ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS TÉZISFÜZETE

VÁCZI DÁNIEL

Kiberbiztonsági humán kockázati matematikai modell szenzitív digitális információszivárgás potenciáljának mérésére

Témavezető: Dr. habil. Szádeczky Tamás

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2021. 09. hónap 27. nap

TARTALOMJEGYZÉK

1 SUMMARY

In general, cybersecurity is a complex area based on risk management, which includes not only IT and information security, but also the proper management of the related legal, social and economic processes.

In many cases, the human factor has played a crucial role in the various successful cyberattacks on organisations. There is still no common methodology for determining this risk factor, as it is not trivial. The reason is that human beings are complex and individuals are very different from each other. For this reason, the identification of individuals at risk from a cyber security perspective is currently tentative and not based on data supported by concrete calculations. Moreover, in the absence of an appropriate methodology, the energy invested is not commensurate with the usability of the result, which is unlikely to be a good approximation of reality. However, it is useful to know which employees need more attention.

I conducted literature research in psychology, sociology, crime and cybersecurity, a questionnaire survey and in-depth interviews to identify and structure risk factors that could have an impact on digital information leakage. These risk factors became the inputs of a hierarchical fuzzy model. I defined membership functions and rules separately each model using MatLab Fuzzy Toolbox and then I built the whole structure in MatLab SimuLink. As an output, the system can measure the risk level of an individual employee. Combining its result with the regularities of network theory makes a much more efficient methodology as I wrote in the fourth chapter.

To validate the model I have created three case studies where I could show how the system works. The MatLab files of the model can be downloaded as described in the first appendix of the thesis. The system can be further developed based on the risk tolerance and characteristics of the current organisation.

My research can be used to address the human risks of cybersecurity, including the threat of digital information leakage, in organisations and critical infrastructures where the employer has sufficient quantity and quality of information and a sufficiently large pool of employees. The created model can help the security team and the management to make the right risk-reducing decisions.

2 A KUTATÁS ELŐZMÉNYEI

Az alap- és mesterképzésben eltöltött tanulmányaim és tudományos tevékenységem során mindig is kiemelt figyelmet fordítottam az informatika- és információbiztonság területeinek megismerésére, azon belül is az emberi tényező veszélyeinek feltárására. Tudományos kíváncsiságom arra motivált, hogy számos elméleti kutatást végezzek ezen a területen, és különböző célirányos gyakorlati feladatot hajtsak végre. Az üzleti életben szerzett szakmai tanácsadói és cégvezetői tapasztalataim megerősítettek abban, hogy a humán faktor kockázatainak megismerése a kiberbiztonság területén egy olyan fennálló probléma, amelynek kezelésére nagy szükség van.

A különböző nemzetközi és hazai ajánlások, szabványok és jogszabályok mind kitérnek arra, hogy a biztonság növelése érdekében nem csak technikai fejlesztésekre van szükség, hanem az emberi tényezőből fakadó kockázatot is csökkenteni kell. A kiber-ellenállóképesség egyik fontos dokumentuma az Amerikai Egyesült Államokban működő ASPENS által kiadott A National Cybersecurity Agenda for Resilient Digital Infrastructure[1] c. kiadvány. Ez a dokumentum ajánlást tesz az adott elnöki ciklus legfontosabb kiberbiztonsági fejlesztési területeire vonatkozóan. A legfrissebb, 2020. decemberi kiadványukban az öt javasolt célkitűzés közül első helyen az oktatást és a munkaerő fejlesztését emelték ki.

A megfogalmazott célok között szerepel a technikai szakemberek foglalkoztatása mellett minél több terület bevonása a megfelelő védelem kialakítása érdekében. Jól látszik, hogy az emberi tényező kezelése nemzetközileg is egyre nagyobb prioritásúvá válik, ráadásul a kiber-ellenállóképesség a digitálisan függő szervezetek életében már nem csak a szűk biztonsági szakember munkáján múlik, hanem a teljes munkaerő felkészültségén. Ezt a felkészültséget az erőforrások optimalizálása érdekében tervezett módon szükséges fejleszteni, melynek alapja egy megfelelő kockázatszámítási módszertan.

[1] A cím tükörfordításban a következő: Az ellenálló digitális infrastruktúra nemzeti kiberbiztonsági menetrendje

3 CÉLKITŰZÉSEK

A kutatásom célja az, hogy a piacon megjelenő valós igényekre megoldást találjak tudományos munka segítségével. Az emberi tényező különböző aspektusait figyelembe véve létrehoztam egy olyan egzakt matematikai modellt és módszertant, melyet magukra szabva és alkalmazva a szervezetek – a megfelelő információk birtokában – meg tudják határozni a kiberbiztonsági szempontból kockázatos személyeket. Az eredményeket felhasználva célzottan lehet a munkavállalók biztonságtudatosságát, kiber-higiéniáját növelni. A modell használata által kapott eredményeket a képzésen kívül a valós számszerű adatok segítségével az üzleti oldal is felhasználhatja újabb biztonsági kontrollok bevezetésére, a régiek optimalizálására, illetve adott esetben a kockázatok felvállalására.

Értekezésemben a kiberbiztonsági fenyegetettségek közül a szándékos vagy gondatlan módon elkövetett minősített digitális információszivárgást vizsgálom a modell működésének könnyebb érthetőség miatt. A modellalkotás során e speciális fenyegetettségre fókuszálva a hálózatkutatás területét és a fuzzy logika alkalmazását együttesen alkalmaztam a szervezeten belüli kockázatelemzés elősegítése érdekében.

4 VIZSGÁLATI MÓDSZEREK

Kutatásom alapját a fuzzy logika és a hálózatelemzés módszereinek vizsgálata, valamint a humán faktor kiberbiztonsági aspektusainak tanulmányozása adta. Értekezésem elkészítése céljából irodalomkutatást végeztem kiberbiztonsági, pszichológiai, matematikai (fuzzy logika, hálózatkutatás), szociológiai, kriminalisztikai területeken, illetve áttekintettem a vonatkozó jogszabályokat, ajánlásokat és szabványokat. A hiányzó információk elérése érdekében mélyinterjúkat készítettem, és egy specifikus kérdőíves kutatást is végrehajtottam.

A két matematikai módszer pozitív tulajdonságait kihasználva alkottam meg az emberi kockázat vizsgálására alkalmas modellt, ahol az egymásba ágyazott fuzzy rendszerek kimeneti értéke határozza meg az élek száma mellett a hálózat pontjainak súlyát. A modellek elkészítéséhez a MatLab R2020a-t, illetve a Fuzzy Logic Toolboxot és a Simulink kiegészítőket használtam. A fuzzy modell bemeneteit képző kockázati tényezőkön tartalmi szempontból rendezést végeztem és külön-külön tagsági függvényeket határoztam meg.

