DOKTORI (PhD) ÉRTEKEZÉS SZERZŐI ISMERTETŐJE

NEMZETI
KÖZSZOLGÁLATI EGYETEM
Doktori Tanács

JÉRI TAMÁS

A Kritikus Internetes Szolgáltatások biztonsági kérdései a védelmi szférában

című doktori (PhD) értekezésének szerzői ismertetése és
hivatalos bírálatai

Budapest
2020.

NEMZETI KÖZSZOLGÁLATI EGYETEM

KATONAI MŰSZAKI DOKTORI ISKOLA

JÉRI TAMÁS

A Kritikus Internetes Szolgáltatások biztonsági kérdései a védelmi szférában

című doktori (PhD) értekezésének szerzői ismertetése és hivatalos bírálatai

Témavezető:

Prof. Dr. Kovács László dandártábornok (DSc)
egyetemi tanár

Budapest
2020.

A TARTALMI RÉSZ PONTJAI

1. A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

2. KUTATÁSI CÉLOK

3. KUTATÁSI MÓDSZEREK

4. AZ ELVÉGZETT VIZSGÁLAT TÖMÖR LEÍRÁSA FEJEZETENKÉNT

5. ÖSSZEGZETT KÖVETKEZTETÉSEK

6. ÚJ TUDOMÁNYOS EREDMÉNYEK

7. A KUTATÁSI EREDMÉNYEK GYAKORLATI FELHASZNÁLHATÓSÁGA

8. AJÁNLÁSOK

9. A DOKTORJELÖLT TÉMÁVAL KAPCSOLATOS PUBLIKÁCIÓS JEGYZÉKE

10. A DOKTORJELÖLT SZAKMAI-TUDOMÁNYOS ÉLETRAJZA

Budapest, 2020. év december hó 08. nap

aláírás

A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

Az információtechnológia fejlődése a védelmi szférában is kikényszeríttette a gyors és hatékony eszközök és alkalmazások használatát, amelyek a napi munkavégzés részévé és létfontosságú adathordozóvá váltak. A megjelent internetes szolgáltatások hasonlóan a társadalomban alkalmazott internetes szolgáltatásokhoz, beivódtak a szervezetek, szervek életébe, nélkülük az alaptevékenységek ellátása is veszélybe kerülne, így joggal nevezhetjük azokat is létfontosságú szolgáltatásoknak. Problémaként jelentkezik ugyanakkor, hogy ezeknek a rendszereknek és szolgáltatásoknak sem a feltérképezése, sem a védelme nem megoldott teljes körűen.

1. Jogszabályi kötelezettségek

Az elektronikus információbiztonságról-, valamint az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló törvények előírják, a társadalom pedig elvárást támaszt a közigazgatási szervek, így a védelmi szféra számára is, hogy

- az elektronikus információbiztonsággal kapcsolatos szabályok kerüljenek minden körülmény között betartásra;
- az ügyek lehetőleg papírmentesen, elektronikusan intéződjenek;
- az információk legyenek naprakészek, felhasználóbarát formában gyorsan-, könnyedén-, és állandóan elérhetők.

Ezeknek az elvárásoknak a teljesítése egészen mást jelent egy épület falai között, vagy a kibertérben. Az utóbbi nyilvánvalóan másfajta kihívást és nyomást jelent az érintett szervezetekre nézve, ugyanakkor egyben jelenthet késztetést is a kor vívmányainak kihasználására vonatkozóan. A megvalósítás jár néhány további megoldandó problémával is, hisz úgy kell szavatolni az információbiztonságot az interneten, hogy

- a szervezet informatikai rendszerében tárolt adatok hitelesen, csak és kizárólag a szükséges mértékben-, és állandó rendelkezésre állás mellett legyenek elérhetők;
- az állampolgároktól bármely időpontban indított ügyintézési folyamat a szervezet informatikai rendszerében is tárolódjon és a befelé érkező információk elérjenek az érintettekhez.

