ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS
TÉZISFÜZETE

BRÉDA GÁBOR

Védett helyiségek komplex biztonsága

Témavezető: Dr. Varga Péter János PhD

BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA

Budapest, 2022 október 25.

Tartalomjegyzék

1 Summary

The focus of my research is on the theoretical feasibility of the location of personal, confidential human-to-human communication. The thesis presents the research process and results in five chapters. I review the theoretical background of the data-information interconnection. I examine the information security concerns that arise related to direct human-to-human communication. I identify the emerging security gaps and define the notion of a protected room relevant to the topic. I review the legislative measures in force in Hungary. I have not found clear guidance on the technical design of the protected room under discussion. I review the relationship between security and safety and the economic considerations for the planning of security measures, and the traditional elements of site security as well. Based on this, it is possible to identify the sectors in which the design of a protected room may be necessary. I propose possibilities for the location of a protected room and the development of an autonomous protection infrastructure. I review and structure the general methods of intelligence gathering for the theoretical development of applicable protection elements. Following the theoretical overview, the results of the demonstrative measurements are presented. I demonstrate the formation of information leakage channels coinciding with acoustic resonance and optical propagation during communication interactions. I confirm the non-operational radio frequency emissions of display devices and their correlation with the information content. I prove the relevance of the electromagnetic shielding design. I conclude that there is a serious contrast between SMART meeting rooms and devices, and the technical solutions that can be used in protected rooms. Bellow I summarise the theoretical cornerstones of the physical design of protected rooms, with a multi-level definition of the protection solutions implemented for the identified risk factors. I review the structured options for technical measures to achieve complex security in protected rooms. I illustrate the residual risk-reducing effect of the components necessary to achieve a safe environment by describing each of these elements. I contrast the hazards identified in the research with the options for protective measures against them. I propose the definition of practical values of absorption. I propose the feasibility of a linear data link, a topic on which I have conducted research. The design and operation of protected rooms is inconceivable without quality control, inspection and maintenance, the results of which confirm the safe condition of the protected room. Based on these sources, I have made a summary, from which I have developed the pairing "inspection area - inspection device", "detection device - sources of danger". Screening - maintenance is one of the most effective means of reducing the residual risk. Radio frequencies in the vicinity

of protected rooms pose a risk, for the detection of which I provide a novel conceptual solution, based on my own concept. I propose a suitable technical design for the entry of persons into the protected room.

Summarizing the research results, I present a new scientific result in this thesis, a model for the design of a protected room that is resistant to the risks involved, in which the confidentiality of the spoken word and the visual content displayed can be ensured by applying technical solutions.

2 A kutatás előzményei

A kutatásom az információbiztonság megteremtésének sajátságos technikai területével foglalkozik, amely az ember - ember közötti közvetlen kommunikáció környezetének információbiztonsági védelmét célozza. Az elérhető előírásokban előzetes kutatást végeztem. A tanulmányozás során célzottan olyan előírásokat kerestem a kommunikációs környezet védelme érdekében, amelyek konkrét műszaki tartalmat határoznak meg. Kutatásom alapján az adat tárolására, az adathordozókon illetve informatikai rendszerben tárolt adatok védelmére, - különösen, ha azok szenzitívek, vagy minősítéssel rendelkeznek - elérhetőek fizikai és adminisztratív védelmet célzó előírások. Azonban a különböző titokvédelmi és jogi eszközöket is figyelembe véve a szenzitív vagy minősített adatokat - információt - tartalmazó elhangzott szó és a vizuálisan megjelenő szenzitív tartalom fizikai környezetének konkrét kialakítására nem található egyértelműen meghatározott ajánlás.

Az információ emberek közötti feldolgozása és megosztása a beszéd, látás és hallás útján lehetséges, amely megfigyelhető. Az előírásokkal és szabályokkal, műszakilag védett környezetből kikerülő információ olyan közegbe kerülhet, amely biztonsági szintje nem egyezik az tároló rendszer biztonsági szilárdságával. Az információ megjelenése új formát ölt, a kommunikáció során a tároló rendszertől eltérő új fizikai jellemzőkké alakul, amely technikai berendezésekkel észlelhető.

3 Célkitűzések

A kutatási témám az ember- ember közötti közvetlen kommunikáció során előálló hang és vizuálisan megjelenő információ fizikai védelmére irányul. A szakirodalmi kutatás során találtam olyan hazai és külföldi ajánlásokat, leírásokat, amelyek részben kapcsolódnak a problémakörhöz, de egyértelmű ajánlást vagy hozzáférhető, megfelelő intézkedési utasítást nem adnak. Kutatásom célja, egy olyan környezet megteremtése, ahol az információ nagyfokú biztonságának egyenszilárdsága garantálható az elvi biztonsági rések kiküszöbölésével. Feltételezem, hogy létrehozható egy védett környezet modell szintű megalkotása, amely mint védett helyiség definiálható.

A kutatás során az alábbi célokat valósítottam meg:

- Meghatározni a "védett helyiség" fogalmát;
- Megvizsgálni a jogi forrásokat, igazolva a téma relevanciáját, igazolva az előzetes kutatások állítását;
- Javaslatot tenni egy megfelelő védett tárgyaló helyiség épületen belüli elhelyezésére,
- Igazolni az analóg módon előálló információcsere során létrejött információszivárgási csatornák kialakulását;
    - Igazolni demonstrációval az akusztikus hangrezgések terjedését a védeni kívánt kommunikáció során használt helyiségek határoló falazatában és azok szomszédos környezetében az információszivárgási lehetőségek igazolására;
    - Igazolni az optikai úton történő információszivárgás tényét;
    - Igazolni a megjelenítő eszközök nem üzemszerű rádiófrekvenciás sugárzásait a kisugárzott információtartalom tekintetében;
    - Igazolni a rádiós árnyékolás, mint védelmi intézkedés szükségességét;
    - Áttekinteni a technikai információszerzés lehetséges autonóm módjait, majd rendszerezni a nyílt forrásból megismerhető fenyegetést jelenő technikai eszközök fő működési paramétereit;
- Meghatározni a védett helyiség kialakításának elvi modelljét
    - Javaslatot tenni védett helyiség tekintetében akusztikai és rádiós árnyékolás csillapítási értékeire;
    - Javaslatot tenni védett helyiségek közötti pont - pont összeköttetés megvalósítására a fizikai réteg monitorozhatóságának tekintetében;
    - Javaslatot tenni felhasználható prezentáló eszközök optimális szoftver technológiai paramétereinek meghatározására;
    - Javaslatot tenni védett helyiségek kialakítása és üzemeltetése során szükséges vizsgálatok kialakítására;

- Javaslatot tenni és elvi megoldást adni a védett helyiségek környezetében megjelenő rádiós források lokális közeltéri azonosítására, az épített környezet rádiós csillapítási jellemzőinek figyelembevételével;

• Áttekintést adni kiegészítő rendelkezés megalkotásához a minősített adat szóbeli megjelenési környezetének biztonságosabbá tételéhez, a szóbeli kommunikációs interaktus helyszínének ajánlott defenzív átvizsgálási műveleteinek meghatározásával.

