NEMZETI
KÖZSZOLGÁLATI EGYETEM
Doktori Tanács

KOVÁCS ZOLTÁN
NB. DANDÁRTÁBORNOK

- Az infokommunikációs rendszerek nemzetbiztonsági kihívásai -

című doktori (PhD) értekezésének szerzői ismertetése és
hivatalos bírálatai

Budapest
2015.

NEMZETI KÖZSZOLGÁLATI EGYETEM

KOVÁCS ZOLTÁN NB. DANDÁRTÁBORNOK

- Az infokommunikációs rendszerek nemzetbiztonsági kihívásai -

című doktori (PhD) értekezésének szerzői ismertetése és
hivatalos bírálatai

Témavezető:

Prof. Dr. Kovács László ezredes (PhD)
egyetemi tanár

Budapest
2015.

1. A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

Az elmúlt évtizedekben az infokommunikációs rendszerek rohamosan fejlődtek. A mobil kommunikációs rendszerek és az internet világméretű elterjedése, a rendelkezésünkre álló adatátviteli sávszélesség folyamatos növekedése, és a felhasználási lehetőségek gyarapodása azt eredményezte, hogy mára a gyors és nagy tömegű adatcsere életünk szerves részévé vált. Az elterjedt technológiák alkalmazásával olcsón, gyorsan és hatékonyan vagyunk képesek ellátni munkahelyi feladatainkat és megoldani hétköznapi problémáinkat egyaránt. Napjaink két, az infokommunikációt jelentősen meghatározó trendje a felhő alapú rendszerek előretörése, valamint a mobil eszközök és az azokon futó alkalmazások piaci részesedésének a növekedése.

Ezek a trendek a nemzetbiztonsági és a rendvédelmi szerveket **kettős kihívás** elé állítják. **Egyrészről** az új technológiák egy részét **felhasználóként** – vagy saját maguk, vagy az általuk információbiztonság szempontjából is védett állami vezetők – **igénybe fogják venni**, ezért meg kell győződniük arról, hogy az adott rendszer kielégíti az általuk meghatározott – sokszor igen magas – biztonsági követelményeket, ugyanakkor tisztában kell lenniük azok minden fennmaradó biztonsági kockázatával is. **Másrészről az új technológiák esetében is meg kell oldani a hatáskörükbe tartozó törvényes ellenőrzést.**

Jelenleg azonban nem létezik olyan egységes ajánlás, amely megmutatja, hogy milyen kritériumokat kell vagy célszerű megvizsgálni egy teljes körű biztonsági elemzéshez felhő alapú rendszer szervezeti szintű felhasználása esetén, mint ahogy nincs egységes ajánlás arra nézve sem, hogy mit kell vagy célszerű oktatni a kiemelt, védett vezetőknek egy információbiztonság-tudatossági felkészítés keretében.

Nem található továbbá olyan összehasonlító elemzés sem, amely a szolgálatokat segítendő bemutatná az új technológiák törvényes ellenőrzésére jelenleg alkalmas technikai módszereket, összehasonlítaná azokat előnyeikkel, hátrányaikkal együtt, mint ahogy nem található olyan egységes szempontrendszer sem, amellyel akár egy már meglévő, akár egy új módszer adott feladatra alkalmassága megvizsgálható. Hiányként merül fel továbbá, hogy jogszabályba illeszthető fogalmi meghatározása csupán a hagyományos hírközlési szolgáltatóknak van, az új típusú, újonnan megjelent szolgáltatóknak viszont nincs, és ez ma már jelentősen akadályozza a hatékony törvényes ellenőrzést.

2. KUTATÁSI CÉLOK

A fentiek alapján kutatásom célja is kettős. Egyfelől felhasználói, másfelől törvényes ellenőrzési szempontból vizsgálom meg a korszerű infokommunikációs rendszerek közül az internet-technológiára épülő szolgáltatásokat, azon belül pedig kiemelten a felhő alapú rendszereket.

