Óbudai Egyetem

Doktori (PhD) értekezés

tézisfüzete

A kritikus információs infrastruktúrák biztonságos üzemeltetésének vizsgálata hálózatelméleti megközelítésből, az ember-technika-környezet relációjában

Puskás Béla

Témavezetők:

Dr. Magyar Sándor

Biztonságtudományi Doktori Iskola

Budapest, 2017

Tartalomjegyzék

1 Summary

The safe operation of critical informatics systems includes several components. The maintenance of high level safety measures is essential for the safe operation of a system through its whole life cycle.

Apart from the numerous environmental effects, which have impact on the network, the most influential of them are the human beings and the legislation regulating the connection between them and the system. Based on my personal experiences gained during the operation of informatics systems, conferences, discussions with the specialists and experts and other information obtained from relating sources of the special literature I presume, that the management of this matter is quite insufficient. While on governmental level the cyber security has improved significantly, the operation of critical informatics systems is regulated only on the level of informatics security. Another problem is the lack of systematic, overall consideration of the matter, which can be improved by an approach based on network theory. This method could also be expanded by the accurate registration of the system elements and the definition of their processes, which are usually insufficiently done by the governmental sector. The principles of system approach and the results of the network theory researches could obviously contribute to the development of the software, which could support the high level availability of the critical informatics infrastructures and improve the safe operation of the informatics systems.

The main goal of my doctoral essay is to highlight the importance of system approach and the complexity of informatics infrastructure. I intend to introduce the complexity of a data centre and the network of its numerous elements and processes, mainly concentrating on the structure of the data centre besides the hardware, software and technologies, which are described in a less detailed way. The factors of financial, human resources and legislation matters, which are also important elements of the system, are also mentioned in my work.

Two physical IT networks are virtually connected by the human beings and their societal networks. The essay also examines the links between the humans and the systems and their influences on the operation of the networks. My main goal is to elaborate proposals regarding the necessary alterations of legislation and operation in order to ensure the safe operation of critical informatics systems. During my researches I have studied the physical and logical structures of several financial, industrial and military critical informatics networks.

2 A kutatás előzményei

A kritikus informatikai rendszerek biztonságos üzemeltetése több összetevőből áll. Ahhoz, hogy egy rendszer az életciklusa egészében biztonságosan működjön elengedhetetlen az üzemeltetés biztonság magas színvonalú biztosítása. A kutatásom során ezt a területet vizsgáltam meg részletesen.

A kritikus informatikai rendszerek – mint az élet számos területén megtalálható egyéb más rendszerek is – bonyolult hálózati felépítést mutatnak. A kritikus informatikai rendszerek létfontosságú infrastruktúrát szolgálnak ki ezért is tartottam fontosnak azok részletesebb tanulmányozását. Az értekezésemben többször használom a kritikus információs infrastruktúra megfogalmazást, ami alatt a kritikus informatikai rendszereket értem.

Az üzemeltetésben a számos környezeti hatás mellett a legmeghatározóbb talán az ember és az őt, az ő kapcsolatát a rendszerrel szabályzó jogszabályi háttér. Az informatikai üzemeltetés során felhalmozott személyes tapasztalatom, a konferenciákon való részvételeim, a szakirodalomban leírtak, valamint a szakmában dolgozókkal folytatott személyes megbeszélések során azt tapasztaltam, hogy hiányosságok mutatkoznak ezen a területen. Az információbiztonság területén hatalmas lépések történtek kormányzati szinten, azonban a kritikus informatikai rendszerek üzemeltetésével csak az informatikai biztonság kapcsán foglalkoznak a szabályzók. Az informatikai vezetők magukra vannak hagyva döntéseikben, a képzésekben, sokszor személyes képességeiken múlik, hogy meggyőzzék a vezetést egy-egy döntés fontosságáról. A másik problémát a rendszerszintű, átfogó gondolkodás hiányosságában látom. Ebben segítene a hálózatelméletű megközelítés. Ehhez a gondolatmenethez szorosan kapcsolódik a rendszerelemek pontos nyilvántartása, valamint az ezekhez kapcsolódó folyamatok pontos definiálása, amelyek sok esetben az állami szektorban hiányosak. Az értekezésben rámutatok, hogy amennyiben rendszerszemléletben gondolkodunk és a hálózatelméleti kutatások eredményeit is helyesen tudjuk alkalmazni, akkor lehetőség nyílik egy olyan szoftver megalkotására, amely segíteni tudja a magas rendelkezésreállást a kritikus információs infrastruktúrákban. Ezzel növelhető az informatikai rendszer biztonságos működése is.

3 Célkitűzések

A doktori értekezés célja, hogy rávilágítsak a rendszerszemlélet fontosságára és a kritikus információs infrastruktúra üzemeltetésében feltárjak olyan hiányosságokat, amelyek kiküszöbölésével az üzemeltetés biztonsága jelentősen javítható Magyarországon.

A doktori értekezésben az alábbi célokat határoztam meg:

1) A szakirodalom feldolgozását követően bemutatom a hálózatelméleti alapokat, amelyek szoros kapcsolatban állnak a rendszerszemléletű gondolkodással és a rendszermodellezéssel egyaránt.
2) Célom felkutatni, hogy milyen összefüggés lehetséges az ember és az általa üzemeltetett informatikai rendszer között, illetve milyen környezeti tényezők befolyásolják az informatikai rendszerek működését.
3) Célként fogalmaztam meg, hogy megvizsgáljam, milyen struktúrát kell megkövetelni a szervezeti felépítésben, az infrastruktúrában vagy a jogi környezetben.
4) Felkutatom a kritikus informatikai rendszerek, a kapcsolódó kritikus infrastruktúrák üzemeltetésével, védelmével kapcsolatos jogszabályokat. A jogszabályi hiányosságok feltárását követően megfogalmazom, milyen keretek között kell üzemeltetni a kritikus informatikai rendszereket és milyen területeknél szükséges új jogszabály kidolgozása.
5) Az előző célokban megfogalmazott információk birtokában célom meghatározni egy informatikai rendszer üzemeltetését támogató szoftver alapkritériumait.

4 Vizsgálati módszerek

Kutatásom során egyaránt alkalmaztam az empirikus (tapasztalati) és az elméleti kutatási módszereket.

Az elméleti kutatásomban nagy szerepe volt a szintézisnek, ahol az egyes elemeket viszonyítottam az egészhez és a közöttük lévő kapcsolatrendszert térképeztem fel.

Induktív módszerekkel feldolgoztam az évek alatt összegyűlt tapasztalataimat, amelyekből általánosításokat tettem. Ezután az általánosításokat megvizsgálva meggyőződtem azok helyességéről. Az ellenkező irányú módszer alkalmazásakor (deduktív) megvizsgáltam, hogy az általánosságban megfogalmazott állítások a valóságban hogyan érvényesülnek a konkrét területeken, egyedi esetekben.

A feladatom elvégzéséhez a személyes konzultációk során, a kutatási cél elérése érdekében a következő területekkel ismerkedtem meg:

Felkerestem a kutatási témában eredményeket elért kutatókat, szakembereket, cégeket, szervezeteket. Helyszíni bejárás során tanulmányoztam több Magyarországon működő cég kritikus infrastruktúrájának felépítését, valamint irányításának, felügyeletének és üzemeltetésének kialakítását. Szakirodalmak, szakértők segítségével tanulmányoztam a mai kor színvonalának megfelelő kiemelten védett adatközpont kiépítésének követelményeit. Személyes tapasztalatot szerezhettem egy kiemelten védett Magyarországi adatközpont megtervezésében és kivitelezésének irányításában, valamint tanulmányoztam a NATO új főhadiszállásának adatközpont kiépítését, részt vettem az adatok migrálásának megtervezésében.