A kérdőíves kutatás során statisztikai módszerekkel állapítottam meg a számmal jellemezhető értékeket, illetve a speciális szövegkijelölést igénylő kérdéseknél egyesével elemeztem a válaszok gyakoriságát.

5 ÚJ TUDOMÁNYOS EREDMÉNYEK

Az értekezésem új tudományos eredményeit az alábbi tézisek tartalmazzák:

1. Meghatároztam azokat a kockázati tényezőket, amelyek nagy valószínűséggel befolyásolják azt, hogy digitális minősített információt szivárogtasson ki egy személy.

Az értekezés 2.1. fejezetében ismertetett különböző kiberbiztonsági, szociológiai, pszichológiai irodalmak és a lefolytatott mélyinterjúk, valamint a 2.2. fejezetben elemzett kérdőív alapján megállapítottam, hogy jól körülírható azoknak a különböző kockázati tényezőknek a köre, amelyek befolyásolják azt, hogy egy személy gondatlanságból vagy szándékosan szenzitív információt szivárogtat ki egy szervezetből. Ezeket a 3. fejezetben rendszereztem, illetve indokoltam fontosságukat. Mivel ezek nem egyszerű crisp (szám) értékek, hanem a köznyelvben használatos szavakkal jellemezhető értékek, ezért mindegyik tényezőhöz fuzzy tagsági függvényeket rendeltem.

2. Megalkottam egy olyan fuzzy modellt, amelyet alkalmazva a megfelelő információk (bemenetek) ismeretében megsejthető, hogy mely személyek jelentenek kockázatot a szervezeten belül az információszivárogtatást, mint fenyegetettséget figyelembe véve egy célzott támadás esetén.

A MatLabban létrehoztam egy olyan specifikus különböző fuzzy rendszereket egymásba ágyazott rendszert, amely bemeneti értékeit az értekezés 3. fejezetében leírtak szerint alkalmazva valóságot megközelítő eredményt ad. A 4. fejezetben ismertetett modell kimenete a kérdőíves kutatásom során megadott válaszokkal összhangban vannak, melyet három esettanulmánnyal alátámasztottam. A modell kezeli az esetleges bizonytalanságokat. A bemenetek és a szabályok módosításával bármely szervezet alkalmazni tudja a saját kockázatvállalása és szabályzata alapján.

3. Megállapítom, hogy a hálózatelemzési módszerek és a fuzzy logika külön-külön is alkalmas a kockázatok mérésére, de együtt pontosabb eredményt adnak. Együttes alkalmazásukra létrehoztam egy modellt a kiberbiztonsági szempontból kockázatos személyek beazonosítását figyelembe véve.

A szakirodalom feldolgozása alapján megvizsgáltam a hálózatelemzési módszerek és a fuzzy logika szabályszerűségeit és azok együttes használatának lehetséges módját. A

fuzzy logika alkalmazhatóságát az értekezés 2.4 fejezetében ismertettem, míg a hálózatelméletét a 2.5 fejezetében. Együttes alkalmazásukat a 4. fejezetben fejtettem ki.

6 AZ EREDMÉNYEK HASZNOSÍTÁSI LEHETŐSÉGEI

Kutatásaim elsősorban olyan szervezetek, kritikus infrastruktúrák kiberbiztonsági, azon belüli is a digitális információszivárgás fenyegetettségének humán kockázatainak kezelésére alkalmazhatók, ahol megfelelő mennyiségű és minőségű információ áll a munkáltató részére, és kellően nagy a munkavállalók köre.

A rendszert általánosan azonban minden magán- és állami intézmény profiltól függetlenül használhatja a kockázatai kezelésének csökkentése, hiszen a fuzzy logika képes kezelni a rendelkezésre nem álló információkat. Amennyiben az adott szervezet létszáma nem éri el a kritikus tömeget, ahol van értelme a hálózati összefüggések elemzésének, ott csak a fuzzy értékek meghatározása is segíthet a döntéshozóknak.

7 IRODALOMJEGYZÉK

[1] K. Fehér, *Digitalizáció és új média*. Budapest: Akadémiai Kiadó, 2016.

[2] „CYBERCRIME: COVID-19 IMPACT”. INTERPOL General Secretariat, 0 2020.

[3] *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról - Hatályos Jogszabályok Gyűjteménye*. Elérés: aug. 16, 2020. [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1300050.tv

[4] *Magyarország Nemzeti Kiberbiztonsági Stratégiájáról*. 2013. Elérés: aug. 16, 2020. [Online]. Elérhető: http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845

[5] *A hálózati és információs rendszerek biztonságára vonatkozó Stratégia*. 2018. [Online]. Elérhető: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf?fbclid=IwAR1kVfAyc8Ro6kYyKaQbBS6wY_mgE-Iq6bqhtAKk8zjsZZjPwlZoP8PbxA8#!DocumentBrowse

[6] ISACA, „The Business Model for Information Security”. ISACA, 2010.

[7] Y. K. Dwivedi *és mtsai.*, „Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life”, *International Journal of Information Management*, o. 102211, júl. 2020, doi: 10.1016/j.ijinfomgt.2020.102211.

[8] „A National Cybersecurity Agenda for Resilient Digital Infrastructure”. Aspen Cybersecurity Group, 2020. Elérés: jan. 05, 2021. [Online]. Elérhető: https://www.aspeninstitute.org/wp-content/uploads/2020/12/FINAL-Aspen-Natl-Cybersecurity-Agenda-Dec-2020.pdf

[9] P. Fehér-Polgár és P. Michelberger, „The Information Security Risks of the BYOD, From Theoretical Point of View”, in *2019 IEEE 17th International Symposium on Intelligent Systems and Informatics (SISY)*, szept. 2019, o. 83–88. doi: 10.1109/SISY47553.2019.9111514.

[10] A. Keszthelyi, „Paradigmaváltás - biztonság - emberi tényező”, *TAYLOR: GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT: A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI*, köt. 7, o. 406–412, 2015.

[11] N. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, 1. Cambridge: Techlology Press, 1948.

[12] C. E. Shannon, „A mathematical theory of communication”, *The Bell System Technical Journal*, köt. 27, sz. 3, o. 379–423, júl. 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.

[13] G. Fülöp, *Az információ*, 2. bővített és Átdolgozott kiadás. Budapest: Eötvös Loránd TudományegyetemKönyvtártudományi - Informatikai Tanszék, 1996. Elérés: jan. 20, 2021. [Online]. Elérhető: https://mek.oszk.hu/03100/03118/03118.pdf

[14] J. De Vriendt, P. Laine, C. Lerouge, és Xiaofeng Xu, „Mobile network evolution: a revolution on the move”, *IEEE Commun. Mag.*, köt. 40, sz. 4, o. 104–111, ápr. 2002, doi: 10.1109/35.995858.

[15] A. Tóth, „A felhőinformatika alapjai”, *HÍRVILLÁM = SIGNAL BADGE*, köt. 2, o. 85–90, 2011.