Felhasználói szempontból két fő célom van. Egyrészt egy olyan biztonsági követelményrendszer megalkotása, amellyel az említett rendszerek, kiemelten a felhő alapú rendszerek vizsgálhatóak, azok használatának, alkalmazásának kockázatai felmérhetőek, másrészt pedig ezen rendszerek használatához kapcsolódóan egy lehetséges biztonságtudatossági felkészítés tartalmi elemeinek kidolgozása védett vezetők számára.

Törvényes ellenőrzési szempontból pedig célom egy olyan keretrendszer felállítása, amely megmutatja az említett rendszerek törvényes ellenőrzésének lehetőségeit, azok előnyeit, hátrányait, kockázatait, és ajánlásokat fogalmaz meg kialakításukkal, kialakíthatóságukkal kapcsolatban, valamint – akár jogszabályba illeszthető módon – fogalmi meghatározást ad az újonnan megjelent szolgáltatókra.

Céljaimat a fejlett országok nemzeti és nemzetközi szervezetei által megalkotott elérhető ajánlások, az iparági szabványok és bevált gyakorlatok, valamint a törvényes ellenőrzésről nyíltan rendelkezésre álló információk felhasználásával és továbbfejlesztésével, valamint a nemzetbiztonsági és rendvédelmi szervek igényeihez történő hozzáigazításával kívánom elérni. A kutatási területek kiválasztásánál azokra a részfeladatokra koncentrálok, melyek világszerte kidolgozatlan és megoldatlan problémaként jelentkeznek a nemzetbiztonsági és a rendvédelmi szervek számára.

A kutatási célkitűzéseimet a következő részcélokra bontott kutatómunkával valósítom meg:

1. A felhő alapú rendszerek biztonsági vizsgálatához szükséges követelményrendszer megalkotása;
2. Információbiztonsági felkészítés tartalmi elemeinek kidolgozása védett vezetők számára;
3. Az internet-technológiára épülő szolgáltatások törvényes ellenőrzési lehetőségei elvi kialakítása, előírásainak megfogalmazása.

3. 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,
- összehasonlító elemzés;
- általánosítás, mint vizsgálati módszer;
- kutatások másodelemzése: korábbi, a témában készült kutatási eredmények elemzése feldolgozása,
- logikai elemzés: a feltárt adatok feldolgozása, elemzése, értékelése, ebből következtetések levonása után javaslatok megfogalmazása
- empirikus kutatások: saját megszerzett szakmai tapasztalatok felhasználása, leírása
- konferenciákon, konzultációkon, rendezvényeken való részvétel, jogszabályi javaslatok kidolgozása, projektekben való részvétel
- eredmények publikálása: kutatási eredmények feldolgozása, cikkek, egyetemi jegyzet fejezetek formájában történő publikálása, valamint konferenciákon és oktatásban történő előadása.

4. AZ ELVÉGZETT VIZSGÁLAT TÖMÖR LEÍRÁSA FEJEZETENKÉNT

A fentieknek megfelelően az értekezésemet az alábbi négy fejezet szerint építettem fel:

Az **első fejezet**ben a felhő alapú rendszerek értelmezésével foglalkozom, szolgáltatási -, és telepítési modellek szerint csoportosítva megvizsgálom azok tulajdonságait, előnyeit, hátrányait. Elemzem, hogy mi a különbség a felhő alapú rendszerek és a virtualizáció, a kiszervezés, valamint az internet-technológiára épülő szolgáltatások között. Megvizsgálom, hogy ma értelmezhető-e a kormányzati és a rendvédelmi felhő fogalma, valamint bemutatom, hogy a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek érdemes és kell is foglalkozniuk a felhő alapú rendszerekkel.