A téma jelenőségét tekintve specifikus, az információbiztonság - fizikai rétegének - kialakítása területén. A hagyományos mechanikai - fizikai, elektronikus vagyonvédelmi és objektumvédelmi elemek ugyan részei a kutatás tárgyát képező helyiség biztonsági elemeinek, azonban azok az elvi feltételezések révén, nem képesek teljes mértékig biztosítani a téma szempontjából megfelelő biztonság kialakítását. A kutatás kimenete a feltárt kockázatok ismeretében speciális, az objektumvédelemben nem megszokott, technikai-információvédelmi műszaki intézkedések alkalmazásának feltárása, az elvi információbiztonsági rések kiküszöbölése, a védett helyiség modelljének kialakítása céljából.

4 Vizsgálati módszerek

1. Irodalomkutatást és elemzést végeztem a témához kapcsolódó hazai jogi dokumentumok vonatkozásában;

2. Irodalomkutatást és elemzést végeztem a témához közvetlenül kapcsolódó források tekintetében;

3. Irodalomkutatást és elemzést végeztem az adat és információ elméleti definiálásának pontos meghatározása érdekében, a témához kapcsolódó tudásmenedzsment diszciplína tudományág területén;

4. Kutatást és elemzést végeztem, nyílt forrásból elérhető, a témában meghatározó hírszerzési módszerek tekintetében, az információbiztonságot befolyásoló problémacsoport behatárolása érdekében;

5. Kutatást és műszaki elemzést végeztem a védelmi intézkedések pontos meghatározása céljából, a nyílt forrásból elérhető, a védett helyiség technikai információbiztonságát növelő technológiák tekintetében;

6. Gyakorlati kutatást folytattam az ember-ember közötti közvetlen kommunikáció során megjelenő fizikai jelenségek terén, a felmerülő probléma sajátosságainak feltérképezése érdekében;

7. Megvizsgáltam és összegeztem a feltárt elvi információbiztonságot veszélyeztető komponenseket, következtetéseket vontam le belőle, majd ezen következtetések alapján javaslatot tettem a lehetséges védelmi alkalmazási eljárásokra;

8. Kísérleteket, méréseket hajtottam végre a célokban megfogalmazott akusztikai és rádiótechnikai fizikai jellemzők igazolásához, melyek eredményeiből következtetéseket vontam le;

9. Kutatási eredményeimet tudományos konferenciákon ismertettem mind itthon, mind külföldön magyar, illetve angol nyelven;

10. Eredményeimet a konferenciákon túlmenően, lektorált folyóiratokban is publikáltam;

A kutatás lezárásra került 2021. május 15-én.

5 Új tudományos eredmények

Kutatásom eredményeinek hasznosíthatósága szempontjából, megállapítható, hogy egy kevésbé publikált tudomány részterületet érintek a vizsgálódásaim során. A munkám során hét hipotézist állítok, melyek igazolásával tudományos eredményként meghatározom a „Komplex Védett Tárgyló - KVT” - védett helyiség- egyértelmű leírását, ezzel definiált terminus-technicust teremtve a témában. A fellehető források elemzése révén összegzem a technikai információszerzés módozatait és elkészítem az elektronikus információszerző eszközök csoportosítását a működési alapelvük tekintetében. A paraméterek ismeretében megállapítható azoknak az intézkedéseknek a struktúrája, melyek kialakítása során megalkotható az a környezet, amely szavatolja a technikai eszközök kockázataiból fakadó információbiztonsági rések mentességét. Konkrétan az eredményeket felhasználásával kialakítható egy védett - tárgyaló - helyiség, amely komplex intézkedések implementálása révén biztonságos környezetet nyújt szenzitív megbeszélések számára. A védelmi elemek tárgyalása során javaslatot teszek a kialakított védett helyiségek csillapítási szintjeire, valamint javaslatot teszek az üzembe helyezés - üzemeltetés - alatti rádiófrekvenciás csillapítások mérésének metódusára.

A javaslati részben megfogalmazottak alapján, áttekintést kapunk a „lehallgatás mentes környezet” kialakításához javasolt technikai átvizsgálás rendszerére, amely komponensei a szenzitív kommunikációs környezet és a védett helyiség karbantartásának alapjául szolgálhatnak.

Műszeres méréseket végeztem, amely eredményei alapján demonstrálható a vizuális megjelenítők rádiós sugárzásainak információtartalma. Részkutatást végeztem az épített környezetben történő rádiós sugárforrás lokalizáció területén, melynek eredményéül egy rádiós mérőműszer elvi kialakítására teszek javaslatot. A rádiós mérőműszer megalkotása révén egy olyan egyedülálló képességgel rendelkező készüléket kaphatunk, amelynek alkalmazásával épületeken belüli rádiós lefedettségi térképet készíthetünk, egy kiválasztott frekvenciának megfelelően.

Részkutatást végeztem az optikai távközlés területén, melynek eredményéül átfogó képet kaphatunk a szálellenőrzési metódusok lehetőségeiről. A kutatás új tudományos eredményéül modellt alkotok a védett helyiség fizikai kialakításának tekintetében, amely ellenáll a kutatás során feltárt technikai kockázatoknak.

TÉZIS I. Definíció szerűen meghatároztam a védett helyiség fogalmát, amely egyértelmű leírást ad a kutatás tárgyát képező védett helyiség meghatározására. [K1];[K4]; [K10];[K15]; [K16]

TÉZIS II. Megfogalmazott feltevést igazolva, rendszerezhetők azok az állami és magán szektorok intézményei, melyekben az információ biztonságának egyenszilárdsága szempontjából javasolt a kutatás eredményeként létrehozott védett helyiség alkalmazása. [K2];[K4];[K8];[K14];[K15];[K17]; [K19]; [K23]

TÉZIS III. Megfogalmazott felvetést igazolva, meghatároztam a védett helyiségek elhelyezésének és kialakításának általános struktúráját. [K2];[K3]; [K4]; [K8]; [K17]; [K19]; [K23]

TÉZIS IV. Feltételezésem negyedik pontját analitikus kutatási stratégiát folytatva igazoltam, hogy a nyílt felületeken elérhetőek egyedi eszközös elektronikus információszerző eszközök, működési alapparamétereik szerint rendszerezhetőek. A rendszerezés során meghatároztam a működés rendszertanára vonatkozó alapelvek struktúráját. Kísérleteket végeztem és megjelöltem azokat a technikai pontokat és védelmi megoldásokat, amely pontok

megzavarásával, valamint technikai kialakítások bevezetésével gátolható a fenyegetettség kialakulása, közvetlen védelmi hatást kifejtve az információ megjelenésének környezetére. [K1]; [K3];[K8];[K9];[K10];[K11];[K23]

TÉZIS V. Demonstratív kísérletekkel igazoltam az ember-ember közötti kommunikáció során keletkező, a kommunikáció információtartalmával korreláló fizikai jelenségek biztonsági kockázatait. [K1];[K3];[K8];[K23]

