ZRÍNYI MIKLÓS
NEMZETVÉDELMI EGYETEM

Kassai Károly mk. alezredes

A MAGYAR HONVÉDSÉG INFORMÁCIÓVÉDELMÉNEK — MINT A BIZTONSÁG RÉSZÉNEK — FELADATRENDSZERE

Doktori (PhD) értekezés

Tézisfüzet

Témavezető: Dr. habil Sándor Miklós nyá. ezds.

Budapest, 2007

A TUDOMÁNYOS PROBLÉMA MEGFOGALMAZÁSA

A napjainkban tapasztalható fejlődés robbanásszerűen növeli a vezetéshez és működéshez szükséges információk fontosságát és mennyiséget, így az adatokat, és az információs rendszereket egyre bonyolultabb védelemmel kell ellátni. NATO és EU tagságunk is új információbiztonsági kihívásokat és kötelezettségeket jelent.

A Magyar Honvédségnél (MH) a jogszabályoknak és az állami irányítás egyéb jogi eszközeinek megfelelő eszközökkel és eljárásokkal történik a kezelt adatok védelme. Azonban hazánkban az információvédelemre vonatkozó szabályozók *nem ölelnek fel minden védelmi területet* (pl. a nemzeti elektronikus adatok védelme), másrészt *nem egyformán részletezettek*, illetve *nem pontosan illeszkednek egymáshoz* (pl. a nemzeti és NATO minősített adatok védelmének rendszabályai). Az MH belső rendelkezéseiben sehol sem szerepel az *információvédelem átfogó értelmezése, területeinek és feladatainak kijelölése*.

A fentiek alapján indokolt, hogy az információbiztonság területén is megkezdődjön a feladatok *rendszer szemléletű* vizsgálata, mert *az adatkezelő rendszerek korszerűsítése a védelmi kérdések kutatása nélkül elképzelhetetlen*.

KUTATÁSI CÉLOK, A TÉMA HATÁROLÁSA

Az egyre veszélyesebb információs fenyegetések ellensúlyozásaként az információs rendszerek védelmi feladatainak *rendszerszemléletű megközelítésével* megfogalmazható, hogy *milyen területeken, milyen módszerekkel lehet és kell védeni* az MH-nál kezelt nemzeti és szövetségi (vagy egyéb külföldi) adatokat, és *hogyan kell a védelmi rendszabályokat egységesen menedzselni*. Ennek igazolására a kutatási célok a következők:

- A magyar stratégiai szintű dokumentumok információvédelemre vonatkozó megállapításainak kimutatása, és az MH szakterületi feladatainak felső szintű megalapozottságának meghatározása. Az MH összhaderőnemi szempontból legfontosabb hatályos doktrínáinak információvédelmi szempontú elemzése, a hiányosságok kimutatása és javaslatok megfogalmazása.
- Az információvédelmi szakterületek általános jellemzése, a nemzeti és NATO, EU védelmi rendszabályok összehangoltságának megállapítása és a fontosabb gátló tényezők feltárása, az egységes szintű védelem érdekében általános biztonsági alapelvek kidolgozása.
- Az információvédelmi rendszabályok menedzseléséhez szükséges feladatok jellemzése, a felső szintű jogszabályok hatásainak kimutatása, és az MH információvédelmi szakterület szabályozásának összefogására vonatkozó javaslatok megfogalmazása.

Az értekezésben az „információbiztonság” kifejezés a nemzeti, NATO, EU (és egyéb nemzetközi szerződés hatálya alá tartozó) adatok *szükséges mértékű védettségét értem*.

A közfeladatot ellátó szervezetnél a szerző álláspontja szerint *minden szervezeti célú adatot (és információs rendszert) megfelelő szintű (fenyegetettséggel arányos) védelemben kell részesíteni*, így az *értekezésben az „információvédelem” a „titokvédelem” kategóriájánál szélesebb területet fed le. A* titokvédelem az MH jelenleg érvényben lévő meghatározása szerint *a minősített adatok védelmét jelenti*.