A **második fejezet**ben nemzetbiztonsági szolgálatok és a rendvédelmi szervek szempontjából elemzem és értékelem a felhő alapú rendszerekkel foglalkozó nemzeti és nemzetközi szervezetei által megalkotott, nyíltan elérhető, a dolgozat célkitűzése szempontjából releváns biztonsági ajánlásokat, majd felállítok egy, az említett rendszerek komplex vizsgálatához alkalmazható új szempontrendszert. Ennek segítségével, az elemzett ajánlásokat összefoglalva, kiegészítve, elkészítek egy, a felhő alapú rendszerek biztonsági elemzését a rendvédelmi szervek számára egységes keretek között lehetővé tevő sablont.

A **harmadik fejezet**ben elemzem a védett vezetők információbiztonsági felkészítésének főbb kérdéseit, bemutatom a védett vezetők információbiztonsági védelme kiterjesztésének szükségességét az általuk használt kibertérre. Az előző fejezetben felállított szempontrendszer segítségével elemzem az általuk leggyakrabban használt internet-technológiára épülő szolgáltatások és személyi használatú hordozható infokommunikációs eszközök jellemzőit, azok veszélyeit, majd a védett vezetőkre szabott keretrendszer segítségével összeállítom a biztonságtudatos használatra történő felkészítés egy lehetséges módszerét.

A **negyedik fejezet**ben az internet-technológiára épülő szolgáltatások törvényes ellenőrzési lehetőségeit veszem górcső alá. Nyíltan elérhető forrásokból származó nemzetközi példákon keresztül bemutatom, hogy a törvényes ellenőrzésére milyen lehetőségek állnak rendelkezésre, milyen technikai és jogi problémák merülnek fel alkalmazásuk kapcsán. Ezeket felhasználva felállítok egy, a törvényes ellenőrző módszerek vizsgálatához általánosan használható szempontrendszert, amellyel az erre feljogosított szervek képesek akár a meglévő, akár a jövőben megjelenő új módszerek adott célra való megfelelőségét is megvizsgálni. Mindemellett javaslatot teszek egy, a mára már elavult hírközlési modellt potenciálisan felváltani képes új modellre úgy, hogy jogszabályokba illeszthető fogalmi meghatározást is adok annak egyes szereplőire.

5. Összegzett következtetések

Értekezésem elkészítése során a felhő alapú rendszerek nemzetbiztonsági kihívásaira koncentráltam, ugyanakkor figyelembe vettem azt a tényt, hogy ezek a rendszerek önállóan nem vizsgálhatóak.

Az első fejezetben bemutattam a felhő alapú rendszereket, azok meghatározásait, az elfogadott modelleket, sajátosságaikat, jellemezőiket, meghatároztam azok előnyeit, hátrányait, egységesen összefoglalva és kiegészítve a szakirodalomban található, meglehetősen heterogén, sokszor hiányos és nem konzekvens felsorolásokat. Áttekintettem **a kormányzati felhőre** adott meghatározásokat, és **megállapítottam**, hogy erre jelenleg **nincs egységesen elfogadott definíció**. Miután véleményem szerint **ennek gyakorlati haszna is lenne, ezért saját meghatározást adtam először a kormányzati felhő, majd ebből kiindulva a rendvédelmi felhő fogalmára**. Tisztáztam azt is, hogy mi a különbség a felhő alapú rendszerek és egyrészt a hagyományos ICT rendszerek virtualizációja, másrészt a kiszervezett ICT rendszerek és szolgáltatások, harmadrészt az internet-technológiára épülő szolgáltatások között. Megállapítottam, hogy jelenleg nem lehet éles határvonalat húzni az

internet-technológiára épülő szolgáltatások és az annak részhalmazát képező PC/SaaS rendszerek között, sőt és az új szolgáltatások megjelenésének ütemét, az általuk kínált, a korábbiaktól sokszor merőben eltérő új funkcióikat, lehetőségeket figyelembe véve, ezt jó ideig még nem is lehet egyértelműen megtenni. Az iparági tendenciák és előrejelzések figyelembevételével **bizonyítottam, hogy a nemzetbiztonsági szolgálatoknak és a rendvédelmi szerveknek a felhő alapú rendszerekkel a** lehetséges **felhasználás, a védett vezetők információbiztonságának emelése és a törvényes ellenőrzés biztosítása okán is mindenképpen foglalkozniuk kell**.

