HADMÉRNÖK

IX. Évfolyam 4. szám - 2014. december

Prisznyák Szabolcs
prisznyak.szabolcs@bv.gov.hu

A BVOP EGYES HELYISÉGEINEK INFORMATIKAI KOCKÁZATELEMZÉSE

Absztrakt

A cikk bemutatja a Büntetés-végrehajtás Országos Parancsnoksága helyiségeinek informatikai fenyegetettség szerinti csoportokba sorolását. Ezt követően ismerteti az egyes csoportokra vonatkozó kockázatelemzést. Az elemzés az ISO/IEC 27005 (2008) szabvány előírásai szerint készült. A cikk végén összegzi a tapasztalatokat, továbbá ismerteti a szükséges fejlesztési lehetőségeket.

The article presents the grouping by IT threat of several premises of headquarters of Hungarian prison system. After then the author shows the risk analysis of several groups by ISO/IEC 27005 (2008) standard. The author concludes the article by summarising the experience gained and outlining the prospects for further development.

Kulcsszavak: *büntetés-végrehajtás, információ-technológia, ISO/IEC 27005 (2008) szabvány, kockázatelemzés ~ prison service, information technology, ISO/IEC 27005 (2008) standard, risk analysis*

BEVEZETÉS

Az elmúlt években történt a büntetés-végrehajtási szervezet eddigi legnagyobb volumenű informatikai fejlesztése a „Felelősen, felkészülten a büntetés-végrehajtásban” elnevezésű, EKOP-1.1.6-09-2009-0001 azonosítószámú, az Európai Unió támogatásával megvalósult projekt[i].

A megvalósított fejlesztés – és a változásokhoz illeszkedő rendszerlogikai módosítások - eredményeként összességében jelentős rendszertechnológiai, logikai változások következtek be[ii]. Korábban ezt a fejlesztést részleteiben ismertettem a „Haditechnika – Kommunikáció 2012” nemzetközi szakmai tudományos konferencián[iii] és a „Kriminalexpo 2012” nemzetközi biztonsági és informatikai, bűnmegelőzési, bűnüldözési, igazságszolgáltatási konferencián[iv]. Az erősen centralizálttá vált rendszer esetében kulcsfontosságú, hogy a Büntetés-végrehajtás Országos Parancsnoksága (BVOP) informatikai központja nagy rendelkezésre állással szolgálja ki a teljes szervezet információigényét. A rendelkezésre állás biztosításához szükséges felmérni a BVOP-n meglévő kockázatokat. A felmérés első lépéseként az egyes helyiségeket kockázati csoportokba kell sorolni az informatikai rendszer működése szempontjából megvalósított funkcióik szerint. Ezt követően történhet meg a funkciók szerint csoportosított helyiségek kockázatelemzése az IEC/ISO 27005 (2008) szabvány[v] szerint. A helyiségek csoportokba sorolását követően a kockázatelemzést két részre bontottam. Ennek oka, hogy megállapítottam, hogy a központi gépterem olyan kiemelt fontosságú funkciót tölt be az informatikai rendszer működése, rendelkezésre állása szempontjából, hogy önálló cikkben[vi] ismertettem a lehetséges kockázatokat, valamint a bekövetkezés valószínűségének, illetve az esetlegesen keletkezett károk elhárításához szükséges fejlesztéseket. Jelen publikációban a kommunikációs szempontból szintén kulcsfontosságú távbeszélő központot, valamint a további négy csoportba sorolt helyiségeket elemzem. Összképet adok a nagy rendelkezésre állást biztosító működés feltételeinek meglétéről, illetve ismertetem a szükséges fejlesztéseket.

A cikk elkészítéséhez feldolgoztam a témakörrel kapcsolatos tudományos publikációkat, valamint a kapcsolódó jogszabályokat. Az objektív kockázatelemzéshez figyelembe vettem Kerti András közleményében foglaltakat[vii]. Tanulmányoztam a jelzett fejlesztés során keletkezett műszaki dokumentációkat. A több éves projektben, mint a BVOP informatikai fejlesztési osztályvezetője vettem részt. Ennek következtében munkám során a legfontosabb támaszomat a megvalósítás és az üzemeltetés során szerzett személyes szakmai tapasztalatok jelentették.

A BÜNTETÉS-VÉGREHAJTÁS SZERVEZETI FELÉPÍTÉSE

A büntetés-végrehajtás állami, fegyveres, rendvédelmi szerv, amely külön jogszabályban meghatározott szabadságelvonással járó, büntetéseket, intézkedéseket, valamint büntetőeljárási kényszerintézkedéseket, továbbá elzárást hajt végre [viii].