TÉZIS VI. A védett helyiséget a kutatás során megalapozott védelmi kialakításokat implementálva, modell készítésével bizonyítottam, hogy komplex megoldások révén, létrehozható egy olyan környezet, amely a kutatás során megismert, biztonsági kockázatokat hordozó jellemzőknek ellenáll, valamint létrehozható egy olyan tevékenységi protokoll, amely alkalmazásával, a biztonság fenntartását igazolva üzemeltethető egy védett helyiség. A tevékenységi protokollok kialakítása kapcsán a rádiófrekvenciás jelek lokalizálására újszerű megoldási javaslatot hoztam létre. [K3]; [K4]; [K5]; [K6]; [K8]; [K12]; [K13]; [K15]; [K17]; [K18];[K20];[K21];[K22];[K23]; [K24]; [K25]

TÉZIS VII. Dokumentumelemzéssel igazoltam, hogy meghatározható vonalas adatátviteli módszer és technológia, amely fizikai rétegét tekintve folyamatos ellenőrzés alá vonható. Kísérlettel bizonyítottam a paraméterváltozás azonnali kimutathatóságát. [K2]; [K7]; [K17]

6 Az eredmények hasznosítási lehetősége

A kutatási eredményeimet az oktatás, a biztonságtudomány, az információ védelmi tevékenység kialakítása során, valamint a műszaki tudományok területén ajánlom hasznosítani, mivel az eredmények és azok struktúrája, tág horizontot teremt a témában. A téma feldolgozása során, több diszciplínához tartozó kérdéskör is beépítésre került, melynek eredményéül ok-okozati összefüggések kerültek párosításra a védett helyiség kialakításának érdekében, az ember-ember között létrehozott, közvetlen kommunikáció információtartalmának védelmére, a védett helyiség megvalósítását szem előtt tartva.

Az eredményeimet felhasználva a kutatás folyamán publikált ismeretek, képet adhatnak a szervezeti biztonság kialakításán dolgozó személyek képzési anyagának összeállításához, valamint választ adhatnak a döntéshozók biztonságtudatos kommunikációs környezet kialakítására vonatkozó kérdéseire. Az értekezésben képet kapunk az információ értékké

alakulásának folyamatáról, amely során a figyelem a kommunikációs interaktus és annak értékteremtő folyamataira, valamint a kommunikáció biztonságának sebezhetőségére irányul.

Az értekezés eredményeinek felhasználását, ajánlom a biztonságos szervezeti struktúra technikai kialakításán dolgozó szakemberek számára, mivel a védett helyiségek kialakítása során, a kialakítani kívánt helyiség leírásával, a védett helyiség definíciója hasznos fogalom lehet a védett helyiségek egyértelmű azonosításának megfogalmazásával.

Az értekezést ajánlom nagy információs vagyonnal rendelkező szervezetek, intézmények biztonsági területekért felelős döntéshozói számára. Elemzés eredményei alapján és demonstratív úton is áttekintést adtam a témában megismerhető fenyegetettségeket összefoglalva, döntéstámogatói háttérismeretek növelése céljából. A kutatással elősegíthetem a védett helyiség szükséges kialakításának döntési relevanciáját, a szervezetekhez illesztve. Ajánlom a védett helyiség struktúra megvalósíthatóságának lehetőségét, valamint modellen keresztül konkrét megvalósítási javaslatot teszek „a védett helyiség" kialakítására.

A kutatás eredményeinek esetleges felhasználását javaslom a jogalkotó számára, biztonságos környezet kialakításának megteremtését célzó további szabályzó megfogalmazása céljából. A „Védett helyiség karbantartása, technikai átvizsgálása" című alfejezetében kifejtett gondolatok mentén elvégezhető technikai műveletek esetleges implementálása, és azok lehetőség szerinti elvégzése, jelentős mértékben csökkentő hatást fejtenek ki a kommunikációs környezet maradványkockázatának mértékére.

Az innováció tekintetében, az elképzelt rádiós forrás lokalizáció eljárást hardverfejlesztéssel foglalkozó szervezetek figyelmébe ajánlom,a gyakorlati kialakítás céljából.

A kutatás optikai távközléssel foglalkozó részeit az oktatásban javaslom hasznosítani, a monitorozható fizikai réteg megismerése céljából.

Továbbá a munkám teljes terjedelmét mindazon érdeklődők számára ajánlom, akik érdeklődnek a téma iránt és átfogó képet kívánnak kapni e témában.

7 Irodalmi hivatkozások listája/ Irodalomjegyzék

[1] R. Lincoln Ackoff, „From Data To Wisdom," Journal of Applies Systems Analysis 16, %1. kötet16, pp. 3-9, 1989.

[2] M. Pollányi, The Tacit Dimension, New York: Dubleday and Company; Garden City, 1966.

[3] Z. Zoltayné Paprika, Döntéselmélet, Budapest: Aliena, 2005.

[4] G. Bellinger, D. Castro és A. Mils, „Data Information Knowledge and Wisdom," 2004. [Online]. Available: http://www.systems-thinking.org/dikw/dikw.htm.

[5] A. Dr Keszthelyi, Információbiztonság technikai alapismeretek, OEKGK Szervezési és Vezetési Intézet, Vállalkozásfejlesztés a XXI. században, Budapest, 2012.

[6] I. Nonaka és H. Takeuchi, The Knowledge creating Company: How Japanese Companies Create the Dynamics of Innovation, New York: Oxford University Press, 1995.

[7] L. Tóth és P. Szikora, „Data, Information, Knowledge in FUTÁR: Case Study of a Public Transportation Information System," Science Journal of Business and Management, %1. kötet3., %1. szám1-1., pp. 66-72., 2015.

[8] A. Miller George, „The magical number seven, plus or minus two: Some limits on our capacity for processing information.," Psychological Review, %1. szám63, pp. 81-97, 1956.

[9] S. March, A. Hevner és S. Ram, „Research Commentary: An Agenda for Information Technology Research in Heterogeneous and Distributed Environments," 2000. [Online]. Available: http://dx.doi.org/10.1287/ isre.11.4.327.11873. [Hozzáférés dátuma: 30. Nov 2014.].

[10] L. Muha, Fogalmak és definíciók, Budapest: Verlag Dashöfer Szakkiadó, 2002.

[11] L. S. Mátrail, „Üzleti hírszerzés, gazdasági (ipari) kémkedés 1. szám," Terror & Elhárítás, 2018.

[12] C. Gémes, „Az információbiztonság alapkérdései," Hadmérnök XII. évfolyam 4-szám; Budapest, pp. 128-137, 2017.

[13] E. Szűcs és L. Záhonyi, „Információbiztonság fejlődés-történeti vizsgálata-Mérföldkövek, események és válaszok,” Biztonságtudományi Szemle 3:3, pp. 81-91, 2021.