A második fejezetben **elemeztem és értékeltem a fejlett országok felhő alapú rendszerekkel foglalkozó nemzeti-, és a nemzetközi szervezetei által megalkotott, nyíltan elérhető, a dolgozat célkitűzése szempontjából releváns biztonsági ajánlásokat**, így a CSA, a NIST, a FedRAMP, a BSI, valamint az ENISA illeszkedő dokumentumait, és ezekben feltártam a biztonság értékeléséhez szükséges kockázatokat. **Megállapítottam, hogy az egyes szervezetek heterogén módon vizsgálják az adott kérdést**, ahol három alapvető kiindulásbeli különbség azonosítható. Az első, hogy a **szolgáltató vagy a felhasználó oldaláról** közelítik-e meg a kérdést, a második, hogy **a megcélzott felhasználó civil vagy kormányzati szervezet, esetleg magánember**-e, a harmadik pedig, hogy az ajánlást készítő szervezet **az Egyesült Államok vagy az Európai Unió jelenlegi technikai és jogi környezetéből indul**-e ki. **Megállapítottam** azt is, hogy bár **egyik sem a rendvédelmi szervek szemszögéből vizsgálódott**, ezek ellenére a dokumentumokban megfogalmazottak megfelelő újragondolással és átalakítással felhasználhatók akár egy, a hazánk rendvédelmi szerveinek szóló biztonsági sablon elkészítéséhez.

A különböző szervezetek ajánlásaiban a telepítési modellek előnyeiről, hátrányairól leírtak alapján azt a következtetetést vontam le, hogy a rendvédelmi szervek számára napjainkban felhasználóként a közösségi felhő jelentheti az optimális megoldást.

A felhő alapú rendszerek biztonsági kérdéseinek rendvédelmi szervek szemszögéből történő komplex vizsgálatához egy új szempontrendszert állítottam fel. Ez egy olyan 4 dimenziós tér, amelynek „a rendvédelmi szerv szerepe – telepítési modellek – szolgáltatási modellek – vizsgálandó biztonsági kérdéscsoportok” az elemei. Ebben a „vizsgálandó biztonsági kérdéscsoportoknál” szintén egy új kategorizálásban vezettem be, az „üzembiztonság – adatbiztonság – egyéb (jogi, fizikai stb.) biztonság – törvényes ellenőrzés” csoportosítást. Ez utóbbiaknál meghatároztam, hogy mit tekintek üzembiztonsági, adatbiztonsági, egyéb (jogi, fizikai stb.) biztonsági, valamint törvényes ellenőrzési kategóriába tartozó kérdésnek, ezek technikai vagy jogi úton oldhatók-e meg, valamint, hogy

a felhasználó és a szolgáltató érdekei és felelősségi körei itt hogyan viszonyulnak egymáshoz. Ennek segítségével az említett szervek bármely feladatuk kapcsán, komplex módon haladhatnak végig egy adott rendszer vizsgálatán.

A fentiek felhasználásával **megalkottam a rendvédelmi szervek számára egy, a felhő alapú rendszerek minimálisan elvárt biztonsági szintjének megállapítására szolgáló elemző sablont**, valamint annak használati útmutatóját. Rávilágítottam, hogy ez egyrészt a technikai fejlődésnek és az egyéb igényeknek köszönhetően akár önmagában is továbbfejleszthető, másrészt ezt alapként használva, a vizsgálati szint kibővíthető az egyes biztonsági részterületeket mélyebben elemző újabb sablonok előállításával.

Feltártam és leszögeztem, hogy a törvényes ellenőrzés kapcsán célszerű lenne bevezetni és szabványosítani a Lawful Monitoring as a Service (LMaaS) (vagy valami hasonló) fogalmát, amelynek keretében a szolgáltató szolgáltatásként, egységes megközelítés és feltételek mellett biztosíthatná az ellenőrzést végző szervek számára a szükséges és a különböző jogszabályok által igényelhető információkat.