A jogszabályok rendje miatt hazánkban kialakult az a gyakorlat, hogy az „adatvédelem” a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló törvény (Avtv.) hatálya alá tartozó adatok védelmét jelenti, míg az egyéb adatok védelme ettől eltérő (más jogszabályok hatálya alá tartozó) tevékenység. A szerző álláspontja az adatok (és adatkezelő

képességek) biztonsága szempontjából nem mérvadó, hogy az adott szintű védelemre vonatkozó követelményt melyik jogszabály határozta meg, így *az „adatvédelem” (vagy „adatok védelme”) kifejezés az értekezésben széles körűen, az érzékeny adatok teljes körére, és nem csak a személyes, illetve a közérdekű adatok védelmére értendő*.

Külföldi források (beleértve a NATO, és EU szabályozását is) az „információ” kifejezést használják. Hazánkban az államtitokról és a szolgálati titokról szóló törvény (Ttv.), az Avtv. és más korszerűen fogalmazó jogszabályok „adat”-ot használnak, de a jogszabályok többségében a két kifejezés vegyes alkalmazása jellemző.

Az MH-nál *a személyes adatok védelmére vonatkozó adatvédelmi területtől való megkülönböztetés érdekében a MINŐSÍTETT a NEM MINŐSÍTETT (de védendő) adatok védelmére az „információvédelem” kifejezés terjedt el*.

Az értekezésnek nem célja *az információvédelmi szakterületen keletkezett információk más célú alkalmazhatóságának vizsgálata* (pl. információvédelmi feladatok felhasználása megtévesztési műveletekben).

Egy általános vizsgálat nem kötődhet egy, vagy több eszköz (rendszer) működési sajátosságaihoz, vagy az őket támogató irányzatokhoz, termékekhez vagy cégekhez, így *értekezés technológia és eszköz független.*

A gazdasági, pénzügyi, személyi lehetőségek gyakran keresztezik a szakmai érdekeket, de az értekezés *a szakmai szükségletekre helyezi a súlypontot.* A védelmi rendszabályok hatályba léptetése a vezetés felelőssége, ami a javaslatok, körülmények mérlegelése után *az értekezésben foglaltaktól eltérő döntéseket is eredményezhet.*

Az *értekezés megállapításai a szerző egyéni álláspontját tükrözik*.

ALKALMAZOTT MÓDSZEREK ÉS ERŐFORRÁSOK

A magyar hadtudomány még sok elméleti és gyakorlati kérdéssel adós az információs rendszerek területén, ami az információbiztonság területén is érzékelhető. Meglévő fogalmi rendszer, vagy felállított modell hiányában a téma bemutatására a MIÉRT kell védeni az adatokat, MILYEN TERÜLETEKEN kell a védelmet kialakítani, és a HOGYAN KELL SZERVEZNI és FENNTARTANI az információs rendszerek és adatok védelmét logikai sorrendben történik.

Az értekezés a nemzeti, NATO és EU információvédelemmel kapcsolatos jogszabályokra, szabályozókra, ajánlásokra, szabványokra támaszkodik. A szerző e mellett figyelemmel kísérte a témával kapcsolatos elkészített és folyamatban lévő értekezések, tudományos diákköri dolgozatok megállapításait, a hadtudományi és műszaki publikációkat, tudományos rendezvényeket és kiállításokat.

Az értekezés ezek mellett hasznosítja a szerző nemzeti (civil és katonai), valamint NATO szaktanfolyamain, továbbképzéseken és munkacsoportüléseken szerzett ismereteit.

A kidolgozás során ugyanígy hasznosultak a katonai szervezeteknél, háttérintézményeknél és iparbiztonsági cégeknél végzett konzultációk, valamint az információs rendszerek kialakítása, fenntartása, valamint a védelmi rendszabályok ellenőrzése, felülvizsgálata során szerzett gyakorlati tapasztalatok.