[16] Gottdank T., *Szolgáltatásalapú világ*. Bicske: SZAK Kiadó, 2013.

[17] Mayer-Schönberger V. és Kenneth Cukier, *Big Data*. Budapest: HVG Kiadó Zrt., 2014.

[18] M. Klausz, *Megosztok, tehát vagyok*. Budapest: Antheneum Kiadó, 2017.

[19] D. Z. H. Marquardt Madeline, „Cognitive Ability and Vulnerability to Fake News”, *Scientific American*. https://www.scientificamerican.com/article/cognitive-ability-and-vulnerability-to-fake-news/ (elérés szept. 28, 2020).
[20] K. Fehér és O. Király, „Álhíresülés – a hamis hírek dinamikája a médiában”, *Századvég*, sz. 2017/2., o. 39–50, 2017.
[21] P. Bányász, L. Dobos, G. Palla, és P. Pollner, „Lélektani műveletek a közösségi médiában”, in *Hálózatok a közszolgálatban*, Á. Auer és T. Joó, Szerk. Budapest: Ludovika Egyetemi Kiadó, 2019, o. 111–133. [Online]. Elérhető: https://m2.mtmt.hu/api/publication/31012112
[22] „Russia-backed Facebook posts »reached 126m Americans« during US election”, *the Guardian*, okt. 31, 2017. http://www.theguardian.com/technology/2017/oct/30/facebook-russia-fake-accounts-126-million (elérés jan. 08, 2021).
[23] D. Váczi, Z. Bederna, V. Szalánczi-Orbán, és T. Szádeczky, „Az incidenskezelés szervezeti háttere”, in *Hálózatok a közszolgálatban*, Á. Auer és T. Joó, Szerk. Budapest: Ludovika Egyetemi Kiadó, 2019, o. 205–222. [Online]. Elérhető: https://m2.mtmt.hu/api/publication/31012112
[24] A. Tóth és P. Török, „IoT attacks and recommendation for protection solutions”, *AMERICAN JOURNAL OF RESEARCH EDUCATION AND DEVELOPMENT*, köt. 2019, o. 15–26, 2019.
[25] Z. Bederna, D. Váczi, T. Szádeczky, és P. Pollner, „Támadás hálózatba szervezve”, in *Hálózatok a közszolgálatban*, Á. Auer és T. Joó, Szerk. Budapest: Ludovika Egyetemi Kiadó, 2019, o. 223–247. [Online]. Elérhető: https://m2.mtmt.hu/api/publication/31012112
[26] Z. Bederna és T. Szádeczky, „Effects of botnets – a human-organisational approach”, *Security and Defence Quarterly*, júl. 2021, doi: 10.35467/sdq/138588.
[27] D. Váczi, „Célzott támadások módszertana”, in *Célzott kibertámadások*, 2018, o. 52–75.
[28] E. H. Spafford, „The internet worm program: an analysis”, *SIGCOMM Comput. Commun. Rev.*, köt. 19, sz. 1, o. 17–57, jan. 1989, doi: 10.1145/66093.66095.
[29] P. Szőr, *A vírusvédelem művészete*. Bicske: SZAK Kiadó, 2010.
[30] Z. Haig és I. Várhegyi, „A cybertér és a cyberhadviselés értelmezése”, *HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA*, sz. Eleektronikus szám, 2008, Elérés: jan. 10, 2021. [Online]. Elérhető: http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf
[31] Európai Tanács, „Convension on Cybercime”, *Treaty Office*. https://www.coe.int/en/web/conventions/full-list (elérés jan. 10, 2021).
[32] P. Tálas, „A varsói NATO-csúcs legfontosabb döntéseiről”, *NEMZET ÉS BIZTONSÁG: BIZTONSÁGPOLITIKAI SZEMLE*, sz. 2, o. 97–101, 2016.
[33] C. Fekete és Z. Sipos, „A kibertér megjelenése az orosz katonai műveletekben a 2008-as orosz–grúz háború tükrében”, *HONVÉDSÉGI SZEMLE: A MAGYAR HONVÉDSÉG KÖZPONTI FOLYÓIRATA*, sz. 145, o. 59–71, 2017.
[34] L. Kovács és M. Sipos, „A Stuxnet és ami mögötte van”, *HADMÉRNÖK*, köt. 5, o. 163–172, 2010.
[35] L. Kovács és M. Sipos, „A Stuxnet és ami mögötte van II.”, *HADMÉRNÖK*, köt. VI, o. 222–231, 2011.
[36] „ENISA Threat Landscape - The year in review”. https://www.enisa.europa.eu/publications/year-in-review (elérés dec. 28, 2020).
[37] K. Fehér, *Kezdő hackerek kézikönyve*. Budapest: BBS-INFO Kiadó, 2016.

[38] K. Finklea, „Dark Web”, Congressional Research Service, 10 2017. [Online]. Elérhető: https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf
[39] P. Warren és M. Streeter, *Az internet sötét oldala*. Budapest: HVG Kiadó Zrt., 2005.
[40] C. Krasznay, „A polgárok védelme egy kiberkonfliktusban”, *HADMÉRNÖK*, köt. 7, o. 142–151, 2012.
[41] C. Vida, „A hírszerzés szerepe, jelentősége, az információgyűjtés fajtái és formái”, in *Nemzetbiztonsági alapismeretek*, Budapest: Nemzeti Közszolgálati Egyetem, 2013, o. 102–105.
[42] H. Modderkolk, „Dutch agencies provide crucial intel about Russia’s interference in US-elections”, *de Volkskrant*, jan. 25, 2018. https://www.volkskrant.nl/gs-b4f8111b (elérés jan. 11, 2021).
[43] T. Szádeczky, „Terrorism in cyberspace”, 2008.
[44] P. Bányász, „Kiberbűnözés és közösségi média”, *NEMZETBIZT SZLE*, köt. 4, sz. 4, o. 55–74, 2017.
[45] M. Zerzri, „The Threat of Cyber Terrorism and Recommen-da-tions for Countermeasures”, *Cyber Terrorism*, sz. 04–2017, o. 6, 2017.
[46] Z. Haig, *Információs műveletek a kibertérben*. Dialóg Campus Kiadó, 2018.
[47] G. Berki, „Kiberháborúk, kiberkonfliktusok”, in *Műhelymunkák*, 2016, o. 245–284.
[48] H. Dalziel, „Cyber Kill Chain (Chapter 2)”, in *Securing Social Media in the Enterprise*, H. Dalziel, Szerk. Boston: Syngress, 2015, o. 7–15. doi: 10.1016/B978-0-12-804180-2.00002-6.
[49] C. Krasznay, „Kiberbiztonsági kihívások az ICS/SCADA világban”, *VÍZMŰ PANORÁMA: VÍZ- ÉS CSATORNAMŰVEK ORSZÁGOS SZAKMAI SZÖVETSÉGE LAPJA*, köt. XXVIII/2020., o. 2–5, 2020.
[50] X. Zhou, Z. Xu, L. Wang, K. Chen, C. Chen, és W. Zhang, „Kill Chain for Industrial Control System”, *MATEC Web of Conferences*, köt. 173, o. 01013, 0 2018, doi: 10.1051/matecconf/201817301013.
[51] R. Messier, *CEH v10 Certified Ethical Hacker Study Guide*. New York: John Wiley & Sons Inc, 2019.
[52] D. P. Twitchell, „Social engineering in information assurance curricula”, in *Proceedings of the 3rd annual conference on Information security curriculum development*, New York, NY, USA, szept. 2006, o. 191–193. doi: 10.1145/1231047.1231062.
[53] H. Cristopher, *Social Engineering - The scinece of Human Hacking*. Indianapolis: John Wiley & Sons, Inc., 2018.
[54] K. D. Mitnick, *A legendás hacker - A rábeszélés művészete*. Budapest: Perfact-Pro Kft., 2003.
[55] F. Schulz Von Thun, *A kommunikáció zavarai és feloldásuk*. Budapest: Háttér Kiadó, 2012.
[56] C. S. Carver és M. F. Scheir, *Személyiségpszichológia*. Budapest: Osiris Kiadó Kft., 2011.
[57] G. Csepeli, *Szociálpszichológia*. Budapest: Osiris Kiadó Kft., 2006.
[58] S. Klein, *Munkapszichológia - a 21. században*. Budapest: Edge 2000 Kft., 2018.
[59] „Pretexting: Your Personal Information Revealed”. Federal Trade Commission, Bureau of Consumer Protection, Office of Consumer and Business Education, 2001. [Online]. Elérhető: https://books.google.hu/books?id=fhETbHbsmKUC
[60] A. Demarais és V. White, *Első benyomás*. Budapest: HVG Kiadó Zrt., 2008.