A kapott, vagy vállalt kötelezettségből eredő internetes szolgáltatások fő problémája, hogy azoknak lehetőleg minden körülmény között, állandó rendelkezésre állással, biztonságosan működniük kell, amelyhez számos ajánlást be kell tartani.

2. Az internetben rejlő lehetőségek kihasználása

Az internet használatának kellemesebb oldala, hisz sokkal könnyebb mások által kifejlesztett alkalmazásokat igénybe venni, mint sajátot készíteni. Ma már szinte mindenki talál kedvére való – akár – ingyenes szolgáltatást az interneten, amibe örömét, vagy kedvét leli, amely érdeklődési körébe tartozik, vagy egyszerűen csak valamilyen okból hasznos rá nézve, amely körbe természetesen a védelmi szféra is beletartozik.

Az internetben rejlő lehetőségek kihasználásának egyik lehetséges problémája az ellenőrizetlen szolgáltatás felhasználás, amely kártékony programok rendszerbe jutását, vagy jogosulatlan rendszerbe lépést vonhat magával, másik lehetséges problémája a túlzott-, vagy megbízhatatlan szolgáltatás igénybevétel, amely annyira erős kötődést eredményezhet, hogy kimaradás, leállás esetén hátrányosan érinti az adott szervezetet.

Összegezve a következő tudományos problémák azonosíthatók:

- a létfontosságú internetes szolgáltatások témaköre – fontossága ellenére – eddig nem került tudományosan feldolgozásra, sem általánosságban sem a védelmi szférában;
- jelenleg nincs olyan iránymutatás, vagy ajánlás, amely rögzítené, hogy mit kell tenni együtt az internetes informatikai szolgáltatások biztonságáért és nagyfokú rendelkezésre állásáért;
    - a védelmi szféra internetes szolgáltatásainak bevezetése elsősorban a várható eredményekre koncentrál, ugyanakkor az esetleges leállás, vagy kimaradás esetére nem készül hatástanulmány, a megelőzés másodlagos szempont;
    - az alkalmazott internetes szolgáltatások egyenrangúak, nincsenek közülük kiemelve azok a kritikusnak tekinthető szolgáltatások, amelyek az átlagnál is nagyobb, folyamatos figyelmet érdemelnek;
    - a feltételezett Kritikus Internetes Szolgáltatásokra vonatkozó üzemeltetési hatáskörök nincsenek definiálva, a szolgáltatások súly-, és gócpontjai nem ismertek;
    - a futó internetes szolgáltatások működésképtelensége esetén az elhárítás öntevékeny, ad-hoc jellegű (mindenki a saját hatásköre szerint).
- az internetes informatikai szolgáltatások igénybevétele nem szabályozott, nincsen rá általános ajánlás, vagy iránymutatás annak ellenére, hogy folyamatos kockázatvállalást jelent.

KUTATÁSI CÉLOK

1. Rá kívánok mutatni a kritikus internetes szolgáltatás jelenségre, létezésre.
2. Célom definiálni a kritikus internetes szolgáltatás (a továbbiakban: KRISZ) fogalmát, bemutatni felépítését, továbbá megvizsgálni működésének aspektusait, áttekinteni az általános és a hazai rendvédelmi alkalmazását.
3. Bizonyítani kívánom, hogy az infrastruktúrák, vagy az információs infrastruktúrák mellett internetes szolgáltatások is lehetnek kritikusak, hiszen egy infrastruktúra működése önmagában még nem jelent garanciát a szolgáltatás működésére.
4. Szeretném megvizsgálni a kritikus infrastruktúrákkal és a kritikus információs infrastruktúrákkal kapcsolatos összefüggéseket, továbbá a kritikusnak vélt internetes szolgáltatások gyakorlati alkalmazásához kívánom bemutatni azokat a módszereket és ajánlásokat, amelyek az információbiztonság betartása mellett hozzásegítenek a folyamatos rendelkezésre állás megvalósításához.
5. Javaslatokat kívánok adni a kritikusnak vélt internetes szolgáltatások biztonságos igénybevételéhez, működtetéséhez.