A harmadik fejezetben a védett vezetők információbiztonsági védelmének főbb kérdéseit elemeztem. Rámutattam, hogy a technikai elhárítást ki kell terjeszteni a védett vezetők által használt személyi használatú hordozható infokommunikációs eszközöket és internet-technológiára épülő szolgáltatásokat is. Megállapítottam azt is, hogy **csak technikai úton az információbiztonsági védelmet nem lehet, vagy irreálisan drága kialakítani, ugyanakkor az információk megvédésének egyik leghatékonyabb és legolcsóbb módja a biztonságtudatos használat**. Ennek kialakításához viszont személyre szabott felkészítési módszert célszerű megalkotni. A korábban már használt kategorizálás mentén bemutattam, hogy milyen releváns veszélyek állnak fenn, ezek közül melyikre és milyen mértékű ráhatása lehet a felhasználónak. **A feltárt veszélyek, valamint a fenti keretrendszer segítségével kidolgoztam a védett vezetők számára a személyükre szabott biztonságtudatos használathoz kapcsolódó alap információbiztonsági felkészítési módszert**, úgy, hogy az akár egy új szolgáltatás vagy eszköz igénybe vétele esetén is megfelelő legyen. Megállapítottam, hogy ez az oktatás szükséges, de önmagában nem elégséges. A továbblépést négy kategóriában tartom célszerűnek: a magasabb szintű megközelítést igénylő, a védett vezető által megtehető, az üzemeltetést végző személyek által megtehető, valamint a technikai elhárítást végzők által megtehető feladatok esetében.

A negyedik fejezetben az internet-technológiára épülő szolgáltatások, ezen belül pedig kiemelten a PC/SaaS felhő alapú rendszerek törvényes ellenőrzési lehetőségeit elemeztem. Ennek kapcsán bemutattam, hogy az infokommunikációs eszközökben, szolgáltatásokban

jelentkező technológiai konvergencia a törvényes ellenőrzés feladatainak konvergenciáját is indukálja, amely alapvető változásokat indít el ebben a feladatkörben is.

Bizonyítottam, hogy az elektronikus úton folytatott kommunikáció egy sokkal szélesebben értelmezhető fogalom, mint a hírközlés, ráadásul a hagyományos hírközlési formák egyre inkább veszítenek jelentőségükből a felhasználók, így a törvényes ellenőrzést végzők számára is. Mivel **a hírközlési szolgáltatói modell már nem felel meg a mai viszonyoknak, ezért felállítottam az azt felváltó új, infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modellt**. Bemutattam azt is, hogy **az elektronikus úton folytatott kommunikáció változásában nagy szerepük van az internet-technológiára épülő szolgáltatásoknak**, **ám ezek törvényes ellenőrzése jogi és technikai** problémákba **ütközik**. Nyílt forrásokból merítve nemzetközi kitekintést adtam a jelenleg rendelkezésre álló jellemző lehetőségekről, módszerekről, majd ezt felhasználva, tulajdonságaikat is ismertetve, csoportosítottam azokat.

Felállítottam egy, a törvényes ellenőrző módszerek vizsgálatához általánosan használható új szempontrendszert, majd az itt megadott értékelési feltételek figyelembe vételével elemeztem a jelenleg rendelkezésre álló módszereket és táblázatos formában összegeztem azok főbb előnyeit, hátrányait. Ennek segítségével a felhatalmazott szervek amellett, hogy képesek dönteni egy adott módszer bevezetéséről, bármilyen más, akár teljesen új ellenőrzési módszer elemzését is elvégezhetik.