AZ ELSŐ FEJEZET ÖSSZEGZÉSE

A magyar Nemzeti Biztonsági Stratégia információbiztonsági részei *összhangban vannak a külföldi megfogalmazásokkal, de a feladatok, erőforrások teljes megalapozása a*

Stratégiában, felső szinten nem történik meg. Az információbiztonságra vonatkozó felső szintű feladatok megjelenítéshez, az alapelvek tisztázásához (beleértve a közigazgatási, védelmi szféra információvédelmi feladatainak támogatását) *nagymértékben hozzájárulna egy átfogó Nemzeti Védelmi Stratégia,* és a N*emzeti Információbiztonsági Stratégia kiadása,* illetve a stratégiák általános irányvonalának megfelelő *követelmények, eljárások jogszabályban, korszerű módon történő rögzítése. Ezek hiányában információvédelmi szempontból az MH feladatrendjét nem találom szakmailag alátámasztottnak.*

A Katonai Stratégia, illetve a fontosabb honvédelmi tárca szintű stratégiák információvédelmi szempontú támogatása érdekében a rögzítendő kulcskérdéseket a következő keretek között tartom célszerűnek megfogalmazni:

- A társadalom különböző területein az információs szolgáltatások biztosítása, valamint a nyilvánosan nem megismerhető adatok-, és az állami funkciók teljesítését szolgáló kritikus infrastruktúrák fenyegetéssel és sebezhetőséggel arányos mértékű védelme az állam alapvető érdeke.
- Az új szolgáltatások, a hálózatok egyre bonyolultabb összekapcsolásai, az internet által biztosított lehetőségek újabb és újabb kihívásokat, és fenyegetéseket jelentenek, mert a gyorsuló ütemű fejlődés *a szolgáltatások támadására, kihasználására alkalmas technológiákat, eljárásokat is támogatja*. A társadalom *egyre jobban függ az információs szolgáltatásoktól*, így a működéssel kapcsolatos problémák (zavarok, meghibásodások, az infrastruktúrák anyagi, technikai, humán és egyéb területű támogatási hiányosságai, a nem megfelelő technológia alkalmazása) halmozott nehézségeket okozhat.
- A nemzetbiztonság szempontjából érzékeny területeken kiemelten fontos a nemzeti függetlenség, a korszerű technikai lehetőségek kihasználása, a kritikus infrastruktúrák koordinált védelme, mely során a hangsúlyt az észlelésre és a megelőzésre kell helyezni.
- Az információs szolgáltatások, és a rájuk irányuló fenyegetések fejlődésével összhangban folyamatos célszerű fejleszteni a kockázatkezelés eszköztárát, valamint az adatkezelő műveletek rugalmasságát és visszaállíthatóságát.

A vizsgált magyar katonai doktrínákban az *információk védelmének szükségessége felismert, a korszerű megfogalmazások kezdetei azonosíthatók*. *Az információs műveletek elemeinek ellentmondásmentes definiálása, szabályainak összehangolása, tevékenységgé gyúrása, valamint a műveleti biztonságra, az információbiztonságra vonatkozó megfogalmazások finomítása soron lévő feladatnak tekinthető az* információs fölény - döntési fölény célkitűzése, a hatás alapú műveletek elvének alkalmazási igénye, a vezetést és működést támogató hálózat alapú hadviselés igénye szerint.

Az MH Összhaderőnemi Doktrína információbiztonsági szempontból jelentős korrekcióra szorul, a másik két említett doktrínába az információbiztonság pontosabb bedolgozása javasolt.

Az *információs műveleteken belül, az adatok védelmére irányuló szakterületi célokat, feladatokat és megoldásokat, a katonai sajátosságokat elemző, bemutató munkák területén hiányosság mutatkozik, a katonai szervezetek sikeres működéséhez szükséges információvédelem napjainkban nem kellően publikált.*

A MÁSODIK FEJEZET ÖSSZEGZÉSE

Az értekezés szakirodalmi áttekintésre támaszkodva megvilágítja, hogy a fizikai, személyi, dokumentum, vagy elektronikus információvédelem, alkotják az információbiztonság szakterületeit. A négy szakterület között *fontossági sorrendet, alá-fölérendeltségi viszonyt nem lehet meghatározni.*

A szerző megállapítja, hogy a megváltozott jogszabályi környezet miatt *az ITB 12. ajánlás szerinti biztonsági besorolást a közigazgatásban nem célszerű alkalmazni, hanem a minősítési szintekhez igazodó ötfokozatú biztonsági osztályozást kell kialakítani* (NEM MINŐSÍTETT, KORLÁTOZOTT TERJESZTÉSŰ, BIZALMAS, TITKOS és SZIGORÚAN TITKOS). A biztonsági osztályokon belül további bontás célszerű, azonban ennek során nem csak a rendelkezésre állást, hanem *az összes biztonsági célt figyelembe kell venni.* Az értékelési szempontokat nem egymástól függetlenül, hanem *komplexen kell alkalmazni, amelynek célszerű formája a „legalacsonyabb értékelési mutató érvényesítése" elv.*

A NEM MINŐSÍTETT biztonsági osztályba sorolt adatok esetében is minimum védelmi rendszabályokat kell meghatározni és meg kell szüntetni a „védelmet nem igényel" típusú megközelítést. Az ebbe a biztonsági osztályba tartozó, de magasabb védelmet igénylő adatok biztonságát specializált védelmi rendszabályokkal kell biztosítani.