[61] M. J. Horowitz, „Modes of Representation of Thought”, *J Am Psychoanal Assoc*, köt. 20, sz. 4, o. 793–819, okt. 1972, doi: 10.1177/000306517202000405.
[62] P. Ekman és W. V. Friesen, *Unmasking the Face: A Guide to Recognizing Emotions from Facial Clues*. ISHK, 2003.
[63] W. Glasser, *Choice Theory: A New Psychology Of Personal Freedom*. New York: HarperCollins Publishers, 1999.
[64] R. B. Cialdini, *Influence: The Psychology of Persuasion, Revised Edition*, Revised edition. New York: Harper Business, 2006.
[65] B. Annis és J. Gray, *Nemek intelligenciája*. Budapest: Trivium Kiadó, 2013.
[66] A. Keszthelyi, „Jelszavakról – iparági legrosszabb gyakorlatok”, *TAYLOR: GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT: A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI*, köt. 7, o. 261–268, 2015.
[67] A. Keszthelyi, „About passwords”, *ACTA POLYTECHNICA HUNGARICA*, köt. 10, o. 99–118, 2013, doi: 10.12700/APH.10.06.2013.6.6.
[68] K. Fehér, *Hackertechnikák*. Budapest: BBS-INFO Kiadó, 2018.
[69] P. J. Varga, „Az okos otthonok vezeték nélküli alkotóelemeinek biztonsága”, *KÖZTES EURÓPA: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI*, köt. 9, o. 83–87, 2017.
[70] Z. Rajnai, „A kritikus információs infrastrukturák összetétele, biztonsági kérdései”, in *Nemzetközi Gépész és Biztonságtechnikai Szimpózium*, 2012, o. 15–22.
[71] „AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/ 679 RENDELETE - (2016. április 27.) - a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/ 46/ EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)”, o. 88.
[72] Horváth A., „A kritikus infrastruktúra védelem komplex értelmezésének szükségessége”, in *Fejezetek a kritikus infrastruktúra védelemből*, Budapest: Magyar Hadtudományi Társaság, 2013, o. 18–37. [Online]. Elérhető: http://mhtt.eu/hadtudomany/KIV_tanulmanykotet.pdf
[73] *UNITING AND STRENGTHENING AMERICA BYPROVIDING APPROPRIATE TOOLS REQUIREDTO INTERCEPT AND OBSTRUCT TERRORISM(USA PATRIOT ACT) ACT OF 2001*. Elérés: jan. 11, 2021. [Online]. Elérhető: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf
[74] *Critical Infrastructure Protection (PDD 63)*. Elérés: jan. 11, 2021. [Online]. Elérhető: https://fas.org/irp/offdocs/pdd/pdd-63.htm
[75] T. Szádeczky, „Information Security Law and Strategy in Hungary”, *Academic and Applied Research in Military and Public Management Science (AARMS) HU ISSN 2498-5392*, köt. 14, o. 281–289, 0 2015.
[76] *A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (EGT-vonatkozású szöveg)*, köt. OJ L. 2008. Elérés: jan. 11, 2021. [Online]. Elérhető: http://data.europa.eu/eli/dir/2008/114/oj/hun
[77] Z. Haig, B. Hajnal, L. Kovács, L. Muha, és Z. N. Sik, *A kritikus információs infrastruktúrák meghatározásának módszertana*. ENO Advisory Kft., 2009.
[78] *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról,kijelöléséről és védelméről*. Elérés: jan. 11, 2021. [Online]. Elérhető: https://net.jogtar.hu/getpdf?docid=a1200166.tv&targetdate=20180101&printTitle=2012.+%C3%A9vi+CLXVI.+t%C3%B6rv%C3%A9ny

[79] W. K. H. Kft, *65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról - Hatályos Jogszabályok Gyűjteménye*. Elérés: jan. 24, 2021. [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a1300065.kor

[80] M. Lajos, *A kritikus információs infrastruktúrák védelme*. Budapest: RelNet Technológia Kft., 2015. [Online]. Elérhető: http://real.mtak.hu/78935/1/A_kritikus_informacios_infrastrukturak_vedelme_u.pdf

[81] International Telecommunication Union, „Measuring digital developmentFacts and figures 2020". 2020. Elérés: jan. 17, 2021. [Online]. Elérhető: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf

[82] K. M. Stine, K. Quill, és G. A. Witte, „Framework for Improving Critical Infrastructure Cybersecurity". febr. 19, 2014. Elérés: jan. 24, 2021. [Online]. Elérhető: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity

[83] C. Krasznay, „Kiberbizonytalanság – A NATO szerepe a kibervédelemben", *FÓKUSZBAN*, köt. 2019, o. 54–59, 2019.

[84] S. Tamás, „Governmental Regulation of Cybersecurity in the EU and Hungary after 2000", *AARMS – Academic and Applied Research in Military and Public Management Science*, köt. 19, sz. 1, Art. sz. 1, okt. 2020, doi: 10.32565/aarms.2020.1.7.

[85] „1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról". http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845 (elérés jan. 18, 2021).