A kutatás során összegyűjtött információkat rendszereztem, az azokból felvetődött kérdésekre válaszokat kerestem.

5 Új tudományos eredmények

1) Hálózat, rendszer, üzemeltetés biztonság és a kritikus informatikai rendszer definíciójának megalkotása.

Definiáltam mit jelent a hálózat, rendszer és az üzemeltetés biztonság amennyiben ezeket a fogalmakat a kritikus informatikai infrastruktúra kapcsán említjük. A hálózat és rendszer definíciója pontosan meghatározza az értelmezési tartományt, amelyben üzemeltetni kell. Az üzemeltetés biztonság pedig definiálja, mi a legfontosabb cél az üzemeltetés számára a biztonság betartása mellett. Az előzőek alapján pedig meghatároztam mi a kritikus informatikai rendszer.

2) Értekezésemben rámutattam az ember-technika-környezet interdependenciájára, ami alapján kimondható, hogy a többdimenziós hálózatelméleti alapok alkalmazásának bevezetése a rendszerszemléletű gondolkodással elősegítheti a biztonságosabb és komplexebb informatikai rendszerüzemeltetést.

Amennyiben a különböző hálózatokat egy szintnek, egy hálózati rétegnek tekintjük, létezik az emberek kapcsolatrendszerét leíró réteg, a technikai eszközöket ábrázoló rétegek (fizikai kábelezések, logikai kapcsolatok az informatikai rendszerek közt, elhelyezkedésük szerinti stb.) az adatkapcsolati réteg, a jogszabályi struktúra alkotta hálózatok stb. Ezeket a rétegeket külön-külön vizsgálva eltérő eredményt kaphatunk, mintha a köztük lévő kapcsolatokat feltérképezve együtt vizsgálnánk az egészet. Későbbi kutatásokkal, algoritmusok kidolgozásával és ezek alkalmazásokba történő implementálásával elősegíthető egy üzembiztosabb informatikai üzemeltetés.

3) **A kritikus információs infrastruktúra üzemeltetéshez szigorúan szabályozott struktúrát kell kiépíteni, mind a szervezeti felépítésben, mind a környezeti jogszabályok területén és az informatikai rendszerünket kiszolgáló infrastruktúrában.**

A kiépítésnek hierarchikus, felülről szerveződőnek kell lennie. A kiépítést a kormányzati szintről kell kezdeni. A kialakított struktúrával csökkenthető a kockázata annak, hogy a skálafüggetlen hálózatoknál tapasztalható, egy hálózati elem gyengesége okozta meghibásodás, az egész hálózat működésére hatással legyen. A másik fontos oka a szabályozásnak a káosz elkerülése, amely a normál és a katasztrófa közti állapotot jelenti. A felülről szerveződött hierarchikus felépítéssel, a központosított oktatási rendszerrel, szoftvergazdálkodással stb. költségtakarékosabb működés érhető el.

4) **Rámutattam, hogy jelenleg Magyarországon a kritikus informatikai rendszerek üzemeltetéséhez szükséges jogszabályi hátterek hiányosak.**

A homogén, hierarchikusan felépülő jogszabályi rendszerrel biztosítható, hogy a kritikus információs infrastruktúrák Magyarországon egységes rendszerként kezeljük. A szabályzókba be kell építeni a szabványokat, ugyanakkor egyes szabványok betartatását jogszabályokban kell elrendelni. Az egységes kezelés érdekében a törvény erejénél fogva létre kell hozni a Nemzeti Létfontosságú Információs Rendszer Üzemeltetést Koordináló Testületet, a Stratégiai Kutatóintézetet, kialakítani az oktatási rendszert és egy szervezetet, amely a magas szintű informatikai támogatásra képes.

5) **Felvázoltam egy felügyeleti és automatikusan beavatkozni képes rendszer felépítésének egy lehetséges módját.**

A döntéstámogató rendszer egységesen kezeli a szenzorok jelétől kezdve a megjelenítő rétegig minden egyes rendszerelem működését. A rendszer alapja a konfigurációs adatbázis, amelyben lévő adatokon végezhető el a különböző vizsgálat. A többdimenziós hálózati modell alkalmazása az információ integrációs és a tudásfeldolgozó elemző rétegben elősegíti a komplex rendszerelemzést. A dinamikus elemzés összehasonlításokat végezhet a múltbeli pillanatképek és a jelenlegi helyzetekkel, ami alapján eseményeket generálhat a rendszer. A jövőben elméleti és alkalmazott matematika módszerekkel továbbfejleszthető a rendszer.

6 Az eredmények hasznosítási lehetősége

Az értekezésem tudományos eredményeit a részletes kidolgozást követően, elsősorban az állam által közvetlen, vagy közvetett módon a kritikus információs infrastruktúra üzemeltetés területén képzelem el hasznosítani. A javasolt megoldásokkal költségek takaríthatók meg és az üzemeltetés biztonság jelentősen javítható. A részletes kidolgozáshoz, a hálózatelmélet alkalmazásához a hazai oktatási intézmények segítségét kell hívni pályázati úton. Ezzel kettős cél érhető el, egyrészt támogathatók az oktatási intézmények, másrészt magasan képzett emberek figyelme irányítható rá a kívánt területre, amellyel színvonalas fejlesztés végezhető el.

A javasolt döntéstámogató rendszer stabil működése kizárólag gondos tervezéssel érhető el és építőelemenként kell bevezetni. Kezdetben kisebb szervezetekre kell kiépíteni, majd kiterjeszteni egyre nagyobbakra, tehát egy alulról induló építkezést javaslok.

Az adminisztratív témaköröket tekintve (jogszabályok, struktúra kialakítása) az előzőekkel ellentétben a felülről lefelé történő kiépítés az indokolt.

7 Irodalmi hivatkozások listája

[1] **Kovács László**, Kritikus információs infrastruktúrák Magyarországon, Robothadviselés 7. Tudományos Szakmai Konferencia, 2007. november 27. Elérhető:http://hadmernok.hu/kulonszamok/robothadviseles7/kovacs_rw7.html#9. [Hozzáférés dátuma: 2017.03.31.].

[2] **Schmidt Eric Emerson**, Elérhető: http://www.citatum.hu/idezet/39268. [Hozzáférés dátuma: 2017.03.31.].

[3] **Beleznay Péter**, *szerző,* Az Internet története, Networkshop 2012 konferencia, Nemzeti Információs Infrastruktúra Fejlesztési Intézet, Elérhető: http://niif.videotorium.hu/hu/recordings/4081/az-internet-tortenete. [Hozzáférés dátuma: 2017.03.31.].

[4] **Georgi Dalakov,** Paul Baran, Elérhető: http://history-computer.com/Internet/Birth/Baran.html [Hozzáférés dátuma: 2017.03.31.].

[5] **Puskás Béla**, The risks of networks' complexity, Hadmérnök, pp. 167-171., 2012. VII. Évfolyam 4. szám, ISSN 1788-1919

[6] **Barabási Albert-László**, Behálózva, Budapest: Magyar könyvklub, 2003., ISBN 963-547-895-x

[7] **Cambridge Computer Lab,** Introduction to Network Theory, Elérhető: https://www.cl.cam.ac.uk/teaching/1011/PrincComm/slides/graph_theory_1-11.pdf. [Hozzáférés dátuma: 2017.03.31.].

[8] **Munk Sándor**, Hálózatok fogalma, alapjai, Hadmernök, 2010. V. Évfolyam, 3. szám, ISSN 1788-1919

[9] **Haig Zsolt; Kovács László**, Kritikus infrastruktúrák és kritikus információs infrastruktúrák, Tanulmány (TÁMOP 4.2.2/B-10/1-2010-0001), **Ványa László** (*szerkesztő)*, Budapest: Nemzeti Közszolgálati Egyetem, 2012.