A NATO, EU és a nemzeti adatkezelésre vonatkozó követelményekből kiderül, hogy *a felső szinten elméletileg összehangolt minősítési szintekhez nincsenek egyenértékű biztonsági követelmények rendelve, így nem garantált az adatok és adatkezelő képességek azonos védelmi szintje. A hálózat-alapú hadviselés elmélete szerinti civil-katonai, és nemzeti-szövetségi együttműködés a védelmi rendszabályok pontos összehangolását igényli, így mielőbb szükség van a szabályok harmonizálására. Az egységes nemzeti kritikus infrastruktúra védelme a gazdasági szféra, a hatósági szervek összehangolt felügyeleti és koordináló tevékenységét igényli*.

Az adatkezelő képességek kialakításához és fenntartásához nemzeti szinten ki kell alakítani a kockázatelemzéshez szükséges részletezett, az alkalmazók számára egységesen értelmezett feladatrendszert. *Nem engedhető meg, hogy a nemzeti kritikus infrastruktúrához tartozó rendszerek esetében egy üzemeltető, vagy alkalmazó szervezet más vizsgálati módszer, vagy eltérő mértékek alapján eltérő kockázatokat mutasson ki, és eltérő szintű védelmi rendszabályokat alkalmazzon.*

Az értekezésben bemutatott biztonsági alapelvek alkalmazása, időszakos felülvizsgálata, és továbbfejlesztése minősítési szinttől és rendszertől függetlenül támogatja a védelmi rendszabályok kialakítását. A korszerűség követelményének megfelelő védelmi rendszabályok érdekében *folyamatosan figyelemmel kell kísérni a szabványok, jogszabályok és ajánlások fejlődését, és a tapasztaltak szerint – a hadműveleti követelményekre alapozva – kell kialakítani a fejlesztési irányokat. Ez a tevékenység információvédelmi területen a jelenlegi kapacitások fejlesztését igényli.*

A HARMADIK FEJEZET ÖSSZEGZÉSE

Az értekezés bemutatja, hogy a kormányzati felelősségi rend, valamint a jogszabályokban meghatározott, az információvédelmi rendszabályok szabályozására vonatkozó követelmények széttagoltak.

Az MH elé kitűzött feladatok és a szövetségi vállalások teljesítése csak egységes szemléletű információvédelmi rendszer támogatásával képzelhető el, aminek kulcskérdése a

szakterületért való felelősség centralizálása. Széttagolt felelősségi rendben nem képzelhető el egységes szabályozás kialakítása és fenntartása.

A felelősségi rend bemutatása alapján megállapítható, hogy az MH teljes szervezeti hierarchiájában megoldandó kérdés az *információbiztonsággal kapcsolatos általános vezetői felelősség pontosabb megfogalmazása, a felelősség korszerű megosztása*. A katonai szervezeteknél a törzsfőnökre és/vagy parancsnok helyettesre ruházott biztonsági funkciót (jelenleg: titokvédelmi felügyelő és/vagy biztonsági megbízott) át kell alakítani általános vezetői felelősségé. Az információvédelmi tevékenység irányítására/vezetésére szakbeosztást (szervezeti feladatoktól függően biztonsági felügyeletet) célszerű kialakítani. A jelenleg csak korlátozott, a NATO, EU minősített adatok védelmére szűkített továbbképzési rendet át kell alakítani és a vezetők számára olyan ismeretanyagot kell összeállítani, ami támogatja a szakmai feladatok végrehajtását.