Egyértelműen megállapítottam, hogy az internet-technológiára épülő szolgáltatások törvényes ellenőrzése minden ország érintett szerve számára kihívást jelent, amelynek egyik oka, hogy egyik módszer sem nyújt teljes körű megoldást az igényelt adatok megszerzéséhez, a másik oka pedig a meglévő jogi szabályozás hiányosságai. Bizonyítottam azt is, hogy az alkalmazásszolgáltatóval való együttműködés **kikerülhetetlen, ugyanakkor éppen ennek jogi szabályozottságában lelhető fel a legtöbb hiány**. **A jogi hiányosság feloldásában elkerülhetetlen az érintett piaci szereplők, azaz a szolgáltatók új, a törvényes ellenőrzés szempontjából is megfelelő meghatározása**, amely az általam felállított infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modell szerint megtehető. A jelenleg elérhető hazai és külföldi fogalmi meghatározások elemzését követően **meghatározást adtam az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmára** oly módon, hogy azok beilleszthetők legyenek a velük foglalkozó, így a törvényes ellenőrzési tárgyú törvényekbe és egyéb jogszabályokba is. Ebbe minden szolgáltató, szolgáltatás elhelyezhető, ugyanakkor leszögeztem, hogy a hírközlési szolgáltató és szolgáltatás fogalmát a továbbiakban is célszerű fenntartani.

6. ÚJ TUDOMÁNYOS EREDMÉNYEK

1. **A felhő alapú rendszerek használatához kapcsolódó** biztonsági kérdések rendvédelmi szervek szemszögéből történő **komplex vizsgálatához új szempontrendszert dolgoztam ki.**
2. **Megalkottam a rendvédelmi szervek számára a felhő alapú rendszerek biztonsági értékeléséhez** szabadon **felhasználható elemző sablont**, valamint annak használati útmutatóját.
3. **Kidolgoztam a védett vezetők számára a személyükre szabott biztonságtudatos használathoz kapcsolódó alap információbiztonsági felkészítési módszert**.
4. **Kidolgoztam egy, a törvényes ellenőrző módszerek vizsgálatához általánosan használható szempontrendszert**, amelyben megadtam az egyes szempontok értékelésének feltételét.
5. A **jelenlegi** hírközlési szolgáltatói modell helyett **kidolgoztam** az azt potenciálisan felváltó **új, infrastruktúra-, alkalmazás-, és tartalomszolgáltatói modellt**, valamint **fogalmi meghatározást adtam az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmára**.

7. A KUTATÁSI EREDMÉNYEK GYAKORLATI FELHASZNÁLHATÓSÁGA

- Felhasználható a nemzetbiztonsági szolgálatok és a rendvédelmi szervek számára az infokommunikációs rendszerek, ezen belül kiemelten a felhő alapú rendszerek biztonságos használata szintjének emeléséhez.
- Segítheti a védett vezetők információbiztonság-tudatosságának emelését.
- Felhasználható a titkos információgyűjtésre és titkos adatszerzésre feljogosított szervezetek számára az infokommunikációs rendszerek, ezen belül kiemelten a felhő alapú rendszerek törvényes ellenőrzése kapcsán egy adott feladathoz a megfelelő módszer kiválasztása, valamint bármilyen más, akár új módszer elemzéséhez.
- A megalkotott szolgáltatói modell és definíciók felhasználhatók az infokommunikációs rendszerekkel kapcsolatos titkos információgyűjtés és titkos adatszerzés új jogszabályi környezetének kialakításához.

- Felhasználható a Nemzeti Közszolgálati Egyetem oktatási tevékenysége során, akár önálló oktatási anyagrészenként, akár forrásmunkaként, akár ajánlott irodalomként.
- Felhasználható a Kormányzati Eseménykezelő Központ (GovCERT) tudatosító tevékenysége során.
- Az értekezés egyes elemei megfelelő adaptációval más kormányzati szervnél, gazdasági társaságnál vagy akár a magán szférában is felhasználhatók.
- További tudományos vizsgálatok, kutatások alapját képezheti.

8. AJÁNLÁSOK

Kutatási eredményeim ajánlom felhasználni továbbá:

- az infokommunikációs rendszerek, azon belül is elsősorban a felhő alapú rendszerek biztonsági kérdéseivel foglalkozó szakembereinek;
- a Nemzeti Közszolgálati Egyetem hallgatóinak és oktatóinak;
- az infokommunikációs titkos információgyűjtésen és titkos adatszerzésen túli új jogszabályainak kialakításával foglalkozó szakemberek számára.