[10] **Husi Géza**, Rendszerelmélet, Elérhető: http://old.eng.unideb.hu/vmt2/images/tantargyak/szimulacio/Rendszer%20szeml%C3%A9let.pdf. [Hozzáférés dátuma: 2017.03.31.].

[11] **Pokorádi László**, Rendszerek és folyamatok modellezése, Debrecen: Campus kiadó, 2008., ISBN 978-963-9822-06-1

[12] **A honvédelmi miniszter 39/2014. (V. 30.) HM utasítása** a Magyar Honvédség Informatikai Szabályzatának kiadásáról.

[13] **Puskás Béla**, Kritikus Információs Infrastruktúrák modellezése, Felderítő Szemle, 1. szám 13/3, pp. 95-107, 2014., HU ISSN 1588-242X

[14] **Ürmösi Károly**, A biztonság, a biztonság fogalma, Hadtudományi szemle, 6.4, pp. 147-154, 2013., HU ISSN 2060-0437

[15] **Miniszterelnöki Hivatal Informatikai Koordinációs Iroda, Informatikai Tárcaközi,** Bizottság Informatikai rendszerek biztonsági követelményei 12. sz. ajánlás, Budapest, 1996.,
Elérhető: https://dsd.sztaki.hu/mockups/itb/ajanlasok/a12/index.html.

[Hozzáférés dátuma: 2017.03.31.].

[16] **Munk Sándor**, Robothadviselés 7. Tudományos Szakmai Konferencia, 2007. november 27., Információbiztonság vs. Informatikai Biztonság, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest

[17] **Szenes Katalin**, (szerkesztő), Az informatikai biztonság kézikönyve Informatikai biztonsági tanácsadó A-tól Z-ig. (27. aktualizálás), Budapest,: Verlag-Dashöfer Szakkiadó, 2007. ISBN: 9639313122

[18] **2013. évi L. törvény** az állami és önkormányzati szervek elektronikus információbiztonságáról.

[19] **2009. évi CLV. törvény** a minősített adat védelméről.

[20] **AXELOS Ltd**., ITIL Foundation Course (FND02 v4.3),
Elérhető: http://www.itsmf.hu/documents/itil2modszertan_osszefoglalo_v3.1.pdf.
[Hozzáférés dátuma: 2017.03.31.].

[21] **2080/2008. (VI. 30.) Korm. határozathoz tartozó Zöld könyv** a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról.

[22] **2012. évi CLXVI. törvény** a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

[23] **Muha Lajos**, A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, Doktori (PhD) értekezés, Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2007.

[24] **65/2013. (III. 8.) Korm. rendelet** a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.

[25] **Dr.Haig Zsolt, Hajnal Béla, Dr. Kovács László, Dr. Muha Lajos, Sik Zoltán Nándor**, A kritikus információs infrastruktúrák meghatározásának módszertana, ENO Avisory Kft., 2009.
Elérhető: http://www.cert-hungary.hu/sites/default/files/news/a_kritikus_informacios_infrastrukturak_meghatarozasanak_modszertana.pdf. [Hozzáférés dátuma: 2017.03.31.]

[26] **Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége - Adatközpont- és Felhő Munkacsoport**,
Elérhető: http://ivsz.hu/wp-content/uploads/2015/09/IVSZ-adatkozpont-fogalomtar.pdf. [Hozzáférés dátuma: 2017.03.31.].

[27] **Kovács László**, Hálózatkutatás és szociolingvisztika, Magyar Nyelvőr. 135/1. 90-96., 2011. ISSN 1585-4515

[28] **David Rehak, Petr Novotny**, Bases for Modelling the Impacts of the Critical Infrastructure, 2016. Elérhető: http://www.aidic.it/cet/16/53/016.pdf.
[Hozzáférés dátuma: 2017.03.31.].

[29] **Fazekas István**, Neurális hálózatok, Debrecen, Debreceni Egyetem Informatikai Kar, 2013. ISBN 978-88-95608-44-0

[30] **Vicsek Tamás**, A Magyar Tudományos Akadémia folyóirata,
Elérhető: http://www.matud.iif.hu/03mar/vicsek.html.
[Hozzáférés dátuma: 2017.03.31.].

[31] **Tél Tamás; Gruiz Márton**, Mi a káosz? (És mi nem az?), Fizikai Szemle 2005/6. 218.o., Fizikai szemle, Magyar fizikai folyóirat, 2005.
Elérhető: http://fizikaiszemle.hu/archivum/fsz0506/gruiz0506.html.

[Hozzáférés dátuma: 2017.03.31.].

[32] **MacKay David John Cameron**, CITATUM,
Elérhető: http://www.citatum.hu/idezet/63938. [Hozzáférés dátuma: 2017.03.31.].

[33] **Gerőcs László; Vancsó Ödön**, (szerkesztő), Matematika, Budapest: Akadémia Kiadó, 2010, pp. 1151-1224, ISBN 978 963 05 8488 3

[34] **Kátai Zoltán**, Gráfelméleti Algoritmusok, Kolozsvár: Scientia Kiadó, 2008., ISBN 978-973-7953-95-7

[35] **Takács Károly** (szerkesztő) **BCE Szociológia és Társadalompolitika Intézet**, Társadalmi kapcsolathálózatok elemzése, Elérhető: http://publikaciok.lib.uni-corvinus.hu/publikus/647793.pdf. [Hozzáférés dátuma: 2017.03.31.].

[36] **Fekete István, Hunyadvári László, Nagy Tibor, Giachetta Roberto, Bartha Dénes, Ilonczai Zsolt, Danyluk Tamás**, Algoritmusok és adatszerkezetek / Minimális költségű feszítőfák, Elérhető: http://tamop412.elte.hu/tananyagok/algoritmusok/lecke28_lap1.html. [Hozzáférés dátuma: 2017.03.31.].

[37] **Podobni Katalin**, Legrövidebb útkereső algoritmusok, diplomamunka, Budapest: Eötvös Lóránd Tudományegyetem Természettudományi kar Operációkutatási tanszék, 2009.

[38] **PlexMath**, MuxViz: visualization of multiplex networks, Elérhető: http://www.plexmath.eu/?page_id=327. [Hozzáférés dátuma: 2017.03.31.].

[39] **Albert Solé-Ribalta, Clara Granell, Sergio Gómez and Alex Arenas**, Information transfer in community structured multiplex networks, Elérhető: http://journal.frontiersin.org/article/10.3389/fphy.2015.00061/full. [Hozzáférés dátuma: 2017.03.31.].

[40] **Vicsek Tamás, Szabados László** (szerkesztő), Hálózatok, Budapest, A Magyar Tudományos Akadémia folyóira. 167. évfolyam – 2006/11. szám, ISSN 0025 0325

[41] **Puskás Béla**, Hálózatelméleti alapok, 2012., Elérhető: http://www.puskashirbaje.hu/index_htm_files/Puskas_Bela_Halozatelmeleti_alapok.pdf, [Hozzáférés dátuma: 2017.03.31.].

[42] **Kormányzati Eseménykezelő Központ (GovCERT-Hungary)**, Spamhaus stílusú DDoS, Elérhető: http://tech.cert-hungary.hu/taxonomy/term/3576. [Hozzáférés dátuma: 2017.03.31.].

[43] **Csermely Péter**, A rejtett hálózatok ereje, Budapest: Vince kiadó, 2005. ISBN 963 9552 64 X

[44] **Kürtös Zsófia**, A társadalmi kapcsolatháló elemzés módszertani alapjai, Letenyei László (szerkesztő), Településkutatás szöveggyűjtemény, Budapest: Ráció, pp. 663-685.

[45] **Puskás Béla**, Kritikus információs infrastruktúrák biztonsága, sérülékenysége, Szakmai szemle, pp. 126-149, 2013., HU ISSN 1785-118

[46] **Székely Balázs**, Markov-láncok, Elérhető: http://www.math.bme.hu/~szbalazs/oktatas/sztoch_info/het_4_Markov.pdf. [Hozzáférés dátuma: 2017.03.31.].