A kutatási célkitűzéseket az alábbi részcélokra bontott kutatómunkával kívánom elérni:

- A Kritikus Internetes Szolgáltatások létezésének és érzékelhető jelenlétének feltárása, valamint az információs infrastruktúrákkal kapcsolatos összefüggések vizsgálata
  - KRISZ definiálása;
  - KRISZ feltárása általánosságban és a védelmi szférában.

- Kritikus Internetes Szolgáltatások összetétele, elemeinek vizsgálata, a szolgáltatás-nyújtás veszélyeinek-, és a helyes alkalmazásrendnek a bemutatása
  - KRISZ felépítése, alrendszerei;
  - KRISZ leggyakoribb előfordulásai, rendszerei, biztonságos üzemeltetése;
  - KRISZ védelmi ajánlásai.

KUTATÁSI MÓDSZEREK

Az értekezésem elkészítéséhez az alábbi kutatási módszereket alkalmaztam:

- irodalomkutatás: a vonatkozó releváns nemzetközi és hazai szakirodalom, jogszabályok és egyéb dokumentumok kutatása, tanulmányozása, feldolgozása;
- kérdőívből kinyert adatok összehasonlító elemzése;
- általánosítás, mint vizsgálati módszer;
- logikai elemzés: a feltárt adatok feldolgozása, elemzése, értékelése, ebből a következtetések levonása után, javaslatok megfogalmazása;
- empirikus kutatások: saját megszerzett szakmai tapasztalatok felhasználása, leírása;
- konferenciákon, konzultációkon, rendezvényeken való részvétel, javaslatok kidolgozása;
- eredmények publikálása: kutatási eredmények feldolgozása, cikkek, egyetemi jegyzet fejezetek formájában történő publikálása, valamint konferenciákon és oktatásban történő előadása.

AZ ELVÉGZETT VIZSGÁLAT TÖMÖR LEÍRÁSA FEJEZETENKÉNT

1. A Kritikus Internetes Szolgáltatások, a kritikus információs infrastruktúrák egyik – egyre bővülő – szegmensén megjelenő, létfontosságú kiszolgálások köre. A kritikus infrastruktúrák (KI), az információs infrastruktúrák (II), és a kritikus információs infrastruktúrák (KII) definícióiból vezethető le a KRISZ tudományos megközelítésben, alátámasztva, hogy egyes internetes szolgáltatások leállása esetén szinte „megáll az élet". Az elvégzett felmérés összességében igazolta azt a feltételezést, hogy a védelmi szférában is léteznek és működnek Kritikus Internetes Szolgáltatások, és levonható az a következtetés is, hogy egyetlen szervezet sem tudná maradéktalanul ellátni feladatait, vagy tudna megfelelni a rá vonatkozó kötelezettségeknek a létfontosságú internetes szolgáltatások rendelkezésre állása nélkül.
2. A KRISZ rendszerszintű vizsgálatával feltérképezésre kerültek az alrendszerek és rendszerelemek, amelyek a szolgáltatások támogatásában közvetlenül és közvetetten egyformán fontosak. Az adatbázis-kezelő rendszerek nélkülözhetetlen „kellékei" korunk információs társadalmának és vele együtt annak eredményeként, valamint következményeként, a Kritikus Internetes Szolgáltatásoknak is. A KRISZ-en keresztül, mind az operációs rendszerhez, a file-rendszerhez, az adatbázis-kezelőhöz és az adatbázishoz szerzett rosszindulatú hozzáférés a szolgáltatás leállásához vezethet.
3. Az elmúlt több mint két évtized dinamikus IT fejlődésének köszönhetően, a Web – amely egyben a leggyakrabban használt KRISZ, – az internet meghatározó információs platformjává vált. Az áldozatul esett, feltört, módosított weboldalak jól mutatják, hogy mit jelent a hibák, vagy figyelmetlenségek kihasználása. Az internetet használók folyamatos létszámemelkedése egyértelműen kihatással van az elektronikus levelezést igénybe vevők számára is, amely előtérben tartja az e-mail címeket, mint lehetséges támadási célpontokat. A kiberbűnözők az elektronikus levelezést, mint eszközt, folyamatosan igénybe veszik, amely még mindig az első számú, mindamellett „legális" támadási eszköz az interneten. A megkerülhetetlen üzemeltetési feladatokon keresztül bemutatásra került, hogy miként lehet a szükséges biztonságot fenntartani.
4. Az összeköttetés védelmére, a szolgáltatás nyújtásra és a szolgáltatás igénybevételének védelmére tett ajánlások, valamint az általános védelmi intézkedésekre vonatkozó javaslatok komplexen, rendszerezve, és nem csak informatikus szemmel segítik a Kritikus Internetes Szolgáltatásokat igénybe vevők, vagy nyújtók munkáját.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Dolgozatomban megfogalmaztam, hogy az internetes szolgáltatások működése infrastruktúra specifikus, ezért a kritikussá minősített típusok megközelítésére a KI-, az II-, és a KII tudományos magyarázata a leghelyénvalóbb. Egy internetes szolgáltatás létfontosságúvá válása mindenkire nézve szubjektív, ezért a KRISZ definícióját az infrastrukturális kötöttségek rendelkezésre állását feltételezve, a szolgáltatási tevékenységet és a szolgáltatás leállásának következményeit alapul véve fogalmaztam meg.