9. A DOKTORJELÖLT TÉMÁVAL KAPCSOLATOS PUBLIKÁCIÓS JEGYZÉKE

Lektorált folyóiratban megjelent cikkek

1. Kovács Zoltán: Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél. Hadmérnök. VI. Évfolyam 4. szám - 2011. december, pp. 176-188. ISSN 1788-1919 Online: http://hadmernok.hu/2011_4_kovacsz.php
2. Kovács Zoltán: Cloud Security in Terms of the Law Enforcement Agencies. Hadmérnök. VII. Évfolyam 1. szám - 2012. március, pp. 144-156. ISSN 1788-1919 Online: http://hadmernok.hu/2012_1_kovacsz.pdf
3. Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési problémái. Hadmérnök. VIII. Évfolyam 1. szám - 2013. március, pp. 233-241. ISSN 1788-1919 Online: http://hadmernok.hu/2013_1_kovacsz.pdf
4. Kovács Zoltán: „Electronic Written Tasking Order System" Accomplished Within the Project „Secure Electronic Communication" I. Hadmérnök. VIII. Évfolyam 3. szám - 2013. szeptember, pp. 171-183. ISSN 1788-1919 Online: http://hadmernok.hu/133_17_kovacsz_1.pdf

5. Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I. Hadmérnök. VIII. Évfolyam 3. szám - 2013. szeptember, pp. 184-197. ISSN 1788-1919 Online: http://hadmernok.hu/133_18_kovacsz_2.pdf
6. Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata II. Hadmérnök. VIII. Évfolyam 3. szám - 2013. szeptember, pp. 198-210. ISSN 1788-1919 Online: http://hadmernok.hu/133_19_kovacsz_3.pdf
7. Kovács Zoltán: „Electronic Written Tasking Order System" Accomplished Within the Project „Secure Electronic Communication" II. Hadmérnök. VIII. Évfolyam 4. szám - 2013. december, pp. 201-209. ISSN 1788-1919 Online: http://hadmernok.hu/134_17_kovacsz.pdf
8. Kovács Zoltán: „Electronic Written Tasking Order System" Accomplished Within the Project „Secure Electronic Communication" III. Hadmérnök. IX. Évfolyam 1. szám - 2014. március, pp. 199-208. ISSN 1788-1919 Online: http://hadmernok.hu/141_19_kovacsz.pdf
9. Gazdag Tibor – Kovács Zoltán: Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei. Nemzetbiztonsági Szemle. II. Évfolyam 2. szám - 2014. június, pp. 36-57. ISSN 2064-3756 Online: http://uni-nke.hu/uploads/media_items/gazdag-tibor-kovacs-zoltan-felho-alapu-uj-penzugyi-tranzakcios-lehetosegek-es-azok-veszelyei.original.pdf
10. Kovács Zoltán: Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából I. Hadmérnök. IX. Évfolyam 2. szám - 2014. június, pp. 277-289 ISSN 1788-1919 Online: http://hadmernok.hu/142_26_kovacsz_1.pdf
11. Kovács Zoltán: Hordozható infokommunikációs eszközök használatának veszélyei a védett vezetők biztonságtudatossági képzésének szempontjából II. Hadmérnök. IX. Évfolyam 2. szám - 2014. június, pp. 290-296 ISSN 1788-1919 Online: http://hadmernok.hu/142_27_kovacsz_2.pdf
12. Kovács Zoltán: Hordozható infokommunikációs eszközök használatához kapcsolódó biztonságtudatossági képzési tematika védett vezetők számára. Hadmérnök. IX. Évfolyam 3. szám - 2014. szeptember, pp. 182-190 ISSN 1788-1919 Online: http://www.hadmernok.hu/143_14_kovacsz.pdf
13. Kovács Zoltán: Infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmi meghatározása a törvényes ellenőrzés szemszögéből. Nemzetbiztonsági Szemle. II. Évfolyam 4. szám - 2014. december, pp. 3-28 ISSN 2064-3756 Online: http://uni-

nke.hu/uploads/media_items/nemzetbiztonsagi-szemle-2014-4-2.original.pdf (2014.11.27.)