[47] **Symantec**, Internet Security Threat Report, Elérhető: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf. [Hozzáférés dátuma: 2017.03.31.].

[48] **Bodnár Balá**zs, A Magyar Köztársaság védelmi igazgatási rendszerének lehetséges korszerűsítése - Doktori értekezés, Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem Kossuth Lajos Hadtudományi Kar Hadtudományi Doktori Iskola, 2009

[49] **Salamon Pál**, A Sorel-ház, Pécs: Alexandra, 2010., ISBN: 9789632972398

[50] **Csernus Im**re, Bevállalja?, Budapest: HTSART, 2004., ISBN: 9632161572

[51] **Muha Lajos, Krasznay Csaba,** Az elektronikus információs rendszerek biztonságának menedzselése, Budapest: Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, 2014., ISBN 978-615-5491-65-8

[52] **Szádeczky Tamás**, Szabályozott biztonság – Az informatikai biztonság szabályozásának elmélete, gyakorlata és az alkalmazás megkönnyítésére felállított módszertan, doktori értekezés, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, 2011.

[53] **Puskás Béla**, Az informatikai rendszerek és a jogi környezet változásai, HÍRVILLÁM = SIGNAL BADGE, 2013. 4. évfolyam 2. szám, pp. 204-214, HU ISSN 2061-9499

[54] **A Katasztrófavédelmi Koordinációs Tárcaközi Bizottság 4/2016 határozata**

[55] **Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve** a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

[56] **Rossella Mattioli, Dr. Cédric Levy-Bencheton**, Methodologies for the identification of Critical Information Infrastructure assets and services, Elérhető: https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport. [Hozzáférés dátuma: 2017.03.31.].

[57] **ENISA**, Gaps in NIS standardisation - Recommendations for improving NIS in EU standardisation policy, Elérhető: https://www.enisa.europa.eu/publications/gaps-eu-standardisation/at_download/fullReport. [Hozzáférés dátuma: 2017.03.31.].

[58] **ENISA**, Communication network dependencies for ICS/SCADA Systems, Elérhető: https://www.enisa.europa.eu/publications/ics-scada-dependencies/at_download/fullReport. [Hozzáférés dátuma: 2017.03.31.].

[59] **Global Forum on Cyber Expertise** , The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers, Elérhető:https://www.tno.nl/media/8578/gpg_criticalinformationinfrastructureprotection.pdf. [Hozzáférés dátuma: 2017.03.31.].

[60] **1995. évi XXVIII. törvény** a nemzeti szabványosításról.

[61] **ISO/IEC 14764:2006** Software Engineering -- Software Life Cycle Processes – Maintenance.

[62] **ISO/IEC/IEEE 29119-1:2013** Software and systems engineering -- Software testing -- Part 1: Concepts and definitions.

[63] **ISO/IEC 33001:2015** Information technology -- Process assessment -- Concepts and terminology.

[64] **ISO/IEC 33002:2015** Information technology -- Process assessment -- Requirements for performing process assessment.

[65] **ISO/IEC 33003:2015** Information technology -- Process assessment -- Requirements for process measurement frameworks.

[66] **ISO/IEC 33004:2015** Information technology -- Process assessment -- Requirements for process reference, process assessment and maturity models.

[67] **ISO/IEC 33020:2015** Information technology -- Process assessment -- Process measurement framework for assessment of process capability.

[68] **IT4IT** - Managing the Business of IT. *(szabvány)*

[69] **ISACA Magyarországi Egyesület**, ISACA magyar szakkifejezés-gyűjtemény, ISACA Magyarországi Egyesület, 1027 Budapest, Horvát u. 14-24., 2013. ISBN: 978-963-08-6769-6

[70] **Holtai András; Magyar, Sándor; Puskás, Béla**, Az informatikai fejlesztés és üzemeltetés határvonalai, Felderítő Szemle, XV. évfolyam 1. szám, pp. 191-203, HU ISSN 1588-242X

[71] **Dr. Michelberger Pál - Lábodi Csaba**, Vállalati információbiztonság szervezése. Elérhető: http://kgk.uni-obuda.hu/sites/default/files/10_Michelberger_Labodi.pdf, [Hozzáférés dátuma: 2017.03.31.].

[72] **MSZ ISO/IEC 20000-1:2013**, Informatika. Szolgáltatásirányítás. 1. rész: A szolgáltatásirányítási rendszer követelményei.

[73] **MSZ EN ISO/IEC 27000:2017** Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Áttekintés és szakszótár (ISO/IEC 27000:2016), 2017.

[74] **MSZ ISO/IEC 27001**:**2014** Informatika. Biztonságtechnika.Az információbiztonság irányítási rendszerei. Követelmények.

[75] **MSZ EN ISO/IEC 27002:2017** Informatika. Biztonságtechnika. Gyakorlati útmutató az információbiztonsági kontrollokhoz/intézkedésekhez (ISO/IEC 27002:2013, tartalmazza a 2014. évi 1. és a 2015. évi 2. helyesbítést).

[76] **ISO/IEC 27005:2008** Information technology -- Security techniques -- Information security risk management.

[77] **AJP-3.10** ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS, 2015.

[78] **Puskás Béla**, Információbiztonsági környezet kialakítása, HÍRVILLÁM = SIGNAL BADGE, 1. szám 6/2, pp. 108-133, 2015. HU ISSN 2061-9

[79] **AAP-31 Ed. 3** NATO Communication and Information Systems Glossary, 2016.

[80] **AC/35-D/2005-REV3** Management Directive on CIS Security, 2015.

[81] **JSP 480-16th Edition** Defence Co-Ordinatinginstallation Design Authority.

[82] **JSP 440 Edition 4.3** The Defence Manual of Security.

[83] **AJP-6 Ed. A,** Allied Joint Docrine for Communication and Information Systems, ’17

[84] **Szádeczky Tamás**, „Információbiztonsági szabványok,” Elérhető: http://vtki.uni-nke.hu/uploads/media_items/informaciobiztonsagi-tudatossag-gyakorlat.original.pdf. [Hozzáférés dátuma: 2017.03.31.].

[85] **Porkoláb Imre**, A hadviselés adaptációja: harc az emberi elméért, HADTUDOMÁNYI SZEMLE, 2014. VII. évfolyam 3. szám., pp. 56-69, HU ISSN 2060-0437

[86] **Symantec**, Internet Security Threat Report 2016 Elérhető: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf. [Hozzáférés dátuma: 2017.03.31.].

[87] **AXELOS Limited**, Elérhető: ITIL® szakkifejezések és rövidítések magyarul. Elérhető: https://www.exin.com/assets/exin/frameworks/108/glossaries/hungarian_glossary_v1.0_201404.pdf [Hozzáférés dátuma: 2017.03.31.].

[88] **KFKI Számítástechnikai Rt**, Az ITIL módszertan áttekintése, Elérhető: http://www.itsmf.hu/documents/itil2modszertan_osszefoglalo_v3.1.pdf. [Hozzáférés dátuma: 2017.03.31.].

[89] **itSMF Hungary**, ITIL® Glossary of Terms, Definitions and Acronyms in Hungarian, V3.1.24.h 2.5, Budapest: itSMF Hungary, 2008., Elérhető: http://www.uni-obuda.hu/users/horvath.zsolt.laszlo/_szakirodalom /ITIL/ITIL%20V3%20fogalomt%C3%A1r%20v2.5.pdf. [Hozzáférés dátuma: 2017.03.31.].

[90] **Delta-3N Kft.**, Karbantartási stratégiák fejlődése Elérhető: http://www.delta3n.hu/gepvedelem/karbantartasi-strategiak-fejlod%C3%A9se. [Hozzáférés dátuma: 2017.03.31.].