Megállapítottam, hogy önmagában a KI, a KII és a KRISZ is önálló halmazt alkotnak, viszont közös metszetük esetén a KRISZ leállása a társadalom jelentős hányadára is kihatással van, vagy miatta a kormányzat valamely szereplője nem képes feladatait maradéktalanul ellátni. Az infrastrukturális háttéren túl, dolgozatomban részleteztem azokat a további nélkülözhetetlen elemeket, amelyek egy internetes szolgáltatást „felépítenek". Áttekintettem, hogy miként alakul ki kötődés internetes szolgáltatásokhoz, az milyen következményekkel jár, és miként változnak kritikussá azok az igénybe vevők számára.

Az elméleti megközelítést alátámasztotta a védelmi szféra dolgozói által kitöltött kérdőív, amely az előforduló internetes szolgáltatások igénybevételére és nyújtására egyaránt kitért. A felméréssel bizonyítottam, hogy egyes internetes szolgáltatások rendelkezésre állása nélkül, a rendvédelmi szervek feladataikat nem képesek maradéktalanul ellátni. Bebizonyosodott, hogy az internetes szolgáltatások meghatározzák a mindennapokat, azok elérhetetlenné válása a működésre súlyos kihatással van, így Kritikus Internetes Szolgáltatások a hipotézisnek megfelelően igenis léteznek.

A nevesített internetes szolgáltatások elemzésekor bizonyosságot nyert, hogy minden rendvédelmi szerv

- működtet információs, tájékoztató honlapot, hírfolyamot és elektronikus ügyintézést;
- biztosít e-mail, webmail hozzáférést a dolgozóinak;
- titkosított internetes csatornán keresztül, rendelkezésre állít bizonyos felhasználói körnek hozzáférést az informatikai rendszeréhez.

Az internetes szolgáltatások rendszerszintű vizsgálata során megállapítottam, hogy azok alrendszerekre és rendszer-elemekre bonthatók, amelyek a rendszerben betöltött szerepüknek megfelelően befolyásolják az internetes szolgáltatások működését. Megállapítottan, hogy az

internetes szolgáltatásoknak léteznek megkerülhetetlen alrendszerei, amelyek közül kiemelkedők az adatbáziskezelők, amelyek korunk információs társadalmának és vele együtt az informatikai szolgáltatásoknak is nélkülözhetetlen elemei. Az elvégzett vizsgálataimból azt a következtetést vontam le, hogy az adatbázisokban tárolt adatok egyrészt befolyásolják az internetes szolgáltatások működőképességét, másrészt a rosszindulatú tevékenységet folytatók célpontja, ezért az adatbáziskezelők internetes szolgáltatások melletti működése kiemelt fontosságú. Megállapítottam, hogy az internetes szolgáltatás és az adatbázis kezelő folyamatos kapcsolata miatt a támadóknak állandó felület áll rendelkezésükre az adatok megszerzéséhez, vagy kompromittáláshoz, és a védelmet legtöbb esetben magának az internetes szolgáltatás felhasználói felületének kell biztosítania.