[14] Á. Vaszari, Üzleti hírszerzés a multinacionális cégeknél és a kis és középvállalkozásoknál, Budapest: Budapesti Gazdasági Főiskola Külkereskedelmi Főiskolai Kar, 2007.

[15] K. Lazányi, „A biztonsági kultúra szerepe a vezetői döntések ámogatásában; TAYLOR Gazdálkodás és szervezéstudományi folyóirat 2016. 1. szám Szeged p.143-150,” 2016. [Online]. Available: https://ojs.bibl.u-szeged.hu/index.php/taylor/article/view/12993/12849. [Hozzáférés dátuma: 10. június 2016].

[16] K. Lazányi, „A biztonsági kultúra, TAYLOR Gazdálkodás és szervezéstudományi folyóirat 2015. 1-2 szám, Szeged, p.398-405,” [Online]. Available: https://ojs.bibl.u-szeged.hu/index.php/taylor/article/view/12936/12792. [Hozzáférés dátuma: 07. december 2015].

[17] Z. Prof Dr Rajnai, „Információbiztonság tudatosság,” XXII. Fiatal Műszakiak Tudományos Ülésszaka,Műszaki tudományos közlemények 7., Kolozsvár, pp. 37-42., 2017.

[18] T. Farkas és E. Hronyecz, „Inokommunikációs szakemberek a védelmi szférában: Szakirányú továbbképzés,” Műszaki Tudományos Közlemények (HU) 9:1, pp. 75-78, 2018.

[19] I. Dobák, „Betekintés az állambiztonság 1960-70-es évei nemzetközi technikai kutatás-fejlesztési folyamatainak szerkezetébe,” Hadmérnök: 8, pp. 319-327, 2013.

[20] I. Dobák és I. Solti, „Az "operatív technika" fejlesztésének helye és szerepe az állambiztonság szervezetrendszerében - A szobalehallgatás,” Hadmérnök 11:3, pp. 121-134, 2016.

[21] 2012. évi C. törvény a Büntető Törvénykönyvről.

[22] G. Fülöp, Az információ, Budapest: Eötvös Lóránd Tudományegyetem, 1996.

[23] C. Lavaud, R. Gerzaguet, M. Gautier, O. Berder, E. Nogues és S. Molton, „Whispering devices: A survey on how side-channels lead to compromised

information," HAL Science Ouverte, 21. Marc 2021. [Online]. Available: https://hal.archives-ouvertes.fr/hal-03176249. [Hozzáférés dátuma: May 2021].

[24] „US National Security Agency. Tempest: A signal problem," 1972.

[25] L. Pokorádi, „Technikai rendszerek megbízhatósága és biztonsága," Szolnoki Tudományos Közlemények 2009:13, 2009.

[26] 2013. évi V. törvény a Polgári Törvénykönyvről 2:46. § [A magántitokhoz való jog].

[27] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

[28] 2009. évi CLV. törvény A minősített adat védelméről.

[29] 2013. évi L. törvény Az állami és önkormányzati szervek elektronikus információbiztonságáról.

[30] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról.

[31] 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról.

[32] 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 meghat.ról.

[33] 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 sérülékenység vizsgálat lefolytatásának. szabályáról.

[34] 161/2010. (V. 6.) Kormány rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól.

[35] 92/2010. (III. 31.) Korm. rendelet az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól.

[36] 90/2010 (III.26.) Kormányrendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről.

[37] 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról.

[38] 2018. évi LIV. törvény az üzleti titok védelméről.

[39] 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokró.

[40] 2012. évi I. törvény A munka törvénykönyvéről.

[41] P. Erdősi, CISA Az üzleti hírszerzés és az ipari kémkedés ajánlás 2. változat, Budapest: Budapesti Műszaki és Gazdaságtudományi Egyetem Gazdaság- és Társadalomtudományi Kar Információ- és Tudásmenedzsment Tanszék, 2005.

[42] „Cégvezetés Az üzleti titok védelme 55.szám," 01. november 2002. [Online]. Available: https://cegvezetes.hu/2002/11/az-uzleti-titok-vedelme/. [Hozzáférés dátuma: 14 Nov 2014].

[43] L. Muha és C. Krasznay, Az elektronikus Információs rendszerek menedzselése, KÖFOP-2.1.1-VEKOP-15-2016-00001 szerk., Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[44] J. Kerekes, L. Stampok, J. Tímár, Z. Tamás, B. Dr. Tóth, B. Nagy és S. Nyilas, Információ - Biztonság, Budapest: Cedit Információtechnikai Kft., 1997.

[45] L. Megyeri és T. Farkas, „Kockázatkezelés,tudomány vagy kurázsi," Hadmérnök 12:3, pp. 198-209, 2017.

[46] T. Berek és I. Elek, „Zárszerkezet, mint a mechanikai védelem sebezhető pontja," Műszaki Katonai Közlöny 25:3, pp. 47-58, 2015.

[47] S. Gyányi és L. A. Keszthelyi, Technológiai ismeretek, Budapest: NKE, 2014.

[48] Z. Haig és L. Kovács, Kritikus infrastruktúrák és kritikus információs infrastruktúrák Tanulmány TÁMOP 4.2.2/B-10/1-2010-0001, Budapest: Nemzeti Közszolgálati Egyetem, 2012.

[49] „Critical Foundations Protecting America's Infrastructures The Report of the President's Commissionon Critical Infrastructure Protection," Washington, 1997.

[50] B. Dr. Bognár, T. Dr. Bonnyai, D. G. Katalin, D. K.-U. Lajos és G. Dr. Vass, Létfontosságú rendszerek és létesítmények védelme, Budapest: Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézet, 2015..

[51] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

[52] „EUR-Lex; Az Europai Parlament és Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységes magas szintjét biztosító intézkedésekről," 06 Jun 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L1148&from=en. [Hozzáférés dátuma: 05 January 2017].

[53] P. J. Varga, „Kritikus infrastruktúrák hatás alapú modellezése," Hadmérnök 4:4, pp. 390-399, 2009.

[54] J. P. Varga, „A kritikus információs infrastruktúrák értelmezése," Hadmérnök III. évfolyam, %1. szám 2., pp. 149-156., 2008.

[55] Z. Précsényi és J. Solymosi, „Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé,"Hadmérnök II.Évfolyam 1.szám," pp. 65-76, 2007.

[56] T. Kovács és A. Pallagi, „Kritikus infrastruktúrák komplex biztonságvédelmi rendszereinek tervezése, kialakítása, különös tekintettel a beléptetőrendszerek alkalmazására," Hadmérnök 14:4, pp. 35-45, 2019.

[57] G. Bréda és B. Hajdu, „A társadalom és a védett helyiségek kapcsolata, valamint a védett helyiségek kialakításához kapcsolódó tudományterületek," KÖZTES EURÓPA: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI 9 : 1-2 pp. 89-96. , 8 p., 2017.

[58] E. Szűcs és M. Szakali, „A biztonság ára, avagy a védelmi költségvetés emelkedésének lehetséges hatásai," Hadmérnök 13:1, pp. 314-325, 2018.