[91] **ENISA**, Critical Information Infrastructures Protection approaches in EU ENISA 2015, Elérhető: https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf. [Hozzáférés dátuma: 2017.03.31.].

[92] **Chandrika Nath**, Cyber Security in the UK, Elérhető: http://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf. [Hozzáférés dátuma: 2017.03.31.].

[93] **Mártonffy Attila**, IT Business Online, Elérhető: http://www.itbusiness.hu/Fooldal/hetilap/business/Az_informatika_es_a_koltsegek.html. [Hozzáférés dátuma: 2017.03.31.].

[94] **ACMP-5** NATO Requirements for Configuration Audits.

[95] **ISACA**, COBIT 5, United States of America, 2012. ISBN 978-1-60420-237-3

[96] **Puskás Béla; Rajnai Zoltán**, Requirements of the installation of the critical informational infrastructure and its management, Interdisciplinary description of complex systems, pp. 48-56, 2015/13., 48-56.pdf. ISSN 1334-4684, 2015.

[97] **Beinschroth József**, Kríziskezelés- Informatikai krízishelyzetek kezelése, Elérhető: http://uni-obuda.hu/users/beinschrothj/Kriziskezeles/Kriziskezeles_c .pdf. [Hozzáférés dátuma: 2017.03.31.].

[98] **MAVIR ZRt.,** P5 – 5. Eljárásrend: Vészhelyzeti üzem, Elérhető: http://mavir.hu/documents/10258/20774/policy5_final+version_H.pdf/8fe133d9-cda2-4581-9703-ff69226a41c2. [Hozzáférés dátuma: 2017.03.31.].

[99] **Puskás Béla; Rajnai Zoltán**, Decision-making support software application option for critical informational infrastructures, Acta Technica Corviniensis –Bbulletin of Engineering, pp. 89-94, 2015. ISSN 2067-3809

[100] **National Critical Information Infrastructure Protection Centre New Delhi**, Guidelines for the Protection of National Critical Information Infrastructure, Elérhető: https://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf. [Hozzáférés dátuma: 2017.03.31.].

[101] **García Zaballos, Antonio; Jeun, Inkyung**, Best Practices for Critical Information Infrastructure Protection (CIIP): Experiences from Latin America and the Caribbean and Selected Countries, Elérhető: https://publications.iadb.org/bitstream/handle/11319/7848/Best-Practices-for-Critical-Information-Infrastructure-Protection-%28CIIP%29-Experiences-from-Latin-America-and-the-Caribbean-and-Selected-Countries.pdf?sequence=1&isAllowed=y. [Hozzáférés dátuma: 2017.03.31.].

[102] **Steve Greenberg, Evan Mills, Bill Tschudi, Peter Rumsey, Bruce Myatt, Wei Bai, Wenli Geng**, Best Practices for Data Centers: Lessons Learned from Benchmarking 22 Data Centers, Elérhető: http://www.ing.unitn.it/~fontana/GreenInternet/Benchmarks/ACEEE-datacenters.pdf. [Hozzáférés dátuma: 2017.03.31.].

[103] **BS 7083:1996** Guide to the accommodation and operating environment for information technology (IT) equipment

[104] **AC/35-D/2001-REV2** Directive on Physical Security, 2008.

[105] **AC/322-D/0048-REV2** Technical Implementation Directive for Computer and Local Area Network (LAN) Security, 2011.

[106] **BS EN 50173-x:2007** Information technology Generic cabling systems.

[107] **90/2010. (III. 26.) Korm. rendelet** a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről.

[108] **Barabási Albert-László**, Villanások A jövő kiszámítható, Budapest: Nyitott Könyvműhely Kiadó KFT, 2010, p. 261. oldal., ISBN 978-963-310-014-1

[109] **Puskás Bél**a, Kockázatelemzés, kockázatértékelés: Informatikai üzemeltetés során fellépő kockázatok értékelése, Az 5. Báthory-Brassai Konferencia tanulmánykötetei., Budapest, Óbudai Egyetem Biztonságtudományi Doktori Iskola, 2014, pp. 438-443., ISBN:978-615-5460-38-8

[110] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**, „BSI-Standard 100-4: Business Continuity Management, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1. [Hozzáférés dátuma: 2017.03.31.]

[111] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**, „BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile&v=1. [Hozzáférés dátuma: 2017.03.31.].

[112] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**, „Risk analysis with the new threat catalogue T 0 "Elementary Threats, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf?__blob=publicationFile&v=1. [Hozzáférés dátuma: 2017.03.31.].

[113] **Abhinav Biswas, Sukanya Karunakaran**, Cybernetic modeling of Industrial Control Systems: Towards threat analysis of critical infrastructure, Elérhető: https://arxiv.org/ftp/arxiv/papers/1510/1510.01861.pdf. [Hozzáférés dátuma: 2017.03.31.].

[114] **Botos Zsolt**, Komputeralgebra Tanszék és a Magyar Tudományos Akadémia Számelméleti Kutatócsoport, Elérhető: http://compalg.inf.elte.hu/~attila/materials/ITbiztonsag_09_kockazat.pdf. [Hozzáférés dátuma: 2017.03.31.].

[115] **Pilar-tools,** Elérhető: http://www.pilar-tools.com/en/index.html. [Hozzáférés dátuma: 2017.03.31.].

[116] **ENISA**, EAR / PILAR, Elérhető: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_EAR_Pilar.html. [Hozzáférés dátuma: 2017.03.31.].

[117] **ENISA**, Threat and Risk ManagementRisk Management, Elérhető: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management. [Hozzáférés dátuma: 2017.03.31.].

[118] **Neumann János**, A számológép és az agy, Budapest: Gondolat Könyvkiadó, 1964., ISBN:0609001048471

[119] **Sunbird**, An Introduction to Data Center Infrastructure Management, Elérhető: https://www.sunbirddcim.com/sites/default/files/WP005_Revised_Sunbird_WhitePaper_Intro_toDCIM.pdf. [Hozzáférés dátuma: 2017.03.31.].

[120] **Schneider-electric**, Data Center Infrastructure Management (DCIM), Elérhető: http://www.schneider-electric.com/b2b/en/solutions/system/s4/data-center-and-network-systems-dcim/. [Hozzáférés dátuma: 2017.03.31.].

[121] **Neumann John von**, First Draft of a Report on the EDVAC,
Contract No. W-670-ORD-4926,
Between the United States Army Ordinance Department
and the University of Pennsylvania Moore School of Electrical Engineering
University of Pennsylvania
June 30, 1945

[122] **ACMP-4** NATO Requirements for Configuration Status Accounting and Configuration Data Management.

[123] **Jeff O'Brien**, 7 Tips for Managing Preventive Maintenance at Data Centers, Elérhető: http://www.datacenterknowledge.com/archives/2014/01/23/7-tips-managing-preventive-maintenance-data-centers/.
[Hozzáférés dátuma: 2017.03.31.].

[124] **Puskás Béla**, Integrált felügyeleti rendszer, Hadmérnök, XII. Évfolyam 1. szám, pp. 268-277, 2017. ISSN 1788-191

[125] **ACMP-3** NATO Requirements for Configuration Control - Engineering Changes, Deviations and Waivers.

[126] **ACMP-7** NATO Configuration Management - Guidance on the Application of ACMP-1 to 6.

[127] **Bognár Balázs**, Országos Katasztrófavédelemi Főigazgatóság, A kritikus infrastruktúra,
Elérhető: http://www.katasztrofavedelem.hu/index2.php?pageid=lrl_index. [Hozzáférés dátuma: 2017.03.31.].