A szakirányításhoz szükséges felső szintű feladatok megfogalmazása kapcsán a szerző megállapítja, hogy hatáskörre, létszámra, szakismeretre, vagy szervezeti kapcsolatokra vonatkozó pontos igények e feladatok rögzítése nélkül nem állapíthatók meg (pl. a közfeladatok ellátásának felülvizsgálatára vonatkozó tevékenység is csak ez után az alapvető lépés után kezdhető).

A szervezeti méretek, struktúra és a vezetési folyamatok bonyolultsága miatt az MH-nál információvédelmi területen a hagyományosan elképzelt „szabályzat” helyett a *szabályozó rendszer kialakítása* a járható út.

A szabályozási rend felső szintű szabályozói közé be kell iktatni a biztonságpolitikát olyan tartalommal, hogy az MH információs folyamataiban résztvevők megkaphassák belőle a szükséges szakmai támogatást.

Az értekezésben bemutatott szabályozási rend elemei lényegesen rugalmasabban kezelhetők, mint a jelenleg tapasztalható, központi szabályzat alapú rendszer. Ebben a rendben a szabályzat funkciója szükségszerűen átalakul, és csak technológia és rendszer független követelményeket, rendszabályokat tartalmazza a rendszer-specifikus védelmi rendszabályok kialakításának támogatása érdekében.

A helyi szabályozók területén a *széttagolt szabályozási rendet integrálni kell* (ez akkor is célszerű, ha a jogszabályok ezt az egységesítést a nem követelik meg). A hálózatok integrálódásával a helyi és a rendszerfüggő szabályozók területén *a helyi (szervezethez köthető) szabályozó szerepének csökkenése és a nagy kiterjedésű rendszerekre vonatkozó központi szabályozó szerepeinek erősödése várható.*

Az információbiztonság szakterületei, valamint a szabályozási és ellenőrzési rend átfogó jellegű áttekintése után megállapítható, hogy a védelmi rendszabályoknak nincs kapcsolatuk a részletes adattartalommal, csak az adatok minősítésével és kezelési jelzésével. *Az adatvédelmi felelősnek a jogszabályok szerinti adatvédelmi követelményeket be kell dolgozni az információ rendszerek biztonsági követelményei közé, így megoldódik az eddig függetlenül működő adatvédelmi funkció és az információvédelmi szakterület együttműködése.*

ÖSSZEGZETT KÖVETKEZTETÉSEK

Az első fejezet megállapítja a Nemzeti Biztonsági Stratégia információvédelmi szempontú korszerűségét, és azt, hogy más nemzetek hasonló dokumentumai lényegesebben szélesebb körben körvonalazzák a feladatokat. *A stratégiai szintű megfogalmazások hiányában (pl. katonai stratégia, információvédelmi stratégia), illetve az MH feladatrendszere nem tekinthető szakmailag felső szinten megalapozottnak.*

Az MH fontosabb doktrínáinak áttekintése alapján megállapítható az információvédelmi szakterület fontosságának felismerése, de ezen túlmenően *korrekciókra van szükség*, melynek a szerző meghatározta a fontosabb paramétereit.

A védelmi rendszabályok vizsgálatán keresztül a szerző bemutatta, hogy *a stratégiai szinten hiányzó egységes irányelvek megmutatkoznak a jogszabályok összehangolatlanságán. Az értekezés bemutatja, hogy nemzeti szinten (pl. közigazgatási szervezetek között) illetve a nemzeti és NATO, EU szervezetek közötti kapcsolattartás szintjén az együttműködést nem támogatja egységesen szabályozott védelmi rendszer.*

Az értekezés a kezelt adatok minősítési szintjeire támaszkodó besorolásnak megfelelően *bemutatja az elektronikus adatkezelő rendszereknél a védelmi rendszabályok egymásra épülésének logikáját*. A várható trendek alapján megjelöli azokat az információvédelmi feladatokat, amelyek az MH-nál hangsúlyt kapnak, így kiemelt támogatást és menedzselést igényelnek.

Kormányzati követelmény hiányában a védelem kialakításának és fenntartásának vezérlése érdekében a szerző *kidolgozta az összes biztonsági osztályra vonatkozó (minősítési szinttől és kezelési utasítástól független) biztonsági alapelveket.*

A HM szintű jogszabályok és az állami irányítás egyéb jogi eszközei kategóriába tartozó egyéb MH szabályozók áttekintésével információvédelmi területen megállapítható a szabályozási hierarchia, illetve az egységes védelmi szemléletet megalapozó alapdokumentum hiánya, mely helyzet változtatása érdekében az értekezés javaslatot tesz a szabályozási rend felső szintű dokumentumával kapcsolatban, és meghatározza a támogató szabályozókkal kapcsolatos alapvető követelményeket.