A büntetés-végrehajtási szervezet kormányzati irányítását a Belügyminisztérium végzi. A büntetés-végrehajtási szervezet központi vezető szerve a Büntetés-végrehajtás Országos Parancsnoksága, amely főosztályai révén a büntetés-végrehajtási intézetekben folyó szakmai munka felügyeletét, ellenőrzését végzi. A büntetés-végrehajtási intézetek ellátják a büntetések és intézkedések végrehajtásával kapcsolatos feladatokat. A büntetés-végrehajtás a legtöbb magyarországi közigazgatási és rendvédelmi szervezettől eltérően nem három, hanem kétszintű szervezet. A központi (országos) szervezet alárendeltségébe közvetlenül a területi jogállású szervezetek tartoznak. Nem jelennek meg a helyi szervezeti egységek, ellentétben pl. a rendőrséggel vagy a katasztrófavédelmi szervezettel.

Magyarországon 28 önálló jogállású büntetés-végrehajtási intézet, 5 – egészségügyi és oktatási – intézmény, valamint 11 gazdasági társaság működik. Az informatikai szakterület kompetenciája a gazdasági társaságokra nem terjed ki, azok a büntetés-végrehajtási szervezet informatikai rendszerétől független önálló, elszigetelt rendszereket alakítottak ki.

A BVOP HELYISÉGEINEK BESOROLÁSA FUNKCIÓK ALAPJÁN

A büntetés-végrehajtási szervezet informatikai rendszere jelentősen megváltozott az EKOP-1.1.6 informatikai fejlesztési projekt eredményeként. A megújulás kulcspontja, hogy a korábbi decentralizált rendszert egy erősen központosított megoldás váltotta fel. Az új homogén rendszer, azonban üzemeltetési szempontból kulcsfontosságúvá vált a BVOP informatikai központjának elérése. A megváltozott körülmények közti üzembiztos működéshez szükséges a BVOP kockázatelemzése az informatikai rendszer vonatkozásában. A kockázatelemzés során legcélszerűbb az IEC/ISO 27005 (2008) szabvány előírásait alkalmazni. A kockázatelemzés megkezdése előtt a BVOP helyiségeit az informatikai üzemeltetés szempontjából betöltött funkcióik szerinti csoportokba kell sorolni, hiszen, az egyes helyiségekre funkcióik szerint értelmezhetők a kockázatok. A helyiségek csoportokba sorolása az alábbi táblázatban látható.

BVOP helyiségeinek kategóriákba sorolása
az informatikai rendszer működésének szempontjából betöltött funkció szerint

funkció meghatározása	helyiség	megjegyzés
az informatikai rendszer működése szempontjából kulcsfontosságú helyiség	központi gépterem	földszinti elhelyezkedés
	telefonközpont	-
kulcsfontosságú támogató berendezések	szünetmentes tápegység helyisége	pince szinten elhelyezve
	aggregátor helyiség	pince szinten elhelyezve
	klímaberendezés (kültéri egység)	kültéri légudvarban elhelyezve
kulcsfontosságú helyi és távoli kommunikációt biztosító helyiségek	rack szekrény (vidéki kapcsolat)	-
	rack szekrények (helyi hálózat)	az épületben több helyen
kulcsfontosságú szolgálati helyiségek (24órás szolgálat)	ügyeletes tiszti helyiség	
	kapuügyelet	földszinti elhelyezkedés
általános célú szolgálati helyiségek	valamennyi iroda és egyéb célú helyiség	-

1. ábra. BVOP helyiségeinek kategóriákba sorolása

A BVOP Budapesten található az V. kerület Steindl Imre utca 8. szám alatt. Az épülethez tartozik a szomszédos Steindl Imre utca 10. szám alatt található épület is. Az épületek teljes beépítésű területen találhatóak, így teljesen egymáshoz épültek. Mindkét épületben találhatók irodák, illetve az informatikai működést befolyásoló helyiségek

A legfontosabb helyiség a központi gépterem, amelyben az informatikai működés központja található, kiesése a büntetés-végrehajtási szervezet informatikai működését rövid időn belül ellehetetleníti, mint fent említettem ennek a helyiségnek a kockázatelemzése korábban megtörtént, így jelen publikációnak nem része. Szintén fontos a telefonközpont, amely a kommunikáció alapját jelenti.