[128] **Device42**, Automated Data Center Management, Elérhető: http://www.device42.com/solutions/automated-data-center-management/?utm_source=Google&utm_medium=cpc&utm_campaign=Data_Center_Management_GA&utm_adgroup=Data_Center_Software&ad=140979572855&utm_term=data%20center%20management%20tools&matchtype=e&gclid=CJ3K. [Hozzáférés dátuma: 2017.03.31.].

[129] **Barabási Albert-László**, Elérhető: www.ceeol.com. [Hozzáférés dátuma: 2017.03.31.].

[130] **Cho Adrian**, „Mathematician claims breakthrough in complexity theory," Science, Elérhető: http://news.sciencemag.org/math/2015/11/mathematician-claims-breakthrough-complexity-theory. [Hozzáférés dátuma: 2017.03.31.]

[131] **ACMP-6** NATO Configuration Management Terms and Definitions.

[132] **Gartner**, Reviews for Data Center Infrastructure Management (DCIM) Software, Elérhető: https://www.gartner.com/reviews/market/data-center-infrastructure-management-tools. [Hozzáférés dátuma: 2017.03.31.].

[133] **Hewlett Packard Enterprise Development LP.**, HPE Operations Orchestration, Elérhető: https://www.hpe.com/h20195/V2/getpdf.aspx/4AA1-5782ENW.pdf. [Hozzáférés dátuma: 2017.03.31.].

[134] **1998. évi LXXXV. törvény** a Nemzeti Biztonsági Felügyeletről.

[135] **2003. évi C. törvény** az elektronikus hírközlésről.

[136] **179/2003. (XI. 5.) Korm. rendelet** a nemzetközi szerződés alapján átvett, vagy nemzetközi kötelezettségvállalás alapján készült minősített adat védelmének eljárási szabályairól.

[137] **27/2004. (X. 6.) IHM rendelet** az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségeiről.

[138] **100/2004. (IV. 27.) Korm. rendelet** az elektronikus hírközlés veszélyhelyzeti és minősített időszaki felkészítésének rendszeréről, az államigazgatási szervek feladatairól, működésük feltételeinek biztosításáról.

[139] **2073/2004. (IV. 15.) Korm. határozat** a Magyar Köztársaság nemzeti biztonsági stratégiájáról.

[140] **2007. évi LXXXVI. törvény** a villamos energiáról.

[141] **2010. évi CLVII. törvény** a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről.

[142] **92/2010. Korm. rendelet** az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól.

[143] **161/2010. Korm. rendelet** a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól.

[144] **346/2010. Korm. rendelet** a kormányzati célú hálózatokról.

[145] **1249/2010. (XI. 19.) Korm. határozat** az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végre.

[146] **309/2011. (XII. 23.) Korm. rendelet** a központosított informatikai és elektronikus hírközlési szolgáltatásokról.

[147] **360/2013. (X. 11.) Korm. rendelet** az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

[148] **363/2013. (X. 11.) Korm. rendelet** a Külügyminisztérium diplomáciai célokra használt informatikai eszközeinek, hardver- és szoftver összetevőinek karbantartása, felügyelete, üzemeltetése, részleges rendszergazdai támogatása szolgáltatás ellátására.

[149] **484/2013. (XII. 17.) Korm. rendelet** a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről.

[150] **512/2013. (XII. 29.) Korm. rendelet** az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről, valamint a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről.

[151] **541/2013. (XII. 30.) Korm. rendelet** a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről.

[152] **7/2013. (II. 26.) NFM rendelet** a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről.

[153] **41/2015. (VII. 15.) BM rendelet** az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre.

[154] **185/2015. (VII. 13.) Korm. rendelet** a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytat.

[155] **187/2015. (VII. 13.) Korm. rendelet** az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek.

[156] **246/2015. (IX. 8.) Korm. rendelet** az egészségügyi létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

[157] **330/2015. (XI. 10.) Korm. rendelet** a pénzügyi ágazathoz tartozó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

[158] **359/2015. (XII. 2.) Korm. rendelet** a honvédelmi létfontosságú rendszerelemek azonosításáról, kijelöléséről és védelméről.

[159] **2016. évi XXX. törvény** a védelmi és biztonsági célú beszerzésekről.

[160] **38/2016. (XII. 29.) MvM rendelet** a fővárosi és megyei kormányhivatalok informatikai működésére vonatkozó szakmai követelményekről.

[161] **368/2016. (XI. 29.) Korm. rendelet** egyes, a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló kormányrendeletek módosításáról.

[162] **1988. évi I. törvény** a közúti közlekedésről.

[163] **1995. évi XCVII. törvény** a légiközlekedésről.

[164] **2000. évi XLII. törvény** a víziközlekedésről.

[165] **2010. évi CLXXXV. törvény** a médiaszolgáltatásokról és a tömegkommunikációról.

[166] **2011. évi CXII. törvény** az információs önrendelkezési jogról és az információszabadságról.

[167] **118/2011. (VII. 11.) Korm. rendelet** a nukleáris létesítmények nukleáris biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről.

[168] **9/2011. (III. 9.) NGM rendelet** a váminformációs rendszerrel kapcsolatos részletszabályokról.

[169] **62/2011. (XII. 29.) BM rendelet** a katasztrófák elleni védekezés egyes szabályairól.

[170] **2012. évi CLIX. törvény** a postai szolgáltatásokról.

[171] **93/2012. (V. 10.) Korm. rendelet** az utak építésének, forgalomba helyezésének és megszüntetésének engedélyezéséről.

[172] **123/2014. (IV. 10.) Korm. rendelet** a közforgalmú személyszállítási szolgáltatásokhoz kapcsolódó adatok, adatbázisok és elektronikus adatkommunikációs technológiák egységességét és átjárhatóságát biztosító műszaki és technológiai előírásokról.

[173] **155/2014. (VI. 30.) Korm. rendelet** a radioaktív hulladékok átmeneti tárolását vagy végleges elhelyezését biztosító tároló létesítmények biztonsági követelményeiről és az ezzel összefüggő hatósági tevékenységről.

[174] **27/2014. (IV. 18.) KIM rendelet** a közfeladatot ellátó szerveknél alkalmazható iratkezelési szoftverekkel szemben támasztott követelményekről.

[175] **2015. évi CCXXII. törvény** az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól, 2015**.**

[176] **46/2015.(XII. 30.) NGM rendelet** a Nemzeti Adó- és Vámhivatal bűnmegelőzési, bűnüldözési, valamint szabálysértési tevékenységével összefüggésben keletkezett adatok kezelésére jogosult szervek meghatározásáról és az adatok kezelésének technikai szabályairól.

[177] **2001/264/EK** Az Európai Unió Tanácsának a Tanács biztonsági szabályzatának elfogadásáról szóló tanácsi határozat.

[178] **Az Európai Parlament és a Tanács 460/2004/EK rendelete** az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról.

[179] **A Tanács 2005/222/IB kerethatározata** (2005. február 24.) az információs rendszerek elleni támadásokról.

[180] **COM (2005) 576 végleges. ZÖLD KÖNYV.** A létfontosságú infrastruktúrák védelmére vonatkozó. Európai programról.

[181] **2008/114/EK tanácsi irányelv** az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről.

[182] **COM (2009) 149 a Bizottság közleménye** az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a régiók bizottságának a kritikus informatikai infrastruktúrák védelméről.

[183] **IP/10/581 Digitális Menetrend:** A Bizottság akcióterve az európai jólét fellendítésére.

[184] **COM (2010) 517 az Európai Parlament és a Tanács irányelve** az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat hatályon kívül helyezéséről.

[185] **COM (2010) 521 az Európai Parlament és a Tanács rendelete** az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA).

[186] **COM (2010) 673 Bizottság közleménye** az Európai Parlamentnek és a Tanácsnak az EU belső biztonsági stratégiájának megvalósítása: öt lépés a biztonságosabb Európa felé.