Az internetes szolgáltatásokat „fogyasztó" társadalom szokásaival párhuzamosan, a Kritikus Internetes Szolgáltatások megjelenési formái is hasonló képet mutatnak. A Web pillanatnyilag is a legnépszerűbb internetes tájékoztatási forma, minden rendvédelmi szerv tart fenn saját honlapot, azokon pedig kötelező és választható tartalmakat egyaránt megjelentet. Fejlődésének köszönhetően számtalan alrendszeri elemmel rendelkezhet, biztosított benne az interaktivitás lehetősége, számtalan fejlesztési-, és keretrendszer áll rendelkezésre, amelyek persze hibázásra is adnak lehetőséget. Áttekintettem, hogy milyen szempontokat kell figyelembe venni egy stabil, hibatűrő webszerver működtetéséhez, továbbá milyen biztonsági intézkedéseket kell megtenni a Web támadásainak elhárításához.
Az elektronikus levelezés népszerűsége vetekszik a Web népszerűségével, továbbá rendelkezésre állása is több évtizedre tekint vissza, ugyanakkor a Kritikus Internetes Szolgáltatások szempontjából teljesen eltérő funkcióval rendelkezik; kettős szerepet is betölt, hisz egyrészt lehet támadási célpont, másrészt lehet támadási eszköz. Az elektronikus levelezés a teljes védelmi szférában rendelkezésre áll, minden rendvédelmi szervnek van saját interneten elérhető webmail rendszere, és szinte minden dolgozónak lehet saját munkahelyi e-mail címe. Dolgozatomban rámutattam, hogy a világon minden internetet használó személynek átlagban kettő darab e-mail címe van, továbbá az e-mail címet a személy megtestesítésére, beazonosítására használják, illetve a személyek beazonosításához az e-mail a legfőbb hitelesítő eszköz. Rámutattam arra a tényre is, hogy az elektronikus levelezés az interneten még mindig a legfőbb támadási eszköz, illetve bemutattam, hogy mit jelent a levelezőrendszer felhasználása és kihasználása. Az elektronikus levelezésben egyfajta szélmalomharc folyik a kártékony kódok és a kéretlen levelek tömege ellen, amely környezetben a megfelelő védelmi intézkedések alkalmazása nélkül, ezen internetes szolgáltatás mások számára szolgál eszközként kibertámadás végrehajtásához.

Egy internetes szolgáltatás üzemeltetése során visszatérően jelentkeznek olyan üzemeltetési feladatok, amelyek megkerülhetetlenek. Összefoglaltam azokat a megoldásokat és betartandó biztonsági intézkedéseket, amelyek hosszú távon segíthetnek megőrizni az internetes szolgáltatások rendelkezésre állását.

Az általam, a dolgozatban javasolt védelmi ajánlások rendszerezve, a KRISZ felépítéséhez igazodva tudnak segítséget adni azok felhasználóinak, és üzemeltetőinek. Természetesen a védelmi felfogások és szemléletek is eltérőek, a mostani egy hosszú évek rendszergazdai gyakorlatával rendelkező-, ugyanakkor döntési helyzetben is résztvevő felhasználó szemszögéből születtek.