A fontossági sorrendben az üzemeltetés alapjait képező rendszerek után azok a gépek, berendezések, megoldások következnek, amelyek az üzemeltetést biztosítják valamilyen rendkívüli helyzetben.

Egy informatikai rendszerben – különösen egy erősen centralizált környezetben – kulcsfontosságú a hálózatok működése, hiszen nélkülük nem érhetők el a központi adattárak, programok, ezért a hálózati aktív eszközök (útválasztók, kapcsolók) külön egységet képeznek.

A szervezet dolgozói által használt helyiségek – irodák és egyéb célú helyiségek – közül a szervezet rendeltetésszerű működése szempontjából kiemeltek a 24 órás ügyeleti szolgálati tevékenységet folytató állomány elhelyezését, munkavégzését biztosító helyiségek.

A BVOP KOCKÁZATELEMZÉSE

A kockázatok elemzését az ISO/IEC 27005 (2008) szabvány C függelékében foglalt „Leggyakoribb fenyegetések" alapján végzem. Az elemzés rendszer szintű kockázatelemzés, bizonyos esetekben – amennyiben az szükséges – részletes kockázatelemzésre is sor kerülhet. Az egyes fenyegetések bekövetkezésének valószínűségét 1-5 skálán sorolom be, ahol a bekövetkezés legkisebb valószínűsége 1. Ezt követően ismertetem a környezeti tényezőket és/vagy a tett intézkedéseket. Amennyiben szükséges ismertetem a kockázatok valószínűségének és/vagy hatásának csökkentéséhez esetlegesen szükséges további intézkedéseket.

TELEFONKÖZPONT

Fizikai károk

A fizikai károk közül a tűz okozta kár a legnagyobb kockázatú – a további felsorolt károk bekövetkezése nem releváns – bekövetkezésének valószínűsége 3.

További szükséges intézkedések: tűzvédelemi rendszer kialakítása, úgy, mint tűzbiztos bejárati ajtó, automatikus oltóberendezés.

Természeti események okozta károk

Nem releváns.

Kulcsfontosságú szolgáltatás kiesése okozta károk

A jelzett elemek közül gyakorlatilag csak az áramkimaradásnak van kockázata. A berendezés szünetmentes tápellátással biztosított, de a biztosító rendszer több esetben rendellenesen működik. A bekövetkezés valószínűsége 2.

További szükséges intézkedések: áramellátás felülvizsgálata a helyiségben.

Sugárzás miatti zavar

Nem releváns.

Információ kompromittálódás

- *Kompromittáló kisugárzott jelek elfogása:* a bekövetkezés valószínűsége: 1; A BVOP nem alkalmaz vezeték nélküli eszközöket. A gépterem az épület belső részén helyezkedik el. Az ingatlan területére ellenőrzötten, dokumentáltan történik a beléptetés. A múlt századi építészeti megoldások következtében a 80-100 cm-es falvastagság is csökkenti a jelfelderítés valószínűségét. További intézkedés nem szükséges.