[187] **2012/2096(INI) Kiberbiztonság és -védelem** Az Európai Parlament 2012. november 22-i állásfoglalása a kiberbiztonságról és -védelemről.

[188] **JOIN/2013/01 közös közlemény** az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a régiók bizottságának az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.

[189] **EU**, Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér című közlemény, 2013.

[190] **C-M(2002) 49** Security Within The North Atlantic Treaty Organisation.

[191] **SDIP-27** NATO TEMPEST requirements and Evaluation procedures.

[192] **SDIP-28** NATO Zoning Procedures.

[193] **SDIP-29** Facility Design Criteria and Installation of Electrical Equipment for Processing Classified Information.

[194] **SDIP-30** Installation of Electronic Equipment for Processing of Classified Data.

[195] **AAP-06** NATO Glossary of terms and definitions (English and French), 2016.

[196] **AC/322-D 0052** NATO Communication and Information Systems Configuration Management Policy, 2006.

[197] **STANAG 4159** NATO Materiel Configuration Management Policy and Procedures for Multinational Joint Projects.

[198] **ACMP-1** NATO Requirements for the Preparation of Configuration Management Plans.

[199] **ACMP-2** NATO Requirements for Configuration Identification.

[200] **AC/35-D/2004-REV3 Primary Directive on CIS Security, 2013.**

[201] **ACO Directive 080-095** Communication and Information System (CIS) Planning Directive, 2014.

[202] **AAITP-06** System Architecture Requirements for Asset, Consignment and Personnel Tracking Information Excchange, 2014.

[203] **JSP480 Edition_16** Manual of Regulations for Installation of Communication & Information Systems.

[204] **BS 6701**:2010 Telecommunications equipment and telecommunications cabling-specification for installation, operation and maintenance.

[205] **BS EN 50174-x**:2009/2003 Information technology Cabling installation.

[206] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**, BSI Standard 100-1 Information Security Management Systems (ISMS), Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile&v=1. [Hozzáférés dátuma: 2017.03.31.].

[207] **Bundesamt für Sicherheit in der Informationstechnik (BSI)**, „BSI-Standard 100-2: IT-Grundschutz Methodology," Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile&v=1 [Hozzáférés dátuma: 2017.03.31.].

[208] **Federal Office for Information Security (BSI)**, „Secure Connection of Local Networks to the Internet v1.0 (ISi-Check), Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/InternetSecurity/ISi-LANA-ISi-Check.pdf?__blob=publicationFile&v=1. [Hozzáférés dátuma: 2017.03.31.]

[209] **Pilar-tools**, Risk Analysis and Management Additional Tools Help Files, Elérhető: http://www.pilar-tools.com/doc/rmat/v55/help_en_e_2017-01-02.pdf. [Hozzáférés dátuma: 2017.03.31.].

[210] **Hendershott Consulting Inc**, Overview of the ITIL v3 Library, Elérhető: http://www.hci-itil.com/ITIL_v3/images/service_improvement_ch7_fig_7_1.jpg. [Hozzáférés dátuma: 2017.03.31.].

[214] **Szegedi Egyetem,** Kombinatorika elemei / Kombinatorika előadás, 2015/2016 ősz, Elérhető: http://www.math.u-szeged.hu/~ngaba/kombi_ea_old/index.html. [Hozzáférés dátuma: 2017.03.31.].

[223] **MuxViz**, Elérhető: http://muxviz.net/index.php. [Hozzáférés dátuma: 2017.03.31.].

IRODALOMJEGYZÉK

[211] **IT Governance Institute**, Office of Government Commerce, isaca.org, Elérhető: http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf. [Hozzáférés dátuma: 2017.03.31.].

[212] **Magyar Szabványügyi Testület**, Elérhető: http://www.mszt.hu/web/guest/msz-iso-iec-20000-1. [Hozzáférés dátuma: 2017.03.31.].

[213] **Galambos Gábor, Árgilán Viktor**, Matematika I., Elérhető: http://www.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0013_galambos_matematika_i/1010_hamilton_krutak.html. [Hozzáférés dátuma: 2017.03.31.].

[215] **Obádovics J. Gyula**, Valószínűségszámítás és Matematikai Statisztika, Budapest: SCOLAR KFT., 2009., ISBN: 978-963-244-067-5

[216] **Informatikai Tárcaközi Bizottság (ITB) 5. számú ajánlása** – Bevezetés a PRINCE projektirányítási módszertanba., Elérhető: http://www.ekk.gov.hu/hu/kib/archivum. [Hozzáférés dátuma: 2017.03.31.].

[217] **Symantec**, Internet Security Threat Report 2013, Elérhető: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf. [Hozzáférés dátuma: 2017.03.31.].

[218] **Karinthy Ferenc**, Láncszemek, Elérhető: http://mek.oszk.hu/07300/07367/html/01.htm#54. [Hozzáférés dátuma: 2017.03.31.].

[219] **Kaspersky**, Corporate threats, 2014., Elérhető: http://report.Kaspersky.com/#corporate-threats. [Hozzáférés dátuma: 2017.03.31.].

[220] **Crysys Lab**, miniduke, Elérhető: http://www.crysys.hu/miniduke/miniduke_indicators_public.pdf. [Hozzáférés dátuma: 2017.03.31.].

[221] **Mcafee**, Threats predictions, Elérhető: https://www.mcafee.com/ru/resources/reports/rp-threats-predictions-2016.pdf. [Hozzáférés dátuma: 2017.03.31.].

[222] **Milgram Stanley**, The Small World Problem, Psychology Today, New York, 1967. Elérhető: http://snap.stanford.edu/class/cs224w-readings/milgram67smallworld.pdf. [Hozzáférés dátuma: 2017.03.31.].

[224] **Pokorádi László**, Üzemeltetési folyamat gráfmodellezése, Elérhető: http://www.repulestudomany.hu/kulonszamok/2014_cikkek/2014-2-19-0114_Pokoradi_Laszlo.pdf. [Hozzáférés dátuma: 2017.03.31.].

[225] **Public Safety Canada**, Forging a Common Understanding for Critical Infrastructure, Elérhető: https://www.dhs.gov/sites/default/files/publications/critical-five-shared-. [Hozzáférés dátuma: 2017.03.31.].

[226] **Information Security Policy Council**, The Basic Policy of Critical Information Infrastructure Protection, Elérhető: http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf. [Hozzáférés dátuma: 2017.03.31.].

[227] **The National Cyber Security Centre**, Elérhető: https://www.ncsc.gov.uk/. [Hozzáférés dátuma: 2017.03.31.].

[228] **U.S. Department of Homeland**, Recommended Practice for Securing Control System Modems, Elérhető: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/RP_SecuringModems_S508C.pdf. [Hozzáférés dátuma: 2017.03.31.].

[229] **Deborah Housen-Courie - ATO Cooperative Cyber Defence Centre of Excellence**, National Cyber Security Organisation in the Israel, Elérhető: https://ccdcoe.org/sites/default/files/multimedia/pdf/IL_NCSO_final.pdf . [Hozzáférés dátuma: 2017.03.31.].

[230] **Mikk Raud - ATO Cooperative Cyber Defence Centre of Excellence**, China and Cyber: Attitudes, Strategies, Organisation, Elérhető: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf. [Hozzáférés dátuma: 2017.03.31.].

[231] **Bob Woolley**, Top 10 Mistakes in Data Center Operations: Operating Efficient and Effective Data Centers, Elérhető: http://www.apc.com/salestools/VAVR-

8RNGFT/VAVR-8RNGFT_R0_EN.pdf. [Hozzáférés dátuma: 2017.03.31.].

[232] **Nlyte**, The Nlyte Solution Suite, Elérhető: http://www.nlyte.com/. [Hozzáférés dátuma: 2017.03.31.].