[86] W. K. H. Kft, *271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól - Hatályos Jogszabályok Gyűjteménye*. Elérés: jan. 18, 2021. [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=A1800271.KOR

[87] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, köt. OJ L. 2016. Elérés: jan. 18, 2021. [Online]. Elérhető: http://data.europa.eu/eli/dir/2016/1148/oj/eng

[88] Anita T., „A magyar kibervédelemmel kapcsolatos szabályozás aktuális kérdései", in *Kritikus Információs Infrastruktúrák Védelme*, Deák V., Szerk. Budapest: Nemzeti Közszolgálati EgyetemKözigazgatási Továbbképzési Intézet, 2019, o. 8–34. [Online]. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/13803/Kritikus%20informacios%20infrastrukturak%20vedelme_Eves%20tovabbkepzes_felelos%20szemely.pdf;jsessionid=8F44F5B1C47A4BD15D3EAB06068234DC?sequence=3&fbclid=IwAR0QR_CVd0l9pB3rRLcwVnhIkiZajGJH3vyciCBvtEWi9sZSHlnhCJPB7lM

[89] ENISA, „Részletes leírás a CSIRT-csoportok létrehozásáról". 2006. [Online]. Elérhető: file:///C:/Users/User/AppData/Local/Temp/CSIRT_setting_up_guide_ENISA-HU.pdf

[90] L. Kovács, *A kibertér védelme*. Dialóg Campus Kiadó; Nordex Kft., 2018.

[91] Z. Haig, *Információ - Társadalom - Biztonság*. Budapest: NKE Szolgál-tató Kft., 2015.

[92] C. Krasznay, „A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban", *NEMZET ÉS BIZTONSÁG: BIZTONSÁGPOLITIKAI SZEMLE*, köt. 10, o. 38–53, 2017.

[93] J. Dykstra és C. L. Paul, „Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations”, előadás 11th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 18), 2018. Elérés: jan. 24, 2021. [Online]. Elérhető: https://www.usenix.org/conference/cset18/presentation/dykstra

[94] W. K. H. Kft, „2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról - Hatályos Jogszabályok Gyűjteménye”. https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (elérés jan. 24, 2021).

[95] K. D. Mitnick és W. L. Simon, *A legendás hacker - A megtévesztés művészete*. Budapest: Perfact-Pro Kft., 2003.

[96] J. Beinschróth, „Informatikai biztonsági szabványok”, 2007.

[97] T. Dezső és I. Kertész, „Információszerzés az ókorban”, in *A hírszerzés története az ókortól napjainkig*, J. Boda és K. Regényi, Szerk. Budapest: Dialóg Campus Kiadó, 2019. Elérés: jan. 20, 2021. [Online]. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12692/web_PDF_Hirszerzes_tortenete_okortol_napjainkig.pdf?sequence=1

[98] J. Boda és K. Regényi, „Középkor – A klasszikus hírszerzés hajnala”, in *A hírszerzés története az ókortól napjainkig*, J. Boda és K. Regényi, Szerk. Budapest: Dialóg Campus Kiadó, 2019. Elérés: jan. 20, 2021. [Online]. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12692/web_PDF_Hirszerzes_tortenete_okortol_napjainkig.pdf?sequence=1

[99] C. Vida, P. Balogh, és J. Kis-Benedek, „A hírszerzés önálló ágai”, in *Nemzetbiztonsagi alapismeretek*, I. Kobolka, Szerk. Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó, 2013. Elérés: jan. 20, 2021. [Online]. Elérhető: https://cmsadmin-pub.uni-nke.hu/document/nbi-uni-nke-hu/nemzetbiztonsagi-alapismeretek.original.pdf

[100] J. Beinschróth, *Kriptográfiai alkalmazások, rejtjelezések, digitális aláírás, digitális pénz*. 2016.

[101] P. Hudoba, „Public key cryptography based on the clique and learning parity with noise problems for post-quantum cryptography”, *Proceedings of the 11th Joint Conference on Mathematics and Computer Science*, o. 102–112, 2018.

[102] *2009. évi CLV. törvény a minősített adat védelméről - Hatályos Jogszabályok Gyűjteménye*. Elérés: jan. 24, 2021. [Online]. Elérhető: https://net.jogtar.hu/jogszabaly?docid=a0900155.tv

[103] *2011/292/EU A TANÁCS HATÁROZATA (2011. március 31.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról*. Elérés: febr. 12, 2021. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32011D0292&from=EN

[104] Z. Kuris és Z. Faggyas, „Minősített adatokat kezelő informatikai rendszerek kockázatértékelése és kockázatmenedzsmentje”, *HADMÉRNÖK*, sz. VI./3., o. 117–130, 2011.

[105] P. Papadimitriou és H. Garcia-Molina, „A Model for Data Leakage Detection”, előadás 25th International Conference on Data Engineering, Shanghai, China, 2009. Elérés: febr. 11, 2021. [Online]. Elérhető: http://ilpubs.stanford.edu:8090/886/

[106] D. Vaczi, E. Toth-Laufer, és T. Szadeczky, „Fuzzy-based Cybersecurity Risk Analysis of the Human Factor from the Perspective of Classified Information Leakage”, in *2020 IEEE 18th International Symposium on Intelligent Systems and Informatics (SISY)*, szept. 2020, o. 000113–000118. doi: 10.1109/SISY50555.2020.9217053.