TUDOMÁNYOS EREDMÉNYEK

1) *Az MK Katonai Stratégia és az MH felső szintű dokumentumaiban megjelenítendő, információbiztonságra vonatkozó általános megállapítások kereteinek meghatározása. A legfontosabbnak tekinthető katonai doktrínák információbiztonsággal kapcsolatos megállapításai hiányosságainak feltárása, és és javaslatokat tétele azok kiküszöbölésére.*
2) Az információvédelmi szakterületek védelmi rendszabályainak rendszerezése és a *nemzeti szabályozásban tapasztalható, nemzeti és szövetségi szintű hálózat-alapú műveletek támogatását gátló legsúlyosabb hiányosságok feltárása*. Az MH adatkezelő rendszereinek egységes szintű védelme érdekében *a rendszer, és minősítési szinttől független biztonsági alapelvek meghatározása*.
3) Az MH információbiztonságot érintő szabályozói összehangolatlanságának megállapítása és a hiányosság megszüntetése *érdekében javaslattétel az MH Információ Biztonságpolitika tartalmára, a végrehajtást támogató szabályozási rendre, az* információvédelem szakirányítási feladatainak és a szabályozási rend felülvizsgálatára vonatkozó követelmények megfogalmazására.

ALKALMAZHATÓSÁG ÉS AJÁNLÁSOK

Az értekezés harmadik fejezetében azonosított MH Információ Biztonságpolitikára vonatkozó követelmények kidolgozása és szakmai köröztetése után javasolt a politika HM utasítás formájában történő kiadása.

Az értekezés második fejezetében azonosított biztonsági alapelveket megjelenítése célszerű az MH Információ Biztonságpolitikában. Az MH Informatikai Stratégia felülvizsgálatának esedékességekor, illetve a NATO elektronikus információvédelmi feladatok áttekintésekor az MH álláspont kialakításakor és meghatározott időszakonként javasolt ezen alapelvek felülvizsgálata.

A szakirányításért felelős szervezeti elemek felé az MH szintű szabályozórendszer felülvizsgálatakor célszerű a felső szintű szabályozók és helyi/rendszer-specifikus szabályozókra vonatkozó ajánlások figyelembe vétele.

Az értekezés második fejezetében az MH Öszhaderőnemi Doktrína információvédelemre vonatkozó részeinek megjelenítése célszerű. Az MK Katonai Stratégiában az információvédelmi részek kialakításához javasolt a bemutatott keretrendszer alkalmazása.

Az információbiztonság szakterületi kérdéseit kutatók számára segítségként használható a második fejezetben a kutatás-fejlesztésre vonatkozó elgondolások, valamint az első fejezetben, a NATO hálózat alapú képességekkel kapcsolatos általános követelményeknek tekinthető részek bemutatása.

Ajánlott az értekezés részeinek e források által jelzett irányok mentén történő továbbfejlesztését, a megvalósíthatóság rendszer-specifikus vizsgálatát, figyelembe véve a központosított biztonsági megoldásokra vonatkozó igényeket.

Az értekezés a szerző javaslata alapján ajánlott irodalomként alkalmazható az MH információvédelmi szakmai tanfolyamain, továbbképzésein.