ÚJ TUDOMÁNYOS EREDMÉNYEK

Az elvégzett vizsgálataimat, valamint a tudományos kutatómunkámat a következő tudományos eredményekben foglalom össze:

1. Megfogalmaztam a Kritikus Internetes Szolgáltatások létezését, megalkottam definícióját és tartalmi elemeit.

Az internetes szolgáltatások kritikussága sokkal inkább szubjektív, mint a hátteret biztosító eszközöké, szolgáltatásoké, ezért létezésükhöz a fennálló függőségeket és az esetleges megszűnés következményeit kellett vizsgálnom. Feltártam, hogy az internetes szolgáltatások kritikussága függ a szolgáltatások mögött húzódó infrastruktúráktól, továbbá az adott internetes szolgáltatás leállásának, kimaradásának hatásaitól, következményeitől. Figyelembe véve, hogy a háttérszolgáltatások leállásának egyenes következménye az internetes szolgáltatások megszűnése, evidens, hogy a Kritikus Internetes Szolgáltatás levezetése a függőségi viszonyból eredően onnét származtatható. A definícióhoz a kritikus infrastruktúrák és a kritikus információs infrastruktúrák megfogalmazásaiból kellett kiindulnom, figyelembe véve, hogy a Kritikus Internetes Szolgáltatás minden esetben részhalmaza a felette álló infrastruktúráknak.

2. Levezettem a Kritikus Internetes Szolgáltatások lehetséges kialakulását, kialakítását.

Rámutattam, hogy egyes internetes szolgáltatásokhoz az igénybe vevők részéről fennálló kötelezettség, vagy saját elhatározás miatt kötődés-, sőt néha függőség alakul ki, amely így kritikussá transzformálja az internetes szolgáltatásokat, így azok a „fogyasztók" lételemévé válnak. A kötődés kialakulása szolgáltatói érdek azzal a céllal, hogy a felhasználók adott internetes szolgáltatáshoz forduljanak, és ahhoz rendszeresen vissza is térjenek. Rávilágítottam, hogy a védelmi szféra hétköznapi működésében megjelenő, internetes szolgáltatásokra irányuló kötődés miként alakíthatja azokat rövid időn belül létfontosságúvá, kritikussá, továbbá mit jelent a kötődésből átalakult függőség és annak milyen következményei lehetnek.

3. Bizonyítottam, hogy Kritikus Internetes Szolgáltatások mind a védelmi szférában, mind a hétköznapokban léteznek.

Tényként kezelve, hogy a védelmi szféra az internet alkalmazása szempontjából egy szegmensét képviseli a társadalomnak, megállapítható, hogy amennyiben a védelmi szférában léteznek Kritikus Internetes Szolgáltatások, úgy a társadalomban is, sőt ott sokkal nagyobb nagyságrendben vannak jelen. Egy internetes szolgáltatás hiányát mérhetővé és tudományosan beazonosíthatóvá tenni az érintettek, azaz a felhasználók objektív megkérdezésével lehet

leginkább. A védelmi szférában készült felmérés kitért az internet „fogyasztói”, és szolgáltatói oldalára egyaránt, továbbá vizsgálta az esetleges megszűnés, vagy leállás következményeit is.
Az aktuális jogszabályokban található, internetes megjelenéssel kapcsolatos kötelezettségek, továbbá az (információs) infrastruktúrák, mint háttérszolgáltatások kritikusságára irányuló kutatások, valamint a védelmi szférában készített felmérés együttesen bizonyítja, hogy internetes szolgáltatások is lehetnek kritikusak, ezáltal a Kritikus Internetes Szolgáltatások léteznek. A felmérésben szereplő, nevesített internetes szolgáltatások összegzése és csoportosítása, valamint a témában folytatott ezirányú kutatómunkám feltárt számos, kritikusnak számító internetes szolgáltatást mind általánosságban, mind rendvédelmi alkalmazásban.