[107] B. Schneier, *Schneier a biztonságról*. Budapest: HVG Kiadó Zrt., 2010.
[108] I. Ajzen, „The theory of planned behavior”, *Organizational Behavior and Human Decision Processes*, köt. 50, sz. 2, o. 179–211, 0 1991, doi: 10.1016/0749-5978(91)90020-T.
[109] Hunyadi G. és Münnich Á., „A szilárd erkölcsiség elvárása a rendvédelemben: egy lehetséges pszichológiai modell”, *Belügyi Szemle*, köt. 64, sz. 6, Art. sz. 6, jún. 2016, doi: 10.38146/BSZ.2016.6.2.
[110] M. Walter, *Personality and Assessment*. Wiley, 1968.
[111] A. W. Wicker, „Attitudes versus Actions: The Relationship of Verbal and Overt Behavioral Responses to Attitude Objects”, *Journal of Social Issues*, köt. 25, sz. 4, o. 41–78, 1969, doi: https://doi.org/10.1111/j.1540-4560.1969.tb00619.x.
[112] Hunyadi G., Malét-Szabó E., és Münnich Á., „A rendvédelmi szervek szervezeti normáinak és kultúrájának, mint a szilárd erkölcsiség egyik alapvető háttértényezőjének empirikus próbavizsgálata”, 2016, [Online]. Elérhető: http://www.bm-tt.hu/assets/letolt/kutat/2016/SZEM.kulktura.tanulmany.pdf
[113] P. Csató, G. Hunyadi, E. Malét-Szabó, és Á. Münnich, *Az erkölcsi értékrend és a személyiség közötti kapcsolat vizsgálati szempontjai*. Budapest: Crew Kft, 2015. Elérés: márc. 07, 2021. [Online]. Elérhető: https://bmprojektek.kormany.hu/download/5/0a/51000/Az%20erk%C3%B6lcsi%20%C3%A9rt%C3%A9krend%20%C3%A9s%20a%20szem%C3%A9lyis%C3%A9g%20k%C3%B6z%C3%B6tti%20kapcsolat.pdf?fbclid=IwAR1HlU1A5XVJ3ufU1toGW1tM3sJPM-tD4z8KN__c5T8BoceAgVP7E4wnlPQ
[114] C.-H. S. Lin és C.-F. Chen, „Application of Theory of Planned Behavior on the Study of Workplace Dishonesty”, előadás 2010 International Conference on Economics, Business and Management, Manila, Philippines, 2010. [Online]. Elérhető: http://www.ipedr.com/vol2/14-P00029.pdf
[115] W. K. H. Kft, „1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról - Hatályos Jogszabályok Gyűjteménye”. https://net.jogtar.hu/jogszabaly?docid=99500125.tv (elérés ápr. 04, 2021).
[116] „Nemzetbiztonsági ellenőrzés - NBF”. https://www.nbf.hu/hasznos-informaciok/nemzetbiztonsagi-ellenorzes/ (elérés febr. 28, 2021).
[117] F. Z. Gozon, E. Laufer, és D. Váczi, „Fuzzy-based Human Factor Centered Cybersecurity Risk Assessment”, *Proc. of the IEEE 19th International Symposium on Intelligent Systems and Informatics*, 2021. (Megjelenés alatt.)
[118] E. Laufer, T. Szadeczky, és D. Váczi, „Human risk factors to measure the potential of digital information leakage”, *Biztonságtudományi Szemle*, sz. III. évf. 3. szám, o. 55–65.
[119] J. Beinschróth, *A kockázatok kezelése, védelmi intézkedések*. 2018.
[120] Z. Horváth, „A kockázatmenedzsment információbiztonsági kérdései”, *MINŐSÉG ÉS MEGBÍZHATÓSÁG*, köt. 50, o. 148–156, 2016.
[121] L. Kovács, *Kiberbiztonság és -stratégia*. Dialóg Campus Kiadó - Nordex Kft, 2018.
[122] S. C. Patel, J. H. Graham, és P. A. S. Ralston, „Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements”, *International Journal of Information Management*, köt. 28, sz. 6, o. 483–491, 0 2008, doi: 10.1016/j.ijinfomgt.2008.01.009.
[123] K. Hiromitsu és H. Ernest J., *Probabilistic Risk Assessment and Management for Engineers and Scientists*, 2. kiadás. Wiley-IEEE Press, 2000. Elérés: márc. 07, 2021. [Online]. Elérhető: https://ieeexplore.ieee.org/book/5264399

[124] P. A. S. Ralston, J. H. Graham, és J. L. Hieb, „Cyber security risk assessment for SCADA and DCS networks”, *ISA Transactions*, köt. 46, sz. 4, o. 583–594, okt. 2007, doi: 10.1016/j.isatra.2007.04.003.
[125] H. Al-Khateeb, G. Epiphaniou, A. Reviczky, P. Karadimas, és H. Heidari, „Proactive Threat Detection for Connected Cars Using Recursive Bayesian Estimation”, *IEEE Sensors Journal*, köt. 18, sz. 12, o. 4822–4831, 2018, doi: 10.1109/JSEN.2017.2782751.
[126] M. M. Silva, A. P. H. de Gusmão, T. Poleto, L. C. e Silva, és A. P. C. S. Costa, „A multidimensional approach to information security risk management using FMEA and fuzzy theory”, *International Journal of Information Management*, köt. 34, sz. 6, o. 733–740, 0 2014, doi: 10.1016/j.ijinfomgt.2014.07.005.
[127] V. Jaganathan, P. Cherurveettil, és P. Muthu Sivashanmugam, „Using a Prediction Model to Manage Cyber Security Threats”, *The Scientific World Journal*, máj. 03, 2015. https://www.hindawi.com/journals/tswj/2015/703713/ (elérés márc. 07, 2021).
[128] Z. Zhang, P.-H. Ho, és L. He, „Measuring IDS-estimated attack impacts for rational incident response: A decision theoretic approach”, *Computers & Security*, köt. 28, sz. 7, o. 605–614, okt. 2009, doi: 10.1016/j.cose.2009.03.005.
[129] A. P. Henriques de Gusmão, M. Mendonça Silva, T. Poleto, L. Camara e Silva, és A. P. Cabral Seixas Costa, „Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory”, *International Journal of Information Management*, köt. 43, o. 248–260, 0 2018, doi: 10.1016/j.ijinfomgt.2018.08.008.
[130] Lotfi. A. Zadeh, „Fuzzy sets”, in *Information and control*, 3. kiad., köt. 8, 1965, o. 338–353.
[131] E. Laufer, „Mamdani-típusú következtetési rendszeren alapuló kockázatkiértékelő módszerek optimalizálása”, PhD Thesis, 2014.
[132] Lotfi. A. Zadeh, „Outline of a New Approach to the Analysis of Complex Systems and Decision Processes”, *IEEE Transactions on Systems, Man, and Cybernetics*, köt. SMC-3, sz. 1, o. 28–44, 0 1973, doi: 10.1109/TSMC.1973.5408575.
[133] E. H. Mamdani és S. Assilian, „An experiment in linguistic synthesis with a fuzzy logic controller”, *International Journal of Man-Machine Studies*, köt. 7, sz. 1, o. 1–13, 0 1975, doi: 10.1016/S0020-7373(75)80002-2.
[134] P. Martin Larsen, „Industrial applications of fuzzy logic control”, *International Journal of Man-Machine Studies*, köt. 12, sz. 1, o. 3–10, 0 1980, doi: 10.1016/S0020-7373(80)80050-2.
[135] T. Takagi és M. Sugeno, „Fuzzy identification of systems and its applications to modeling and control”, *IEEE Transactions on Systems, Man, and Cybernetics*, köt. SMC-15, sz. 1, o. 116–132, 0 1985, doi: 10.1109/TSMC.1985.6313399.
[136] R. Fuller, *Fuzzy Reasoning and Fuzzy Optimization*. Abo: Turku Centre for Computer Science, 1998.
[137] J. Dombi és E. Laufer, „Reducing the Computational Requirementsin the Mamdani-type Fuzzy Control”, *ACTA POLYTECHNICA HUNGARICA*, köt. 17, o. 25–41, 2020, doi: 10.12700/APH.17.3.2020.3.2.
[138] M. Stanley, „The Small-World Problem. Psychology Today”, *PsychologyToday*, sz. 1, o. 61–67, 1967.
[139] A.-L. Barabási - A hálózatok új tudománya, *Behálózva*, 2016. kiad. Budapest: Libri Kiadó.
[140] P. Erdős és A. Rényi, „On The Evolution of Random Graphs”, *Magyar Tudományos Akadémia Matematikai Kutató Intézet Közlöny 5*, o. 17–61, 1960.