[59] H. Szabó és I. Dobák, „Az információs társadalom nemzetbiztonsága," Nemzet és Biztonság:Biztonságpolitikai szemle 14 : 2 , pp. 93-110, 2021.

[60] S. Steven, „The People, Policy, Technology (PPT) Model: Core," [Online]. Available: https://ur.booksc.eu/book/51467443/0a5c17. [Hozzáférés dátuma: 14 március 2020].

[61] L. Berek, Biztonságtechnika ÁROP – 2.2.21, Budapest: Nemzeti Közszolgálati Egyetem, 2014.

[62] B. Boros, R. Bottyán, S. Dessewffy, I. Koskovics, J. Kovács, F. Liszt, L. Móró és L. dr. Szili, Rendészet, vagyonvédelem, Budapest: Buapesti Műszaki Egyetem Mérnöktovábbképző Intézet, 1997.

[63] R. Pető, „Épületvédelem metódusa robbantásos cselekmények ellen," Műszaki Katonai Közlöny 23:1 ISSN 2063-4986, pp. 51-58, 2013.

[64] L. Dr. Berek, T. Dr. Berek és L. Berek, in Személy és vagyonbiztonság, Budapest, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 2016, p. 32.

[65] A. Őszi, „Az e-kereskedelem elvárásai a biometriával szemben," in Vállalkozásfejlesztés a XXI. században: IV. tanulmánykötet, Nagy Imre Zoltán, Szerk., Budapest, Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2014, pp. 427-440.

[66] G. Lukács, A. Dőring és P. Hell, Vagyonvédelmi rendszerek I., Budapest: Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar, 2015.

[67] A. Dőring, P. Hell és G. Dr. Lukács, Analóg áramkörök és érzékelők II., Budapest: Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar, 2015.

[68] Á. Guttengeber, L. Szili, F. Cserhalmi, G. Szűcs, L. Móró és B. K. Dunai, Személy és vagyonőrök, biztonságtechnikai szakemberek tankönyve, Budapest: Pro-Sec Kft..

[69] Z. Kuris, „A komplex információvédelem új irányai a nemzeti minősített adatok védelmével összefüggésben," Hadmérnök V. évfolyam 4. szám; Budapest, 2010.

[70] MABISZ, „Betöréses lopás- és rablásbiztosítás technikai feltételei (Ajánlás)," 12 február 2021. [Online]. Available: http://www.pluto.hu/_A/A2.html. [Hozzáférés dátuma: június 2021].

[71] Z. Prof Dr Rajnai, „Kritikus infrastruktúrák védelme," XXI. Fiatal Műszakiak Tudományos Ülésszaka,Műszaki tudományos közlemények 5., Kolozsvár, pp. 349-352., 2016.

[72] P. Vadász, „Információkeresés a gazdasági hírszerzésben; Hadmérnök IX: évfolyam 2. szám," Budapest, 2014.

[73] Dobák és Imre, „Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében: Hadmérnök 12,” pp. 235-249, 2017.

[74] J. Dr. Boda és I. Dr. Dobák, A nemzetbiztonság technikai kihívásai a 21. században, Budapest: Nemzeti Közszolgálati Egyetem Szolgáltató Nonprofit Kft., 2015.

[75] T. Wührl, G. Lukács és G. Mágel, Híradástechnika I., Budapest: Bidapesti Műszaki Főiskola Kandó Kálmán Villamosmérnöki Kar, 2008, p. 174.

[76] G. Lukács és T. Wührl, Híradástechnika I., Budapest: Óbudai Egyetem, 2012, p. 225.

[77] S. Forgo, „Shannon és Weaver információelmélet (híradástechnikai) modellje,” [Online]. Available: https://forgos.uni-eszterhazy.hu/wp-content/tananyagok/tarsesmedkomm_pc_exe/415_shannon_s_weaver_informcielmleti_hradstechnikai_modellje.html.

[78] S. Forgó, „Tanulás és az új médiumok TÁMOP-4.1.2-A/1-11/1-2011-0021,” in Shannon és Weaver információelméleti (híradástechnikai) modellje, Eger, Eszterházy Károly Főiskola, 2013.

[79] A. S. Tanenbaum és D. J. Wetherall, Számítógép hálózatok, Budapest: Taramix Kft., 2013.

[80] F. A. Everest, Masters Handbook of Acoustics Fourth Edition, USA: McGraw-Hill Companies, Inc., 2001.

[81] T. Dr. Tarnóczy, Akusztikai Tervezés, Budapest: Műszaki Könyvkiadó, 1966.

[82] J. P. Nagy, A hangszigetelés elmélete és gyakorlata, Budapest: Akadémiai kiadó, 2004.

[83] „Paroc Sound insulation,” 2019. [Online]. Available: https://www.paroc.pl/knowhow/sound/sound-insulation?sc_lang=en. [Hozzáférés dátuma: Marc 2021].

[84] F. Agusztinovicz, „Hangterjedés akadályozott terekben; Mérnöki Akusztika oktatási https://last.hit.bme.hu/download/fulop/MernokiAkusztika_14/Hangelnyel%c3%a9s-g%c3%a1tl%c3%a1s_MAkusz.pdf. [Hozzáférés dátuma: május 2020].

[85] Z. Varga, „Hang és halláskárosodás,” 10. március 2019. [Online]. Available: https://www.fuldugo.hu/hirek/aktualis/hang-es-hallaskarosodas. [Hozzáférés dátuma: február 2021].

[86] B. Collings, G. Lietaert és F. Heismann, Reference Guide to Fiber Optic Testing Volume 2; JDSU Corporation, 2010.

[87] H. Tanaka, O. Takizawa és A. Yamamura, „A Trial of the Interception of Display Image using Emanation of Electromagnetic Wave,” Journal of the National Institute of Information and Communications Technology Vol.52, 2005, pp. 213-223.

[88] NBF, „A TEMPEST-ről és a kompromittáló elektromágneses kisugárzás elleni védelem eszközeiről,” [Online]. Available: https://www.nbf.hu/hasznos-informaciok/tempest/. [Hozzáférés dátuma: január 2017].

[89] M. G. Kuhn, „Electromagnetic eavesdropping risks of flat-panel displays,” Privacy Enhancing Technologies, Springer, 2005.

[90] W. V. Eck, „Electromagnetic radiation from video display units: an eavesdropping risk?,” Computers and Security 4., pp. 169-286, 1985.

[91] M. G. Kuhn, „Compromising emanations of lcd tv sets.,” Electromagnetic Compatibility (EMC), 2011 IEEE International Symposium IEEE, 2011, pp. 931-936.

[92] M. G. Kuhn, Compromising emanations:eavesdropping risks of computer;, University of Cambridge Computer Laboratory, 2003.

[93] I. Kubiak, „Laser printer as a source of sensitive emission,” Turkish Journal of Electrical Engineering & Computer Sciences, %1. kötet26., pp. 1354-1366, 2018.