4. A Kritikus Internetes Szolgáltatások biztonságának vizsgálatával rámutattam azok lehetséges támadására, továbbá bizonyítottam a védekezés szükségességét és a védelemben alkalmazható legjobb gyakorlatokat.
A KRISZ alrendszereinek és rendszerelemeinek feltérképezése és vizsgálata bizonyította, hogy az internetes szolgáltatás annyira ellenálló, mint az őt alkotó egységek leggyengébb eleme, továbbá egyértelművé vált, hogy az adatbáziskezelő mint alrendszeri elem, elengedhetetlen napjaink Kritikus Internetes Szolgáltatásaiban. Az adatbáziskezelő, valamint az adatbázisok vizsgálatával bemutattam, hogy önmagában a tárolt adatok biztonságának hiánya is elegendő a KRISZ rendeltetésszerű működésének meghiúsulásához. A leggyakrabban előforduló internetes szolgáltatásokon keresztül, amelyek egyben a legtöbbször előforduló Kritikus Internetes Szolgáltatások is, bemutattam a Kritikus Internetes Szolgáltatási rendszereket, foglalkoztam azok biztonságos üzemeltetésével, illetve biztonsági kérdéseivel. Az elektronikus levelezés működésének részletezésével rámutattam annak kettős szerepére, hisz egyrészt állandó támadási célpontot jelent, másrészt támadási eszközként is funkcionál.

5. Védelmi ajánlást fogalmaztam meg a Kritikus Internetes Szolgáltatások biztonságos és eredményes üzemeltetéséhez, fenntartásához.
Az ajánlás átfogó, gyakorló informatikai és vezetői eszköz lehet a Kritikus Internetes Szolgáltatások fenntartására, a hosszútávú igénybevétel biztosítására.

A KUTATÁSI EREDMÉNYEK GYAKORLATI FELHASZNÁLHATÓSÁGA

Az értekezés felépítése elméleti és gyakorlati témakörök szerint került tagolásra, továbbá az egyik kutatási célkitűzés kimondottan a gyakorlati felhasználhatóságra irányult: „a kritikusnak vélt internetes szolgáltatások gyakorlati alkalmazásához kívánom bemutatni azokat a módszereket és ajánlásokat, amelyek az információbiztonság betartása mellett hozzásegítenek a folyamatos rendelkezésre állás megvalósításához." A harmadik fejezet gyakorlati megvalósításokat mutat be, a negyedik fejezet pedig gyakorlati ajánlásokat is tartalmaz, így a kutatási eredmények alkalmazása egyben a gyakorlati felhasználhatóságot is biztosítja.

AJÁNLÁSOK

1. Felhasználható a Nemzeti Közszolgálati Egyetem oktatási tevékenysége során, kiemelten a Hadtudományi és Honvédtisztképző Kar nemzetbiztonsági alap és mesterképzésén, valamint a Nemzetbiztonsági Intézet által oktatott tárgyak esetében, akár önálló oktatási anyagrészenként, akár forrásmunkaként, akár ajánlott irodalomként.
2. Az egyes fejezetek következtetései részben a leírtaknak megfelelően, további tudományos vizsgálatok, kutatások alapját képezheti, így például a Kritikus Internetes Szolgáltatások szélesebb körű vizsgálata, felmérése is megvalósítható.
3. A dolgozatomban feltártakat ajánlom felhasználásra a védelmi szférában dolgozó vezetőknek és informatikusoknak egyaránt, az informatikai szabályozások megalkotása-, az informatikai tárgyú beszállítókkal kötött szerződések előkészítése-, valamint az internetes szolgáltatások üzemeltetése során.
4. Az internetes szolgáltatások biztonsági kérdéseivel foglalkozó részeket mindenképpen ajánlom az internetet közvetlenül-, vagy közvetetten jövedelemszerzésre használó vállalkozások tulajdonosainak, illetve azon magánszemélyeknek, akik bármilyen formában tartósan működtetnek internet végpontot.
5. Az elektronikus levelezésről szóló fejezetet minden e-mail címmel rendelkező internet használónak ajánlom saját-, és mások internetes biztonságának fenntartása érdekében.