[141] H. Jeong, B. Tombor, R. Albert, Z. N. Oltvai, és A.-L. Barabási, „The large-scale organization of metabolic networks”, *Nature*, köt. 407, sz. 6804, Art. sz. 6804, okt. 2000, doi: 10.1038/35036627.
[142] D. Kiss és D. Váczi, „A vállalatok és a kritikus infrastruktúrák humánhálózata ellen irányuló támadások veszélyei a komplex hálózatok elemélete alapján”, *HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA*, köt. 28, o. 151–168, 2018, doi: 10.17047/HADTUD.2018.28.1.151.
[143] A.-L. Barabási, *A hálózatok tudománya*. Budapest: Libri Kiadó, 2016.
[144] Birher N., Bertalan P., Kele J., Bertalanné Pályi A., Molnárné Barna K., és Molnár T., *Hálózatokban*, 2014. kiad. Veszprém: Okter-Nobus Kiadó.
[145] H. C. Sözen, N. Basım, és K. Hazır, „Social Network Analysis in Organizational Studies”, *International Journal of Business and Management*, köt. 1, o. 21–35, 0 2009.
[146] R. Cross és K. Ehrlich, „Managing Collaboration at the Point of Execution: Improving Team Effectiveness with a Network Perspective”, 0 2008.
[147] G. R. Maio és G. Haddock, *The Psychology of Attitudes and Attitude Change*, 1st edition. Los Angeles ; London: SAGE Publications Ltd, 2010.
[148] D. Katz, „The Functional Approach to the Study of Attitudes”, *The Public Opinion Quarterly*, köt. 24, sz. 2, o. 163–204, 1960.
[149] E. Snowden, *Permanent Record*, 1st Edition. New York: Metropolitan Books, 2019.
[150] J. Gomes, P. Ahokangas, és K. Atta-Owusu, „Business modeling facilitated cyber preparedness”, *International Journal of Business and Cyber Security*, köt. 1, o. 54–67, 0 2016.
[151] Lazányi K., „A szervezeti biztonság és a munkahelyi stressz kapcsolata”, *TAYLOR*, köt. 8, sz. 5, Art. sz. 5, jan. 2016.
[152] R. R. McCrae és P. T. Costa, „Validation of the five-factor model of personality across instruments and observers”, *Journal of Personality and Social Psychology*, köt. 52, sz. 1, o. 81–90, 1987, doi: 10.1037/0022-3514.52.1.81.
[153] T. L. Giluk és B. E. Postlethwaite, „Big Five personality and academic dishonesty: A meta-analytic review”, *Personality and Individual Differences*, köt. 72, o. 59–67, 0 2015, doi: 10.1016/j.paid.2014.08.027.
[154] Tünde P., „A manipulatív viselkedési evolúció perspektívája”, o. 288.
[155] S. Jakobwitz és V. Egan, „The dark triad and normal personality traits”, *Personality and Individual Differences*, köt. 40, sz. 2, o. 331–339, 0 2006, doi: 10.1016/j.paid.2005.07.006.
[156] Goleman D., *Érzelmi intelligencia a munkahelyen*. Budapest: SHL Hungary Kft., 2002.
[157] B. Pikó, „Függőségek és a mértéktelenség kultúrája”, *Valóság: Társadalomtudmányi Közlöny*, köt. 60, sz. 3, o. 16–23, 2017.
[158] G. John M., „Internet Addiction Guide”, *Psych Central*, máj. 17, 2019. https://psychcentral.com/net-addiction (elérés márc. 15, 2021).
[159] J. Talyigás, *Az internet a kockázatok és mellékhatások tekintetében*. Budapest: Scolar Kiadó, 2010.
[160] I. Hullám és L. Muha, „Új típusú függőségek az információs társadalomban és azok hatása az informatikai biztonságra”, *HADTUDOMÁNYI SZEMLE*, sz. 3/2, o. 70–76, 2010.
[161] „Mi az a középosztály, ki a szegény és hol kezdődik a gazdag? – Kiszámoló – egy blog a pénzügyekről”, júl. 03, 2019. https://kiszamolo.hu/mi-az-a-kozeposztaly-ki-a-szegeny-es-hol-kezdodik-a-gazdag/ (elérés márc. 14, 2021).

[162] M. Fathali M., „The Staircase to Terrorism: A Psychological Exploration.”, *American Psychologist*, köt. 60, o. 161–169, 2005, doi: https://doi.org/10.1037/0003-066X.60.2.161.
[163] G. Nógrádi és N. Pákozdi, „A családi háttér szerepe a radikalizálódás folyamatában”, *HONVÉDSÉGI SZEMLE: A MAGYAR HONVÉDSÉG KÖZPONTI FOLYÓIRATA*, sz. 4, o. 25–39, 2016.
[164] Barics T., Juhász É., Karamánné Pakai É., és Szabó J., *Munkahelyi lelki egészségvédelem – mentális egészség, stresszkezelés, változások elfogadásának segítése*. Pécs: Pécsi Tudományegyetem, 2014.
[165] W. K. H. Kft, „2012. évi C. törvény a Büntető Törvénykönyvről - Hatályos Jogszabályok Gyűjteménye”. https://net.jogtar.hu/jogszabaly?docid=a1200100.tv (elérés márc. 14, 2021).
[166] M. A. Moreno, *Szex, drogok, Facebook*. Budapest: Móra Könyvkiadó, 2015.
[167] Z. Nyikes és E. Szűcs, „A zsarolóvírus-támadással szembeni védekezés a biztonságtudatosság növelésével”, *Prevention for ransomware attack by security awareness increasing*, 2019, Elérés: szept. 14, 2021. [Online]. Elérhető: https://eda.eme.ro/xmlui/handle/10598/31230
[168] „cyex | Cyber Security Awareness Platform”, *cyex*. https://cyex.io/ (elérés ápr. 23, 2021).
[169] Z. Bederna, „Components of Security Awareness and Their Measurement Part 1”, *ISACA Journal*, sz. 5, 2020, Elérés: ápr. 23, 2021. [Online]. Elérhető: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/components-of-security-awareness-and-their-measurement-part-1
[170] Z. Bederna, „Components of Security Awareness and Their Measurement Part 2”, *ISACA Journal*, sz. 5, 2020, Elérés: ápr. 23, 2021. [Online]. Elérhető: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/components-of-security-awareness-and-their-measurement-part-2
[171] M. Takács és E. Laufer, „The AHP Extended Fuzzy Based Risk Management”, in *10th WSEAS International Conference on Artificial Intelligence, Knowledge Engeneering and Data Bases (AIKED’11)*, 2011, o. 269–272.
[172] D. Váczi, „Az emberi tényező kockázatainak modellezési lehetősége Fuzzy-logikával a vasútnál, mint kritikus infrastruktúrában”, *HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA*, köt. 29, o. 80–91, 2019, doi: 10.17047/HADTUD.2019.29.3.80.
[173] D. Váczi, „Informatikai behatolások és felismerésük”,
[174] D. Váczi és T. Szádeczky, „A Threat for the Trains: Ransomware as a New Risk”, *INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS*, köt. 17, o. 1–6, 2019, doi: 10.7906/indecs.17.1.1.
[175] T. Szádeczky és D. Váczi, „Kiberbiztonsági változások a fizetési szolgáltatásoknál”, *HADMÉRNÖK*, köt. 13, o. 443–452, 2018.

