *Informatikai Rendszerek Biztonsági Követelményei (Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság 12. számú ajánlás)*, Budapest: Miniszterelnöki Hivatal 1996. – 217p.
7. MUHA Lajos: *Adatvédelmi Jogszabálygyűjtemény* – FIXX Kft., Budapest: 1993 / Miniszterelnöki Hivatal (*a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság 8. számú ajánlás 5. számú mellékleteként*) 1995. – 213p.
8. MUHA Lajos: *A szabályozási környezet által támasztott igények*, 6. fejezet In. SZIGETI Szabolcs, KRASZNAY Csaba, KREMSER Csaba, MUHA Lajos, RIGÓ Ernő: *Útmutató az informatikai biztonság megvalósítására önkormányzatok számára* (szerk. Szigeti Szabolcs) – Informatikai és Hírközlési Minisztérium ajánlása, Budapest, 2006. ([http://www.itktb.hu/resource.aspx?ResourceID=it\\_bizt\\_onkormanyzatoknak\\_v1\\_0\\_rev\\_d\\_e\\_V1.doc](http://www.itktb.hu/resource.aspx?ResourceID=it_bizt_onkormanyzatoknak_v1_0_rev_d_e_V1.doc)) – p.104-109.
9. MUHA Lajos: *Az önkormányzati környezet specialitásai*, 7. fejezet In. SZIGETI Sz. et al.: *Útmutató az informatikai biztonság megvalósítására önkormányzatok számára* – Budapest, 2006. – p.110-112.
10. MUHA Lajos: *Jogszabályok*, 11. fejezet In. SZIGETI Sz. et al.: *Útmutató az informatikai biztonság megvalósítására önkormányzatok számára* – Budapest, 2006. – p.132-134.
11. MUHA Lajos: *Jogszabályok* – 1. kötet 2.2. pont In. *Az informatikai biztonság kézikönyve* (szerk. Muha Lajos) – Budapest: Verlag Dashöfer, 2000-2005 – ISBN 963 9313 12 2, 2000. november - 2005. március (többször frissítve)

12. MUHA Lajos: *Szabványok és ajánlások* – 1. kötet 2.3. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november - 2005. március (többször frissítve)
13. MUHA Lajos: *Fogalmak és definíciók* – 1. kötet 2.4. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2003. március, 2004. szeptember (frissítve)
14. MUHA Lajos: *Az informatikai biztonság kialakulása* – 1. kötet 3.2. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november, 2004. szeptember (frissítve)
15. MUHA Lajos: *Az informatikai biztonság meghatározása* – 1. kötet 3.3. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november, 2001. december, 2004. november (frissítve)
16. MUHA Lajos: *Az informatikai biztonság jogi szabályozása* – 1. kötet 3.4.1-3.4.6. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november, 2002. március (frissítve)
17. MUHA Lajos: *A számítógépes bűnözés* – 1. kötet 3.4.7. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november - 2005. március (többször frissítve)
18. MUHA Lajos: *ISO/IEC 17799:2000* – 1. kötet 3.5.1.6.1. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2001. szeptember
19. MUHA Lajos: *Az Informatikai Biztonság Irányításának Követelményrendszere* – 1. kötet 3.5.1.8. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2004. szeptember
20. MUHA Lajos: *Az informatikai biztonság irányításának vizsgálata és a tanúsítás eljárásrendje* – 1. kötet 3.5.1.9. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2004. szeptember
21. MUHA Lajos: *A Common Criteria* – 1. kötet 3.5.3.4. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2003. június
22. MUHA Lajos: *A titokvédelem és az Uniós csatlakozás* – 1. kötet 3.5.3.5. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2003. június
23. MUHA Lajos: *Az informatikai biztonsági hatóság* – 1. kötet 3.5.3.6. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2003. június
24. MUHA Lajos: *A titokvédelmi és az ügyviteli szabályzat* – 2. kötet 5.4.4. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november
25. MUHA Lajos: *Dokumentumkezelés, ügyvitel* – 2. kötet 5.7. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november, 2004. szeptember (frissítve)
26. MUHA Lajos: *Informatikai rendszerek biztonsági ellenőrzése* – 2. kötet 5.9.1. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november, 2001. szeptember (frissítve)
27. MUHA Lajos: *Az informatikai biztonsági vizsgálatot végző szervezetekkel és személyekkel szembeni követelmények* – 2. kötet 5.9.3. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2005. március