- *Távoli kémkedés okozta kár*: a bekövetkezés valószínűsége: 1; A BVOP a kormányzati hálózat része, amelyet a NISZ Zrt. üzemeltet. A hálózat a távoli behatolás ellen több szintű logikai és fizikai védelemmel ellátott. További intézkedés nem szükséges.
- *Lehallgatás okozta kár:* a bekövetkezés valószínűsége: 1; A lehallgatáshoz a hálózatra fizikailag kell rácsatlakozni. Az épület fent ismertetett védelme jelentősen csökkenti a kockázatot. További intézkedés nem szükséges.
- *Média (adathordozó) vagy dokumentumok ellopása:* a bekövetkezés valószínűsége: 2; A kockázatot elsősorban a saját dolgozók jelentik. Az épületbe, az informatikai helyiségekbe a belépés korlátozott. Az adathordozók biztonságosan tároltak (lemezszekrény, páncélszekrény). A dolgozók tájékoztatása, oktatása megtörtént. További szükséges intézkedések: Az informatikai biztonsági oktatások számának növelése, rendszeressé tétele, a megszerzett ismeretek ellenőrzése. A dolgozókban a felelősségtudat kialakítása.
- *Berendezések ellopása: a bekövetkezés valószínűsége: 2;* A tett és a szükséges intézkedések azonosak a fenti pontban megfogalmazottakkal.
- *Kidobott, újrafelhasznált média (adathordozó) helyreállítása:* a bekövetkezés valószínűsége: kevesebb, mint 1; Minden használatból kivont adathordozó esetében adat helyreállítást lehetetlenné tevő roncsolásra kerül sor. További intézkedés nem szükséges.
- *Árulás, információk közzététele:* a bekövetkezés valószínűsége: 2; A dolgozók felkészítése, oktatása megtörtént. További szükséges intézkedés: további rendszeres oktatások a dolgozók részére, a tudatos magatartás kialakítása.
- *Megbízhatatlan forrásból származó adat:* a bekövetkezés valószínűsége: 2; A rendszerbe kerülő adatok ellenőrzöttek, hiteles forrásból származnak. Nem megfelelő adat csak tévedésből vagy szándékosan kerülhet a rendszerbe. További szükséges intézkedések: tudatos magatartás kialakítása oktatással.
- *Hardverek működésének befolyásolása*: a bekövetkezés valószínűsége: 2; A központi gépteremben található hardverekhez csak a kijelölt állomány férhet hozzá. További szükséges intézkedések: tudatos magatartás kialakítása oktatással.
- *Szoftverek működésének befolyásolása:* a bekövetkezés valószínűsége: 2; A központi rendszeren futó szoftverek logikailag és fizikailag is védettek. A szoftverekhez csak a kijelölt állomány férhet hozzá. A BVOP megfelelő vírusvédelemi rendszerrel rendelkezik, a vírusinformációs állomány frissítése rendszeres és automatikus. Minden szoftverelem csak előzetes tesztelés után kerül telepítésre. Problémát jelenthetnek a nem a BVOP állománya által felügyelt szoftverek. További szükséges intézkedések: tudatos magatartás kialakítása oktatással. A vírusvédelmi rendszer rendszeres ellenőrzése. A külső – szoftvereket telepítő, üzemeltető – partnerek esetében a megfelelő együttműködés kialakítása.
- *Pozíció (hely) kinyomozása*: a bekövetkezés valószínűsége: 1; A BVOP elhelyezkedése ismert, nyilvános információ, de ebből nem következik egyenesen a központi gépterem elhelyezkedése. A kockázatot csökkenti az épület védelme, a ki- és beléptetés szabályrendszere, annak betartása. További intézkedés nem szükséges.

Technikai meghibásodás

A technikai meghibásodásoknál fontos körülmény, hogy a telefonközpontot a NISZ Zrt. üzemelteti, így a kockázatok – részben – náluk jelentkeznek.

- *Eszközök, berendezések meghibásodása*: a bekövetkezés valószínűsége: 2; Az informatikai eszközök, berendezések használatuk során meghibásodhatnak, ennek kezelésére a központi rendszer elemei szinte valamennyi esetben megfelelő redundanciával kerültek kialakításra, továbbá tartalék eszközök állnak rendelkezésre.

Szükséges intézkedés: redundancia kialakítása valamennyi rendszer esetén, a rendelkezésre állás további növelése.

- *Üzemzavar, hibás működés:* a bekövetkezés valószínűsége: 2; A fenti pontban megfogalmazottakkal azonos intézkedések történtek és szükségesek.
- *Információs rendszer telítettsége:* a bekövetkezés valószínűsége: 1; A rendszer folyamatosan ellenőrzött, mind automatikusan, mind humán erőforrás bevonásával. Szükség esetén a rendszerek automatikus megelőző figyelmeztetést küldenek. További intézkedés nem szükséges.
- *Szoftverek hibás működése:* a bekövetkezés valószínűsége: 2; A központi rendszeren futó szoftverek logikailag és fizikailag is védettek. A BVOP megfelelő vírusvédelemi rendszerrel rendelkezik, a vírusinformációs állomány frissítése rendszeres és automatikus. Minden szoftverelem csak előzetes tesztelés után kerül telepítésre. További szükséges intézkedések: A vírusvédelmi rendszer rendszeres ellenőrzése.
- *Az információs rendszer helyreállíthatóságának megsértése:* a bekövetkezés valószínűsége: 1; Az adatállományokról mentéssel rendelkezünk. A mentések megfelelő helyen őrzöttek. A távoli telephelyre történő tükrözött adatállomány is rendelkezésre áll. Szükséges intézkedések: a távoli mentések rendszeres felülvizsgálata.