[94] M. Marinov, „Remote video eavesdropping using a software-defined radio platform; Doctoral Dissertation,” 11 Jun 2014. [Online]. Available: https://github.com/martinmarinov/TempestSDR/blob/master/documentation/acs-dissertation.pdf. [Hozzáférés dátuma: Okt 2020].

[95] M. Marinov, „TempestSDR program,” 14. Apr 2020. [Online]. Available: https://github.com/martinmarinov/TempestSDR/tree/master/TempestSDR. [Hozzáférés dátuma: Okt 2020].

[96] „Advanced Electronic Security Co.,” [Online]. Available: www.bugsweeps.com/info/spytech.html. [Hozzáférés dátuma: Febr 2019].

[97] „TIME, ELECTRONICS Bug Thy Neighbo, pp.55-56,” 06. March 1964. [Online]. Available: https://time.com/vault/issue/1964-03-06/page/61/. [Hozzáférés dátuma: Jul 2019].

[98] I. dr. Solti, A titkos információgyűjtés, elvei, eszközei és módszerei, alkalmazásának lehetőségei a nemzetbiztonsági munkában Doktori (PhD) értekezés, Budapest: Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, 2017.

[99] T. Johnes, „3rd International Security Symposium - TSCM - Modern Eavesdropping Threats Presentation,” October 2020. [Online]. Available: https://www.youtube.com/watch?v=KFrZ6SPMZNo. [Hozzáférés dátuma: Dec 2020].

[100] I. Dr. Töltési, „Lehallgatásvédelem az üzleti szférában 1.,” Detektor plusz, %1. szám7., pp. 32-33, július 2006..

[101] I. Dr. Töltési, „Lehallgatásvédelem az üzleti szférában 2.,” Detektor plusz, pp. 58-59, augusztus-szeptember 2006.

[102] I. Dr. Töltési, „Lehallgatásvédelem az üzleti szférában 3.,” Detektor plusz, pp. 47-49, október-november 2006.

[103] „Special Report DIGITAL 2021,” [Online]. Available: https://wearesocial.com/uk/blog/2021/01/digital-2021-uk/. [Hozzáférés dátuma: Nov 2021].

[104] T. Berek, „Okos rendszerek lehetőségei és biztonsági kihívásai,” Biztonságtudományi Szemle 1:1-2, pp. 7-16, 2019.

[105] „CICS - Center for Strategic and Internetional Studies, Significant Cyber Incidents Since 2006 - 2021,” 05. Nov 2021. [Online]. Available: https://csis-website-prod.s3.amazonaws.com/s3fs-public/211105_SignificantCyberIncidents.pdf?_Bux.NVhaioSPTAcspLrKuLx.xCZNSP3. [Hozzáférés dátuma: Dec 2021].

[106] „Global Security Mag, Significant cyber attacks 2006 May - 2020 June,” Jul 2020. [Online]. [Hozzáférés dátuma: Marc 2021].

[107] P. J. Varga, „Az okos otthonok vezeték nélküli alkotóelemeinek biztonsága,” Köztes Európa: Társadalomtudományi Folyóirat: A VIKEK Közleményei 9:1 , pp. 83-87, 2017.

[108] L. Ványa, „Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre,” in Doktori értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, 2001.

[109] Z. Haig, „Az információbiztonság komplex értelmezése,” Hadmérnök, Robothadviselés 6., %1. kötetKülönszám, p. 9., 2006.

[110] A. Kerti, A vezetési és információs rendszerek technikai alrendszerének vizsgálata különös tekintettel a minőségbiztosításra és az átvitelbiztonságre Doktori értekezés, Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola, 2010.

[111] Z. Haig, „Az információs társadalmat fenyegető információalapú veszélyforrások,” Hadtudomány XVII. évfolyam 3. szám, Sept 2007.

[112] L. Muha, A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, Doktori értekezés, Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2007.

[113] L. Muha és Á. Bodlaki, Az informatikai biztonság, Budapest: PRO-SEC KFT, 2007.

[114] M. Környei, „Üzleti titok védelme,” Pécsi Tudományegyetem Óriás Nándor Szakkollégium, Scriptura Folyóirat I. kötet, pp. 170-185., 2015.

[115] Z. Kuris, „Komplex információbiztonság megvalósítási lehetőségeinek megközelítésa,” Hadmérnök II. évfolyam 1. szám, pp. 311-318, 2009.

[116] S. Bulja, R. Kopf, T. A és T. Hu, „High Frequency Dielectric Characteristics of Electrochromic WO3 and NiO Films with LiNbO3 Electrolyte,” Scientific Reports, %1. kötet DOI: 10.1038/srep28839, p. 6:28839 |, 30 June 2016.

[117] „FORTUNE,” [Online]. Available: https://fortune.com/2015/10/28/smart-windows/. [Hozzáférés dátuma: April 2021].

[118] S. d. o. s. insulation, „https://www.designingbuildings.co.uk/wiki/Sound

_insulation_in_buildings,” [Online].

[119] K. h. s. hatása, „https://www.rigips.hu/hu/epuletakusztika,” [Online]. Available: https://www.rigips.hu/hu/epuletakusztika. [Hozzáférés dátuma: november 2019].

[120] F. Augusztinovicz, „A beszéd, Segédlet,” [Online]. Available: https://last.hit.bme.hu/download/kommtech/5_Beszed.pptx.

[121] B. Berglund és T. Lindvall, „Community Noise,” [Online]. Available: https://www.nonoise.org/library/whonoise/whonoise.htm. [Hozzáférés dátuma: may 2020].

[122] H. Flechter és R. H. Galt, „The Preception os Speech and Its Relation to Telephony,” The Journal of the Acustical Society of America, %1. kötetVol22 Number 2, 1950 march.

[123] T. Tarnóczy, „A beszédérthetőség mint fizikai fogalom,” Fizikai Szemle, 1995 marc. [Online]. Available: http://fizikaiszemle.hu/archivum/fsz9503/tarn9503.html#ir. [Hozzáférés dátuma: marc 2020].

[124] G. Dr. Wersényi, „Telekommunikácio 2,” Széchenyi István Egyetem Távközlési Tanszék , 2022. [Online]. Available: http://vip.tilb.sze.hu/~wersenyi/TK2_J.pdf. [Hozzáférés dátuma: jan 2022].

[125] „reiusa.net,” REI, [Online]. Available: https://reiusa.net/wp-content/uploads/2017/11/ANG_Manual_revG.pdf. [Hozzáférés dátuma: marc 2020].

[126] L. H. Hemming, Architectural Electromagnetic Shielding Handbook, New York: The Institute of Electronics Engineers, Inc. IEEE Press, 1992.

[127] „ResearchGate EM field,” [Online]. Available: https://www.researchgate.net/figure/An-EM-wave-consists-of-2-components-electric-field-and-magnetic-field-oscillating-in_fig8_280872394. [Hozzáférés dátuma: maj 2021].

[128] „Electronics Notes EMI coupling mechanism,” [Online]. Available: https://www.electronics-notes.com/articles/analogue_circuits/emc-emi-electromagnetic-interference-compatibility/what-is-emi-basics-tutorial.php.