8 PUBLIKÁCIÓK

8.1 A tézispontokhoz kapcsolódó tudományos közlemények

Az értekezésem új tudományos eredményeit az alábbi tézisek tartalmazzák:

1. Meghatároztam azokat a kockázati tényezőket, amelyek nagy valószínűséggel befolyásolják azt, hogy digitális minősített információt szivárogtasson ki egy személy.

Kapcsolódó publikációim:

- D. Váczi, Z. Bederna, V. Szalánczi-Orbán, és T. Szádeczky, „Az incidenskezelés szervezeti háttere”, in Hálózatok a közszolgálatban, Á. Auer és T. Joó, Szerk. Budapest: Ludovika Egyetemi Kiadó, 2019, o. 205–222. [Online]. Elérhető: https://m2.mtmt.hu/api/publication/31012112
- D. Váczi, „Célzott támadások módszertana”, in Célzott kibertámadások, 2018, o. 52–75.
- D. Váczi, „Az emberi tényező kockázatainak modellezési lehetősége Fuzzy-logikával a vasútnál, mint kritikus infrastruktúrában”, HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA, köt. 29, o. 80–91, 2019, doi: 10.17047/HADTUD.2019.29.3.80.
- D. Váczi és T. Szádeczky, „A Threat for the Trains: Ransomware as a New Risk”, INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS, köt. 17, o. 1–6, 2019, doi: 10.7906/indecs.17.1.1.
- T. Szádeczky és D. Váczi, „Kiberbiztonsági változások a fizetési szolgáltatásoknál”, HADMÉRNÖK, köt. 13, o. 443–452, 2018.

2. Megalkottam egy olyan fuzzy modellt, amelyet alkalmazva a megfelelő információk (bemenetek) ismeretében megsejthető, hogy mely személyek jelentenek kockázatot a szervezeten belül az információszivárogtatást, mint fenyegetettséget figyelembe véve egy célzott támadás esetén.

Kapcsolódó publikációim:

- D. Vaczi, E. Toth-Laufer, és T. Szadeczky, „Fuzzy-based Cybersecurity Risk Analysis of the Human Factor from the Perspective of Classified Information Leakage”, in 2020 IEEE 18th International Symposium on Intelligent Systems

and Informatics (SISY), szept. 2020, o. 000113–000118. doi: 10.1109/SISY50555.2020.9217053.

- F. Z. Gozon, E. Laufer, és D. Váczi, „Fuzzy-based Human Factor Centered Cybersecurity Risk Assessment”, Proc. of the IEEE 19th International Symposium on Intelligent Systems and Informatics, 2021. (Megjelenés alatt.)
- E. Laufer, T. Szadeczky, és D. Váczi, „Human risk factors to measure the potential of digital information leakage”, Biztonságtudományi Szemle, sz. III. évf. 3. szám, o. 55–65.
- D. Váczi, „Az emberi tényező kockázatainak modellezési lehetősége Fuzzy-logikával a vasútnál, mint kritikus infrastruktúrában”, HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA, köt. 29, o. 80–91, 2019, doi: 10.17047/HADTUD.2019.29.3.80.

3. Megállapítom, hogy a hálózatelemzési módszerek és a fuzzy logika külön-külön is alkalmas a kockázatok mérésére, de együtt pontosabb eredményt adnak. Együttes alkalmazásukra létrehoztam egy modellt a kiberbiztonsági szempontból kockázatos személyek beazonosítását figyelembe véve.

Kapcsolódó publikációim:

- D. Váczi, Z. Bederna, V. Szalánczi-Orbán, és T. Szádeczky, „Az incidenskezelés szervezeti háttere”, in Hálózatok a közszolgálatban, Á. Auer és T. Joó, Szerk. Budapest: Ludovika Egyetemi Kiadó, 2019, o. 205–222. [Online]. Elérhető: https://m2.mtmt.hu/api/publication/31012112
- Z. Bederna, D. Váczi, T. Szádeczky, és P. Pollner, „Támadás hálózatba szervezve”, in Hálózatok a közszolgálatban, Á. Auer és T. Joó, Szerk. Budapest: Ludovika Egyetemi Kiadó, 2019, o. 223–247. [Online]. Elérhető: https://m2.mtmt.hu/api/publication/31012112
- D. Vaczi, E. Toth-Laufer, és T. Szadeczky, „Fuzzy-based Cybersecurity Risk Analysis of the Human Factor from the Perspective of Classified Information Leakage”, in 2020 IEEE 18th International Symposium on Intelligent Systems and Informatics (SISY), szept. 2020, o. 000113–000118. doi: 10.1109/SISY50555.2020.9217053.

- F. Z. Gozon, E. Laufer, és D. Váczi, „Fuzzy-based Human Factor Centered Cybersecurity Risk Assessment”, Proc. of the IEEE 19th International Symposium on Intelligent Systems and Informatics, 2021. (Megjelenés alatt.)
- E. Laufer, T. Szadeczky, és D. Váczi, „Human risk factors to measure the potential of digital information leakage”, Biztonságtudományi Szemle, sz. III. évf. 3. szám, o. 55–65.
- D. Kiss és D. Váczi, „A vállalatok és a kritikus infrastruktúrák humánhálózata ellen irányuló támadások veszélyei a komplex hálózatok elemélete alapján”, HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA, köt. 28, o. 151–168, 2018, doi: 10.17047/HADTUD.2018.28.1.151.
- D. Váczi, „Az emberi tényező kockázatainak modellezési lehetősége Fuzzy-logikával a vasútnál, mint kritikus infrastruktúrában”, HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA, köt. 29, o. 80–91, 2019, doi: 10.17047/HADTUD.2019.29.3.80.

8.2 További tudományos közlemények

- A. Beláz és D. Váczi, Vasút-irányítási rendszerek kiberbiztonsági incidensmenedzsmentje, In: Rajnai, Zoltán (szerk.) Kiberbiztonság - Cyber Security: Tanulmánykötet a Biztonságtudományi Doktori Iskola kutatásaiból, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Budapest, 2018, pp. 51-61. ,