Illetéktelen cselekedetek

- *Illetéktelen eszközhasználat*: a bekövetkezés valószínűsége: 2; Az eszközök be- és kivitele az épületbe történő be- és kiléptetés során ellenőrzésre kerülnek. A gépterembe történő belépés korlátozott. Az eszközök hálózatra csatlakoztatása sem lehetséges a fizikai címre (MAC address) történő szűrés alapján. Egyes esetekben kockázatot jelenthet az USB alapú eszközök használata. Szükséges intézkedések: az USB alapú eszközök egyedi azonosító alapján személyekhez rendelt módon történő központi felügyeletének kialakítása.
- *Szoftverek illegális másolása*: nem releváns esemény, bekövetkezés valószínűsége: 1;
- *Hamis szoftverek használata*: nem releváns esemény, bekövetkezés valószínűsége: 1
- *Adatok elrontása (meghamisítása):* a bekövetkezés valószínűsége: 2; A rendszerbe kerülő adatok ellenőrzöttek, hiteles forrásból származnak. Nem megfelelő adat csak tévedésből vagy szándékosan kerülhet a rendszerbe. További szükséges intézkedések: tudatos magatartás kialakítása oktatással.
- *Illegális adathasználat (adatfeldolgozás)*: fentivel azonos.

Funkció kompromittálódása

- *Használat közbeni hiba*: a bekövetkezés valószínűsége: 3; A központi rendszer elemei szinte valamennyi funkciót tekintve redundánsak, illetve szükség esetére tartalék eszköz, alkatrész áll rendelkezésre. További szükséges intézkedések: újabb redundáns megoldások kialakításának folyamatos vizsgálata.
- *Jogokkal való visszaélés*: a bekövetkezés valószínűsége: 2; A jogosultsági rendszer úgy került kialakításra, hogy minden felhasználó csak a munkavégzéséhez szükséges jogosultsággal rendelkezik. További szükséges intézkedések: tudatos, felelősségteljes magatartás kialakítása oktatással, ellenőrzéssel.
- *Jogokról való megfeledkezés*: a bekövetkezés valószínűsége: 2; Fentivel azonos kockázat és intézkedések.
- *Tevékenység megtagadás*: a bekövetkezés valószínűsége: 1; A szervezet jellegéből adódóan nem releváns kockázat. További intézkedés nem szükséges.

– *Személyes hozzáférés megakadályozása*: a bekövetkezés valószínűsége: 1; Több személy is rendelkezik rendszerfelügyeletet és rendszerkonfigurációt biztosító jogosultságokkal. A rendszerek jól dokumentáltak. Amennyiben fizikai hozzáférési probléma történik annak kijavításáig távoli adminisztrációval biztosítható a rendelkezésre állás. További intézkedés nem szükséges.

KULCSFONTOSSÁGÚ TÁMOGATÓ BERENDEZÉSEK

Ezen helyiségek esetében kockázatot jelentenek a fizikai kár jellegű fenyegetések, azonban ezek bekövetkezésének valószínűsége alacsony. Valamennyi berendezés az iparági szabványoknak, előírásoknak megfelelően védett. Az aggregátor helyiségében megfelelő füstgázelvezetés, tűzbiztos bejárati ajtó és automatikus oltóberendezés található. A klímaberendezés esetében a fagyás és a víz (csapadék) okozta károk jelenthetnek minimális kockázatot, de ezek ellen a berendezés elsősorban konstrukciójából következően, másrészt szakszerű telepítéséből és rendszeres időközönként történő ellenőrzéséből, karbantartásából következően védett.

KULCSFONTOSSÁGÚ HELYI ÉS TÁVOLI KOMMUNIKÁCIÓT BIZTOSÍTÓ HELYISÉGEK

A hálózati eszközök (switchek, routerek) esetében kockázatként jelentkezik az áramkimaradás során – illetve azt követően az áramellátás helyreállása esetén – bekövetkező működési problémák, mivel a rack szekrények nem rendelkeznek szünetmentes tápellátással. A bekövetkezés valószínűsége 2.

További szükséges intézkedések: szünetmentes áramellátás biztosítása a hálózati elosztó szekrényekhez.

További kockázatot jelenthet az illetéktelen eszközhasználat, hiszen több rack szekrény a folyosón – nem zárt területen – található. A bekövetkezés valószínűsége 2.

További szükséges intézkedések: a rack szekrények zárjainak megerősítése, a hálózati eszközökhöz a fizikai hozzáférés korlátozása, jelző, érzékelő berendezések alkalmazása, a szekrények sértetlenségének rendszeres ellenőrzése.