[233] **Katharina Ziolkowski** - NATO CCD COE Publication, Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, Elérhető: https://ccdcoe.org/publications/books/Peacetime-Regime.pdf. [Hozzáférés dátuma: 2017.03.31.].

[234] **Fejér Tamás**, ORGANIGRAM készítés felsőfokon, Szervezettervezés org.manager szoftverrel, Elérhető: http://www.perbithr.hu/share/HPSZ_10.02.ORG.pdf. [Hozzáférés dátuma: 2017.03.31.].

[235] **Eric Luiijf, Bert Jan te Paske**, Cyber Security of Industrial Control Systems, Elérhető: http://publications.tno.nl/publication/34616507/KkrxeU/%20luiijf-2015-cyber.pdf. [Hozzáférés dátuma: 2017.03.31.].

[236] **Laurent Lessard**, Optimal Control of Two-Player Systems With Output Feedback, IEEE TRANSACTIONS ON AUTOMATIC CONTROL, 60, pp. 2129-2144, 2015.

[237] **Information Security Policy Council- Government of JAPAN**, The Basic Policy of Critical Information Infrastructure Protection (3rd Edition), Elérhető: http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3_r1.pdf. [Hozzáférés dátuma: 2017.03.31.]

[238] **Ian Ellefsen, Sebastiaan Solms**, Implementing Critical Information Infrastructure Protection Structures in Developing Countries, Elérhető: https://hal.inria.fr/hal-01483817/document. [Hozzáférés dátuma: 2017.03.31.].

[239] **Federal Office for Information Security (BSI)**, Open Platform Communications Unified Architecture Security AnalysisOpen Platform Communications Unified Architecture Security Analysis, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/OPCUA/OPCUA.pdf?__blob=publicationFile&v=2. [Hozzáférés dátuma: 2017.03.31.].

[240] **Federal Office for Information Security (BSI)**, The State of IT Security in Germany 2016, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2016.pdf?__blob=publicationFile&v=3. [Hozzáférés dátuma: 2017.03.31.].

[241] **Federal Office for Information Security (BSI)**, Cloud Computing Compliance Controls Catalogue, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/ComplianceControlsCatalogue.pdf?__blob=publicationFile&v=4. [Hozzáférés dátuma: 2017.03.31.].

[242] **Federal Office for Information Security (BSI)**, ICS Security Compendium, Elérhető: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.pdf?__blob=publicationFile&v=3. [Hozzáférés dátuma: 2017.03.31.].

[243] **Sistema di informazione per la sicurezza della Repubblica**, 7 Law No. 124/2007, Elérhető: http://www.sicurezzanazionale.gov.it/sisr.nsf/english/law-no-124-2007.html#_ftn10. [Hozzáférés dátuma: 2017.03.31.].

[244] **BBC, „BBC NEWS technology**, Elérhető: http://www.bbc.co.uk/news/technology-15844230. [Hozzáférés dátuma: 2017.03.31.].

[245] **Budafok-Tétény Polgármesteri Hivatal**, Folyamatelemzést és modellezést támogató szoftveralkalmazási javaslat, Elérhető: http://www.etudasportal.gov.hu/download/attachments/17039444/19.+Folyamatelemz%C3%A9st+%C3%A9s+modellez%C3%A9st+t%C3%A1mogat%C3%B3+szoftverjavaslat.pdf. [Hozzáférés dátuma: 2017.03.31.].

[246] **Balogh Sándor**, Logikai elemek és kapcsolások \ gráfelméleti alapfogalmak, Beregszász: Kárpátaljai Magyar Pedagógusszövetség Tankönyv- és Taneszköztanácsa, 2004. Elérhető: http://mek.oszk.hu/02900/02901/02901.pdf. [Hozzáférés dátuma: 2017.03.31.].

[247] **Presidency of the Council of Ministers**, National strategic framework for cyberspace security, Elérhető: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf. [Hozzáférés dátuma: 2017.03.31.].

[248] **Presidency of the Council of Ministers**, The national plan for cyberspace protection and ict security, Elérhető: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf. [Hozzáférés dátuma: 2017.03.31.].

8 Publikációk

8.1 A tézispontokhoz kapcsolódó tudományos közlemények

1 Puskás Béla
Integrált felügyeleti rendszer
HADMÉRNÖK XII:(1) pp. 268-277. (2017)

2 Puskás Béla
Információbiztonsági környezet kialakítása
HÍRVILLÁM = SIGNAL BADGE 6/2: pp. 108-133. (2015)

3 Zoltán Rajnai, Béla Puskás
Requirements of the installation of the critical informational infrastructure and its management
INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS 13:(1) pp. 48-56. (2015)

4 Rajnai Zoltán, Puskás Béla
Decision-making support software application option for critical informational infrastructures
ACTA TECHNICA CORVINIENSIS – BULLETIN OF ENGINEERING 2015:(4) pp. 89-94. (2015)

5 Puskás Béla
Kritikus Információs Infrastruktúrák modellezése
FELDERÍTŐ SZEMLE 13/3: pp. 95-107. (2014)

6 Puskás Béla
Kritikus információs infrastruktúrák biztonsága, sérülékenysége
SZAKMAI SZEMLE: A KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT TUDOMÁNYOS-SZAKMAI FOLYÓIRATA 1: pp. 126-149. (2013)

7 Puskás Béla
Az informatikai rendszerek és a jogi környezet változásai
HÍRVILLÁM = SIGNAL BADGE 2: pp. 97-107. (2013)

8.2 További tudományos közlemények

1 Puskás Béla, Dr. Magyar Sándor, Holtai András
Az informatikai fejlesztés és üzemeltetés határvonalai
FELDERÍTŐ SZEMLE 15/1: pp. 191-203. (2016)

2 Puskás Béla, Dr. Magyar Sándor, Holtai András
Az informatikai üzemeltetés általános kérdései
FELDERÍTŐ SZEMLE 14/4: pp. 91-102. (2015)

3 Puskás Béla
Kritikus Információs Infrastruktúrák hálózatelméleti megközelítésből
In: Rajnai Zoltán, Fregan Beatrix, Ozsváth Judit (szerk.)
Az 5. Báthory-Brassai Konferencia tanulmánykötetei. 709 p.
Konferencia helye, ideje: Budapest, Magyarország, 2014.05.21-2014.05.22. Budapest: Óbudai Egyetem Biztonságtudományi Doktori Iskola, 2014. pp. 438-443.
1-2. köt. (ISBN:978-615-5460-38-8)

4 Puskás Béla
Supporting the operation of critical information infrastructures
TRADECRAFT REVIEW PERIODICAL OF THE SCIENTIFIC BOARD OF MILITARY SECURITY OFFICE (2012-2014) 2013/1: pp. 110-118. (2013)

5 Puskás Béla
The risks of networks' complexity
HÍRVILLÁM = SIGNAL BADGE 1: pp. 11-16. (2013)

6 Puskás Béla
Dr Fregan Beatrix (szerk.)
Kockázatelemzés, kockázatértékelés: Informatikai üzemeltetés során fellépő kockázatok értékelése
Budapest: Óbudai Egyetem, 2013. 207 p.
(ISBN:978-615-5018-98-5)

7 Puskás Béla
The risks of networks’ complexity
HADMÉRNÖK VII:(4) pp. 167-171. (2012)

8 Puskás Béla
Hálózatelméleti alapok
Haditechnika-Kommunikáció 2012: nemzetközi szakmai-tudományos konferencia.
Konferencia helye, ideje: Budapest, Magyarország, 2012.11.15pp. 1-12.

9 Puskás Béla
A hamis biztonságérzet kialakulásának megelőzése az informatikai rendszerek üzemeltetése során
Haditechnika-Kommunikáció 2012: nemzetközi szakmai-tudományos konferencia.
Konferencia helye, ideje: Budapest, Magyarország, 2012.11.15pp. 1-15.