14. Kovács Zoltán: Védett vezetők hordozható infokommunikációs eszközeinek védelme a rádiófrekvenciás tartományban. Bolyai Szemle. XXIII. Évfolyam 2014/4. szám, pp. 58-75 ISSN 1416-1443 Online: http://uni-nke.hu/downloads/kutatas/folyoiratok/bolyai_szemle/Bolyai_Szemle_2014_04_elektron.pdf

Konferencia kiadványban megjelent cikkek

15. Kovács Zoltán: Felhő-alapú informatikai rendszerek, mint nemzetbiztonsági kihívás. Hadtudomány XXIII. Évfolyam 1-2. szám - 2013. március, pp. 5-12 ISSN 1215-4121 Online: http://mhtt.eu/hadtudomany/2013/1_2/HT_2013_1-2_mhtt.pdf

Konferencia kiadványban megjelent kivonatok

16. Kovács Zoltán: Hordozható infokommunikációs eszközök használatához kapcsolódó biztonságtudatossági képzési tematika védett vezetők számára. In: A haza szolgálatában 2014 konferencia rezümékötet. Szerk.: Kiss Dávid, Orbók Ákos. Nemzeti Közszolgálati Egyetem. Budapest 2014. pp. 160-161. ISBN:978-615-5491--88-7

Egyetemi jegyzet fejezetek:

17. Dobák Imre - Kovács Zoltán: Új technológiák hatása a hírszerzésre. In: A nemzetbiztonság általános elmélete. Szerk.: Dobák Imre. Nemzeti közszolgálati Egyetem Nemzetbiztonsági Intézet. Budapest 2014. pp. 206-220. ISBN: 978-615-5305-49-8

10.A DOKTORJELÖLT SZAKMAI-TUDOMÁNYOS ÉLETRAJZA

Név: Kovács Zoltán
Telefonszám: + 36 30 520-5993
E-mail: zkovacs@nbsz.gov.hu

Végzettség:

2012 –	Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Katonai Műszaki Doktori Iskola
2001 – 2004	Budapesti Közgazdaságtudományi és Államigazgatási Egyetem, Gazdálkodástudományi kar, Vállalatgazdasági szak – mérnök-közgazdász
1986 – 1991	Budapesti Műszaki Egyetem, Villamosmérnöki kar, Híradástechnika szak – okleveles villamosmérnök
1981 – 1985	Corvin Mátyás Híradástechnikai Szakközépiskola – elektronikai műszerész

Nyelvismeret:

nyelv	vizsga típusa	kiállító intézmény
angol	középfok A + B	Állami Nyelvvizsga Bizottság
angol (katonai szakanyaggal bővített)	középfok B	Zrínyi Miklós Nemzetvédelmi Egyetem
francia	komplex alapfok (B1)	Budapesti Műszaki és Gazdaságtudományi Egyetem

Fontosabb tanfolyamok:

2011	Top Senior Police Officer Course TOPSPOC IX – 2011 – European Police College
2011	FBI vezetőképző tanfolyam – International Law Enforcement Academy
2005	Senior Executive Seminar – Georg C. Marshall European Center for Security Studies
1994	A GSM páneurópai digitális mobil távközlő rendszer – Budapesti Műszaki Egyetem Mérnöktovábbképző Intézet
1992	Mobil távközlő rendszerek – Budapesti Műszaki Egyetem Mérnöktovábbképző Intézet

Szakmai tevékenység:

1992 –	Nemzetbiztonsági Szakszolgálat (és jogelődei)
1991 – 1992	CANSYS Informatikai Kft.

Budapest, 2015. év augusztus hó 19. nap

aláírás