KULCSFONTOSSÁGÚ SZOLGÁLATI HELYISÉGEK (24ÓRÁS SZOLGÁLAT)

Ezekben a helyiségekben 24 órás folyamatos munkavégzés zajlik, a helyiségek szünetmentes tápellátással biztosítottak, a kockázatok nem relevánsak.

ÁLTALÁNOS CÉLÚ SZOLGÁLATI HELYISÉGEK

A kockázatok nem relevánsak, hiszen a rendszer kialakításának köszönhetően adattárolás csak központilag történik, a felhasználói jogosultságok erősen korlátozottak – kizárólag a szolgálati feladatok elvégzését biztosítják – így szinte valamennyi kockázat a központi gépteremre vonatkozóan jelentkezik.

ÖSSZEGZÉS

Az EKOP-1.1.6-09-2009-0001 informatikai fejlesztési projekt a büntetés-végrehajtás történetének eddigi legnagyobb informatikai fejlesztése. Napjainkban szinte valamennyi munkafolyamat informatikai eszközökkel támogatott, így a változás a szervezet egészét érinti. A rendszertechnológiai változások nem csak a az informatikai rendszer működésének, elérésnek feltételeit változtatták meg, hanem az egyes kockázatok is máshol, más formában jelentkeztek.

A centralizált informatikai infrastruktúrában kulcsfontosságú a központi rendszer rendelkezésre állása. A rendelkezésre állás biztosításához, növeléséhez elengedhetetlen a teljes rendszer, illetve annak egyes elemeinek a felülvizsgálata. Az egyes kockázatok elemzéséhez, a kockázatok bekövetkezési valószínűségének csökkentéséhez, illetve a bekövetkezett események hatásának csökkentéséhez megtett és a jövőben szükséges intézkedések meghatározásához a nemzetközileg elfogadott ISO/IEC 27005 (2008) szabványt választottam.

A kockázatelemzés alapjául elvégeztem a helyiségek – informatikai működés szerinti – csoportosítását. Majd az egyes csoportokba sorolt helyiségeket azonos kockázatúnak tekintve végeztem el az elemzést. Végeredményül megállapítom, hogy a centralizált rendszereknél – a korábbi decentralizált rendszerekkel összehasonlítva - a központi rendszerelemektől távolodva a kockázat egyre csökken, ellenben az infrastruktúra centrumában ezzel fordított arányban nő.

Az alkalmazott – nemzetközi szabványú - kockázatelemzési módszert célszerű alkalmazni más közigazgatási, rendvédelmi szervezetek hasonló volumenű informatikai rendszereinek, és azok elhelyezésére szolgáló környezet egyes elemeinek vizsgálata során.

Felhasznált irodalom

[1] [i] SEBESTYÉN Attila: Büntetés-végrehajtás informatikai fejlesztési projekt. = Kommunikáció 2009, 2009 Zrínyi Miklós Nemzetvédelmi Egyetemi Kiadó - ISBN 978-963-7060-70-0

[2] [ii] A büntetés-végrehajtás országos parancsnokának 1-1/13/2011.(III. 22.) OP intézkedése a büntetés-végrehajtási szervezet informatikai biztonsági szabályainak kiadásáról

[3] [iii] PRISZNYÁK Szabolcs: „A büntetés-végrehajtás informatikai fejlesztésének eredményei” konferencia előadás „Haditechnika – Kommunikáció 2012” nemzetközi szakmai tudományos konferencia (Budapest, 2012. november 15.)

[4] [iv] PRISZNYÁK Szabolcs: "EKOP 1.1.6. projekt eredményei" konferencia előadás „KRIMINÁLEXPO 2012” nemzetközi biztonsági és informatikai, bűnmegelőzési, bűnüldözési, igazságszolgáltatási konferencia (Budapest, 2012. november 20.)

[5] [v] International Standard ISO/IEC 27005 Information technology – Securtity techniques – Information security risk management

[6] [vi] PRISZNYÁK Szabolcs: A BVOP informatikai központjának kockázatelemzése = Hadmérnök 2014. 9. évf. 1. szám -pp 231-239. - ISSN 1788 - 1919

[7] [vii] KERTI András: Az információbiztonsági kockázatkezelés oktatásának buktatói = Kommunikáció 2013: Communications 2013, 2013 Nemzeti Közszolgálati Egyetem, pp. 53-60. - ISBN:978-615-5305-16-0

[8] [viii] 1995. évi CVII. törvény a büntetés-végrehajtási szervezetről