[129] „IEEE-STD299-2006,” [Online]. Available: https://www.lisungroup.com/wp-content/uploads/2020/02/IEEE-STD299-2006-Standard-Free-Download.pdf. [Hozzáférés dátuma: április 2021].

[130] „MSZ EN 50147-1:1988,” [Online]. Available: http://www.mszt.hu/web/guest/webaruhaz;jsessionid=F5C2352939D449A1BBFBA4F8987EC92D?p_p_id=msztwebshop_WAR_MsztWAportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_msztwebshop_WAR_MsztWAportlet_ref=068379&_msztwebsh. [Hozzáférés dátuma: marc 2021].

[131] „Holland Shielding Fólia és textil árnyékoló anyagok,” [Online]. Available: https://hollandshielding.com/Mu-copper-foil. [Hozzáférés dátuma: February 2022].

[132] „EM shield Árnyékolt szoba,” EM shield, [Online]. Available: https://emshield.de/en/portfolio/radiation-protection-tempest/. [Hozzáférés dátuma: április 2021].

[133] „S101 panel attenuation line,” [Online]. Available: https://www.ets-lindgren.com/products/shielding/rf-shielding-and-accessories/11003/1100312?page=Products-Item-Page. [Hozzáférés dátuma: mac 2021].

[134] „RFD-60 árnyékoló ajtó,” [Online]. Available: https://www.ets-lindgren.com/products/shielding/rf-shielding-and-accessories/11004/1100410?page=Products-Item-Page. [Hozzáférés dátuma: may 2021].

[135] „Hollandshielding Nagyteljesítményű szűrő,” [Online]. Available: https://hu.hollandshielding.com/Ultra-nagy-teljes%C3%ADtm%C3%A9ny%C5%B1-sz%C5%B1r%C5%91k-a-legmagasabb-%C3%A1rny%C3%A9kol%C3%A1si-ig%C3%A9nyekhez-8010. [Hozzáférés dátuma: Jan 202].

[136] „Hollandshield Árnyékolt szellőző átvezető,” [Online]. Available: https://hu.hollandshielding.com/Honeycomb-szell%C5%91z%C5%91-panelek. [Hozzáférés dátuma: February 2022].

[137] „Canadian Centre for Cyber Security; teria for the Design, Fabrication, Supply, Installation and Acceptance Testing of Walk-in, Radio-Frequency-Shielded Enclosures (ITSG-02),” [Online]. Available: https://cyber.gc.ca/sites/default/files/publications/itsg-02-eng.pdf. [Hozzáférés dátuma: February 2022].

[138] „MIL-HDBK-1195,” [Online]. Available: http://www.tscm.com/MIL-STD-1195.pdf. [Hozzáférés dátuma: January 2022].

[139] „MIL-STD-461E; Department of Defense Interface Standard,” [Online]. Available: http://www.chassis-plans.com/PDF/MIL-STD-461E.pdf. [Hozzáférés dátuma: 06 January 2018].

[140] K. E. Németh és T. Gregász, „Development of Measurement Method for Testing the Shielding Properties of Textiles andAnalysis of Avialibity of the Measurment System,” Óbuda University e-Bulletin, %1. kötet2, %1. szám1, pp. 201-215, 2011.

[141] „2003. évi C. törvény Az elektronikus hírközlésről,” [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a0300100.tv.

[142] „7/2015.(XI.13) NMHH rendelet,” [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1500007.nmh. [Hozzáférés dátuma: Marc 2021].

[143] „2/2017. (I. 17.) NMHH rendelet a rádióberendezésekről,” [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1700002.nmh. [Hozzáférés dátuma: March 2021].

[144] G. Bréda, Optikai szálfelügyeleti rendszer tervezése; Diplomamunka, Budapest: Óbudai Egyetem, 2014.

[145] T. Wührl és S. Gyányi, Számitógéphálózati alapismeretek, Budapest: MATÁV Kotatási Központ, 2006, p. 100.

[146] L. Choquet, „Reference Guide to Fiber Optic Testing Glossary,” JDSU Corporation, 2008.

[147] J. Larerriée, G. Lietaert, R. Taws és S. Wolszczak, Reference Guide to Fiber Optic Testing Volume 1; JDSU Corporation, 2007.

[148] „Small Bandwith OTDR (Optical Time Reflectometer) for reflection measurement of DWDM systems used in the Antares project Pieter N.J.M. Jansen rt al.,” January 2004. [Online]. Available: http://www.nikhef.nl/~jelle/antareswebdocuments/Sb_otdr/SB-OTDR.pdf. [Hozzáférés dátuma: May 2018].

[149] NTest Fiber Watch RFTS System-0904, 2008.

[150] „Fiber Optic Cable Tutorial,” [Online]. Available: http://www.fiberoptics4sale.com/Merchant2/fiber-optic-cable.php. [Hozzáférés dátuma: March 2008].

[151] M. Mary, S. P. Varghese, M. Swarish és S. Nair, „A novel real time Remote Fiber Monitoring System,” Ne ST Research & Development Centre, Plot43; CSEZ; Coshin India, [Online]. Available: http://een.iust.ac.ir/profs/Sadr/Papers/netp9.pdf.

[152] Z. Végvári, „A lehallgatás ellen védett mobiltelefonálás összehasonlító vizsgálata, Katonai logisztika 22. évfolyam 2. szám,” pp. 146-170, 2014.

[153] P. Vizi, „Okostelefonok biztonsági kihívásai," Hadmérnök VI. évfolyam 3. szám. Sept 2011.,” pp. 131-141.

[154] Z. Haig és I. Várhegyi, Hadviselés az információs hadszíntéren, Budapest: HM Zrínyi Kommunikációs Kht, 2005.

[155] MSZ 27001:2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények.

[156] G. Schuster és G. Terpecz, „Kritikus sikertényezők vagy elkerülhetetlen veszélyforrások,” Szolnoki Tudományos Közlemének 16: különszám, pp. 347-363, 2012.

[157] „156/2017. (VI. 16.) Korm. rendelet a haditechnikai tevékenység engedélyezésének és a vállalkozások tanúsításának részletes szabályairól,” [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1700156.kor. [Hozzáférés dátuma: January 2021].

[158] „Granite Island Group Technical Sourveillance Counter Measures,” [Online]. Available: http://www.tscm.com/TSCMSequence.html. [Hozzáférés dátuma: January 2021].

[159] R. Sasvár, Üzleti hírszerzés, Budapest: Grafika Press Rt., 2006.

[160] „MURRAY ASSOCIATES TSCM Inspection Process,” [Online]. Available: https://counterespionage.com/tscm-inspection-process/. [Hozzáférés dátuma: January 2021].

[161] „Implementing TSCM Sweeps for Business," [Online]. Available: https://execsecurity.com/wp-content/uploads/2018/10/Implementing-TSCM-for-Corporations.pdf. [Hozzáférés dátuma: January 2021].