A DOKTORJELÖLT TÉMÁVAL KAPCSOLATOS PUBLIKÁCIÓS JEGYZÉKE

Lektorált folyóiratban megjelent cikkek:

1. Jéri Tamás: The Security Of Databases In Critical Internet Services, Hadmérnök X. Évfolyam 3. szám - 2015. szeptember ISSN 1788-1919;
Online: http://hadmernok.hu/153_18_jerit.pdf;
2. Jéri Tamás – Pándi Erik – Jobbágy Szabolcs: A hálózatok világa, Hírvillám, I. évf. 1. szám, Budapest, ISSN 2061-9499, 168-177. oldal, 2010.; Online: http://www.comconf.hu/kiadvany/hirvillam_1evfolyam_1szam.pdf;
3. Jéri Tamás – Pándi Erik – Jobbágy Szabolcs: A hálózatok védelmi aspektusai, Hírvillám, I. évf. 1. szám, Budapest, ISSN 2061-9499, 210-220. oldal, 2010; Online: http://www.comconf.hu/kiadvany/hirvillam_1evfolyam_1szam.pdf;
4. Jéri Tamás – Pándi Erik – Tóth András: A kommunikációs infrastruktúrákkal szembeni rosszakaratú tevékenységek:,
Hírvillám, I. évf. 1. szám, Budapest, ISSN 2061-9499, 276-288. oldal, 2010.; Online: http://www.comconf.hu/kiadvany/hirvillam_1evfolyam_1szam.pdf;
5. Jéri Tamás: A kommunikációs eszközök fejlődésének kihatásai a büntetés-végrehajtás rendszerére, Hadmérnök VII. Évfolyam 2. szám - 2012. június ISSN 1788-1919; Online: http://www.hadmernok.hu/2012_2_jeri.pdf;
6. Jéri Tamás: Kritikus internetes szolgáltatások, Hadmérnök VIII. Évfolyam 1. szám - 2013. március ISSN 1788-1919; Online: http://www.hadmernok.hu/2013_1_jerit.pdf;
7. Jéri Tamás: A kritikus internetes szolgáltatások biztonságos üzemeltetése, Hadmérnök X. Évfolyam 1. szám - 2015. március ISSN 1788-1919; Online: http://www.hadmernok.hu/151_20_jerit_2.pdf
8. Jéri Tamás: Az adatbázis-kezelők szerepe a kritikus internetes szolgáltatásokban, Hadmérnök X. Évfolyam 1. szám - 2015. március ISSN 1788-1919; Online: http://www.hadmernok.hu/151_19_jerit_1.pdf
9. Jéri Tamás: A Web szerepe a kritikus internetes szolgáltatásokban, Hadmérnök X. Évfolyam 3. szám - 2015. szeptember ISSN 1788-1919; Online: http://www.hadmernok.hu/153_17_jerit.pdf

Konferencia kiadványban megjelent cikk:

10. Jéri Tamás: A Kritikus Internetes Szolgáltatások alrendszerei, A Haza Szolgálatában konferenciakötet; Társadalom és Honvédelem XVII. évf. 3-4. szám ISSN 1417-7293 2013. 205-214. oldal;

A DOKTORJELÖLT SZAKMAI-TUDOMÁNYOS ÉLETRAJZA

Személyi adatok

Név: Jéri Tamás

Születési hely, idő: Kalocsa, 1974.07.08

Munkahelyek és beosztások

2020 –	Kalocsai Vagyonhasznosítási és Könyvvezető Nonprofit Kft.; ügyvezető
2018 – 2019	Tolna Megyei Bv. Intézet; mb. parancsnok
2011 – 2017	Kalocsai Fegyház és Börtön; parancsnok-helyettes
2000 – 2011	Kalocsai Fegyház és Börtön; informatikai osztályvezető
1998 – 2000	Büntetés-végrehajtás Országos Parancsnoksága; főmunkatárs
1994 – 1998	Kalocsai Fegyház és Börtön; felügyelő, őr, előadó, főelőadó

Tanulmányok

2015	PhD. Doktori képzés abszolutórium; NKE Katonai Műszaki Doktori Iskola
2010	MSc védelmi vezetéstechnikai rendszerszervező; ZMNE
2004	Mérnök Informatikus diploma; GDF
1992	Érettségi – Közgazdasági szakközépiskola

Nyelvismeret

Angol	középfok, komplex
Orosz	alapfok, komplex