28. BODLAKI Ákos, ENDRÉDI Gábor, MUHA Lajos: *Tanúsított termékek* – 2. kötet 5.10. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november-2005. március (többször frissítve)
29. MUHA Lajos: *Az Informatikai Biztonság Irányítási Rendszer* – 2. kötet 5.12. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2005. június
30. HAJNAL János, MUHA Lajos: *Az informatikai rendszerek vállalkozásba adása* – 2. kötet 6.8. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2000. november, 2005. június (frissítve)
31. MUHA Lajos: *Informatikai Biztonsági Szabályzat (ajánlás)* – 3. kötet 8.5. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2002. szeptember
32. MUHA Lajos: *A BS7799-2 szerinti audit* – 3. kötet 8.8. pont In. Az informatikai biztonság kézikönyve (szerk. Muha L.), 2005. június
33. MUHA Lajos: *Security Risk Analysis in ICT systems* In. Hadmérnök, ZMNE, Budapest, 2007. december
34. MUHA Lajos: *Az informatikai biztonság kérdései a felsőoktatásban* In. Informatika, Gábor Dénes Főiskola, Budapest, 2005. december, 8. évf. 4. sz. – p.96-99.
35. MUHA Lajos: *Az informatikai biztonság átértékelődött jelentősége napjainkban* In. Informatika, Gábor Dénes Főiskola, Budapest, Budapest, 2005. december, 8. évf. 4. sz. – p.135-137.
36. MUHA Lajos: *Az informatikai biztonság oktatása*, Felsőoktatási Matematika-, Fizika- és Számítástechnika Oktatók XXXI. Konferenciája, Dunaújváros, 2007.08.24. –p.202-205.
37. MUHA Lajos: *Informatikai biztonsági szabványok és irányelvek (a nemzetközi és a hazai szabályozás helyzete)*, IX. Országos Neumann Kongresszus, Győr, 2006.06.27. – CD mellékleten 10p.
38. MUHA Lajos: *A terrorizmus és az informatikai biztonság*, HiSec 2004 konferencia, Budapest, 2004.10.26.
39. Muha Lajos: *Szabványok és ajánlások az informatikai biztonság területén*, VIII. Országos Neumann Kongresszus, Budapest, 2003.10.17.
40. MUHA Lajos: *Az informatikai biztonság felügyeleti és tanúsító intézményrendszere*, HiSec 2003 konferencia, Budapest, 2003.10.29.
41. MUHA Lajos: *Az informatikai biztonság*, EDI '98 konferencia, Budapest, 1998.07.18.
42. MUHA Lajos: *Az elektronikus okirat bevezetésének kérdései ...*, HiSec '97 konferencia, Budapest, 1997.06.06.
43. MUHA Lajos: *Az informatikai biztonság auditálása*, HiSec '96 konferencia, Budapest, 1996.06.14.

## Szakmai-tudományos életrajz

### Személyes adatok:

Név: Muha Lajos  
Anyja neve: Gábor Etel  
Szül. hely. idő: Budapest, 1956. 08. 28.  
Lakcím: 2112 Veresegyház, Pázmány Péter utca 43.  
Telefon: +36 - 30 - 940-7860  
E-mail: muha@gdf.hu

### Tanulmányok, képzettségek:

2004: Certified Information Security Manager (CISM), Information Systems Audit and Control Association  
2001-2004: Zrínyi Miklós Nemzetvédelmi Egyetem, levelező PhD hallgatója  
1996: Budapesti Műszaki Egyetem, Mérnöktovábbképző Intézet, UNIX rendszerek kezelése és hálózati szolgáltatásai tanfolyamok  
1993: Közigazgatási alapvizsga – BM  
1989-1990: Külkereskedelmi Oktatási és Továbbképző Kft., felsőfokú külkereskedelmi áruforgalmi szakképesítés  
1981-1986: Katonai Műszaki Akadémia, Kibernetika Kar, informatikai rendszerek szak, okleveles kibernetikus mérnök, Varsó  
1979: 2. Központi Tüzértiszti Tanfolyam, önjáró tüzérségi harcászati tanfolyam, Leningrád  
1974-1978: Kossuth Lajos Katonai Főiskola, tábori tüzér tiszt  
1970-1974: Árpád Gimnázium, Budapest, érettségi

### Munkahelyek, beosztások:

2006-: Gábor Dénes Főiskola, főiskolai docens;  
2004-2005: AerusDPG Bt. projektigazgató;  
2003-2004: Persecutor Vagyonvédelmi Kft., információbiztonsági igazgató;  
2002-2003: Magyar Posta Rt. Vezérigazgatósága, Adat- és Információvédelmi osztályvezető;  
2001-2005: Gábor Dénes Főiskola, óraadó oktató, az informatikai biztonság tantárgy vezető tanára;

- 1995-2001: FIXX Rt. (FIXX Kft.) elnök-igazgató;
- 1993-1995: Jász-Nagykun-Szolnok, Pest és Nógrád Megyei Köztársasági Megbízott Hivatala, a régió adatvédelmi felelőse, címzetes főtanácsos;
- 1991-1992: Cédrus Informatikai Rt, kereskedelmi igazgató-helyettes;
- 1991-: Bolyai János Katonai Műszaki Főiskola, Számítástechnika és Matematika Szaktanszék, főiskolai oktató;
- 1989-1991: Mikroelektronikai Vállalat, Varsói Kereskedelmi-műszaki Iroda, irodavezető;
- 1988-: Zalka Máté Katonai Műszaki Főiskola, Számítástechnika és Matematika Szaktanszék, vezényelt főiskolai oktató;
- 1987-1988: 1. gépesített hadtest, parancsnokság, Rendszerszervezési, Vezetésgépesítési és Automatizálási alosztály, alosztályvezető;
- 1986-1987: MN Rendszerszervezési, Vezetésgépesítési és Automatizálási Intézet, rendszerszervező főtitkár;
- 1978-1980: 33.g.l.e., tüzér szakaszparancsnok.

**Nyelvtudás:**

- 2005: Angol középfok "C"
- 1986: Lengyel felsőfok „C”

**Tudományos, társadalmi szervezeti tagság:**

- 1998-2004: Személy-, Vagyondvédelmi és Magánnyomozói Szakmai Kamara Tudományos Bizottságának tagja
- 1994-1999: Belügyminisztérium: az Országos Közigazgatási Vizsgabizottság tagja
- 1995-: Information Systems Audit and Control Association (ISACA) tagja
- 1995-: Igazságügyi adatvédelmi szakértő

Budapest, 2007. október 10.

Muha Lajos