A TÉMÁVAL KAPCSOLATOS PUBLIKÁCIÓK JEGYZÉKE

1) A vezetés ellenőrzési funkciójának érvényesüléséről; Hadtudomány ISSN 1215-4121, 1999. 3-4. szám p. 94-106.
2) The difficulties of scope of control duties; Hadtudományi Tájékoztató ISSN1419-7758, 2000/4 p. 93-106.
3) A vezetés korszerűsítésének technikai feladatai; Hadtudomány ISSN 1215-4121, 2000. 1. szám p. 63-71.
4) A korszerű rádiókkal kapcsolatos információvédelmi feladatok és lehetőségek, Kard és toll (válogatás a hadtudomány doktoranduszainak tanulmányaiból) Budapest, 2000 ISBN 963 7037 40 3, p. 73-83.
5) A fizikai biztonság, mint az adatbiztonság pillére; Katonai Logisztika, 8. évfolyam, 2000/3. szám p. 154-165.
6) A vezetéshez szükséges korszerű információvédelmi feladatrendszer tanulmányozása és az arra történő áttérés fontosabb feladatai; Nemzetvédelmi Egyetemi Doktorandum 2001, ISSN1588-2233, p. 76-86.
7) A híradó és az informatikai rendszer korszerűsítése és védelme; Hadtudomány 2001/1 p. 92-98.
8) Vezetési és logisztikai műveletek, folyamatok az információvédelmi rendszer hátterében; Katonai Logisztika, 2000/4 p. 23-33.

9) A híradó és informatikai rendszer korszerű szolgáltatásainak hatása és az új információvédelmi feladatok; Nemzetvédelmi Egyetemi Közlemények, 2001. 5. évfolyam 1. szám, ISSN 1417-7323, p. 229-239.
10) Úton a korszerű híradó és informatikai rendszer felé; Új Honvédségi Szemle ISSN 1585-4167, 2001/4 p. 9-23.
11) Biztonságpolitika és információvédelem, Hadtudomány 2001/3 p. 71-76.
12) Responsibility for a secure CIS, 2001. Konferencia kiadvány ISBN 963 008819 3, p. 113-117. *i*
13) Az információvédelem újszerű megközelítése, Kommunikáció 2001. kiadvány, ISBN 963 008819 3, p. 193- 198.
14) Az információvédelem rendszerszintű feladatai, Nemzetvédelmi Egyetemi Közlemények, 2001. 5. évfolyam 4. szám, p. 111- 120.
15) A minősített információk és adatok védelme; Hadtudomány 2002/1 p. 64-70.
16) A korszerű híradó és informatikai rendszer védelmi szempontú vizsgálatának egyes kérdései Nemzetvédelmi Egyetemi Közlemények, 2002, 6. évfolyam 2. szám p. 163-170.
17) Kassai Károly – Magyar Sándor: A zártcélú hálózat felügyeletének biztonsági kérdései Új Honvédségi Szemle 2002/11 p. 88-95.
18) Az elektronikus információk védelmének területei, Hadtudomány 2002/3 p. 95-102.
19) Areas and activities for the information (and information system) security; Kommunikáció 2002. kiadvány, ISBN 963 86229 2 X, p. 75-80.
20) Az elektronikus információvédelem néhány szervezeti kérdése Kard és toll 2002, ISBN 963 7037 52 7, p. 128-133.
21) Az információk és információs rendszerek fenyegetéseinek stratégiai szintű megfogalmazásai, Új Honvédségi Szemle 2003/3 p. 28-36.
22) Az információs rendszerek védelméről, Hadtudomány 2003/1 p.119-126.
23) Az információk, a híradó és informatikai rendszer eszközeinek védelme, Hadtudomány 2003/3-4 p. 61-68.
24) Az információk, valamint a híradó és informatikai rendszer védelmének szabályozása, Kommunikáció 2003. kiadvány, ISBN 963 86229 62 p. 133-140.
25) Kassai Károly – Magyar Sándor: A híradó és informatikai rendszer csomópontjainak védelmi kérdései; Felderítő Szemle III. évfolyam 1. szám 2004. március ISSN 1588-242X p. 128-136.
26) Az elektronikus adatkezelő rendszerek védelmének fontosabb tendenciái (kiemelten a szabályozási területtel kapcsolatos feladatok); Kommunikáció 2005, ISBN 963 7060 11 1. p. 161-170.
27) Az elektronikus információvédelmi rendszabályok megalapozásának fontosabb kérdései, Kommunikáció 2006. kiadvány, ISBN 963 7060 18 2 p. 131-143.
28) Kassai Károly – Kiss József: Információ- és dokumentumvédelem; „A honvédelem négy éve 2002-2006”című kiadvány, HM Zrínyi Kht. 2006. ISBN 963 327408 7, p. 80-81.
29) Az elektronikus adatkezeléssel kapcsolatos kockázatok kezelésének egyes kérdései, Kommunikáció 2007. kiadvány, ISBN 978-963-7060-31-1, p. 77-82.