[162] „Technical Surveillance Countermeasures," [Online]. Available: https://www.energy.gov/sites/default/files/2020/07/f76/HQFMSP-Chapter-9-Technical-Surveillance-Countermeasures-Feb-2018.pdf. [Hozzáférés dátuma: January 2021].

[163] „PURCHASING TSCM EQUIPMENT; INTERNATIONAL INTELLIGENCE LIMITED," [Online]. Available: https://www.international-intelligence.co.uk/purchase-tscm-equipment.html. [Hozzáférés dátuma: January 2021].

[164] „SHEARWATER TSCM; PRODUCT," [Online]. Available: https://shearwatertscm.com/products/. [Hozzáférés dátuma: January 2021].

[165] P. T. Wolf, Lehallgatás technika, Budapest: Marktech Kft., 1990.

[166] „TSCM – Technical Surveillance Counter Measures-CRFS," [Online]. Available: https://www.crfs.com/tscm. [Hozzáférés dátuma: March 2021].

[167] „Radio Inspector," [Online]. Available: https://radioinspector.com/. [Hozzáférés dátuma: February 2021].

[168] „Kestrel TSCM," [Online]. Available: https://kestreltscm.com/. [Hozzáférés dátuma: February 2021].

[169] „Wireless activity monitor," [Online]. Available: https://www.amazon.co.uk/Wireless-activity-JJN-WAM-108T-independent/dp/B0792BRZW2. [Hozzáférés dátuma: April 2021].

[170] K. Rothammel, Antennakönyv, Budapest: Műszaki könyvkiadó, 1977.

[171] Z. Németh, Helymeghatározás vezeték nélküli hálózatokon, Budapest: BME Méréstechnikai és Információs Rendszerek Tanszék; Szakdogozat, 2009. május 04.

[172] „Lokalizáxiós módszerek, protokollok és alkalmazhatóságuk," GOP 1.1.1-11-2011-0048 Tanulmánykötet; Használatalapú Díjfizatést lehetővé tévő hulladékgyűjtési rendszerek, [Online]. Available:

http://www.corvex.hu/files/3214/2668/9380/R14AB_Lokalizacios_modszerek_protokollok_es_alkalmazhatosaguk.pdf. [Hozzáférés dátuma: 05 January 2018].

[173] P. Denisowsky, „An Introduction to Radio Direction Finding Methodologies," [Online]. Available: https://wireless.vt.edu/symposiumarchives/2015_slides/document.pdf. [Hozzáférés dátuma: 05 January 2018].

[174] R. A. Nisar, „Radio Direction Finding Theory and practices," [Online]. Available: https://www.researchgate.net/profile/Nisar_Ahmed10/publication/289779492_Radio_Direction_Finding_Theory_and_Practices/links/569e752508ae21a56424b5a2/Radio-Direction-Finding-Theory-and-Practices.pdf. [Hozzáférés dátuma: 05 January 2018].

[175] G. Takács, „Helymeghatározás mobiltelefonnal LXIII. évf.2008/8," pp. 20-27..

[176] „International Telecommunication Union: Recommendation ITU-R P-1238-7: Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 900 MHz to 100 GHz," [Online]. Available: https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.1238-7-201202-S!!PDF-E.pdf. [Hozzáférés dátuma: 05 January 2008].

[177] T. Wührl, „GPS navigációs problémák UAV alkalmazásokba, Hadmérnök:Különszám," p. 8, 2006.

[178] K. Gyöngyösi, J. P. Varga és Z. Illési, „WLAN heat mapping in hybrid network," INFORMATICS 2017; IEEE 14th International Scientific Conference on Informatics Proceedings.(ISBN:978-1-5386-0888-3), p. 437., 2017.

[179] „A Sort Tutorial on Inertial Navigation System and Global Positioning System Integration," [Online]. Available: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20150018921.pdf. [Hozzáférés dátuma: 20 January 2018].

[180] O. J. Woodman, „An introduction to inertial navigation„" Technical Report University of Cambridge, Computer Laboratory, Number 696, ISSN 1476-2986, 2018. [Online]. Available: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-696.pdf. [Hozzáférés dátuma: 05 January 2018].

[181] „NLJD kapu,” [Online]. Available: https://safrex.net/product-showcase/technical-surveillance-counter-surveillance/. [Hozzáférés dátuma: 10 Nov 2021].

[182] „Test szkenner,” [Online]. Available: https://www.google.com/imgres?imgurl=https%3A%2F%2Fimages.radio.com%2Faiu-media%2Fdupage-county-jail-scanner-1fe96d0f-e304-40a6-b28a-0b8f6427d7f3.jpg&imgrefurl=https%3A%2F%2Fwww.audacy.com%2Fwbbm780%2Farticles%2Fdupage-county-sheriff-purchases-scanning-ma. [Hozzáférés dátuma: 10 Nov 2021].

[183] „Test szkenner 2,” Adany Systems, [Online]. Available: https://www.police1.com/police-products/technology/body-scanners/articles/getting-the-most-from-your-body-scanner-23Cbbm8DZdPigOkK/. [Hozzáférés dátuma: 10 Nov 2021].

[184] „Csomagröntgen 3,” [Online]. Available: https://znz.hu/termekek/rontgenberendezesek/. [Hozzáférés dátuma: 10 Nov 2021].

[185] „Csomagröntgen 2,” [Online]. Available: https://hu.pinterest.com/pin/562105597222449972/. [Hozzáférés dátuma: 10 Nov 2021].

[186] „Csomagrontgen,” [Online]. Available: https://www.gettyimages.com/detail/photo/x-ray-image-of-a-briefcase-carrying-a-mobile-phone-royalty-free-image/57339916. [Hozzáférés dátuma: 10 Nov 2021].

[187] I. P. Antók, Fényvezető hálózatok II. Fényvezető Hálózat alapismeret, Budaoest, 2011.

[188] I. P. Antók, Fényvezető hálózatok VI.; Fényvezető hálózatok létesítése II., Budapest, 2011.

[189] L. Cebe, Fénytávközlés I., Budapest: Kandó Kálmán Műszaki Főiskola, 1990.

[190] L. Smigura, Távközlő kábelek és vezetékek, Budapest: Magyar Posta Könyvkiadó, 1989.

[191] I. P. Antók, Fényvezető Hálózatok VIII., Fényvezető hálózatok tervezése II., 2011., Budapest.

[192] I. P. Antók, Fényvezető hálózatok IX., Szélessávú Optikai Hálózat Tervezése; 2011., Budapest.

[193] I. Jutasi, P. Vámos, E. Márkus, K. dr. Tamay és G. Nádorfi, Fényvezető távközlési rendszer tervezése (CCITT), Budapest: Távközlési Könyvkiadó, 1991.

[194] A. dr. Gyárfás, Optikai elemek mérése EDUCOPTIC mérőberendezéssel, Budapest: Budapesti Műszaki Főiskola; Kandó Kálmán Villamosmérnöki Főiskolai Kar, 2006.

[195] A. dr. Gyárfás, Optikai szálak mérése OTDR-rel, Budapest: Kandó Kálmán Műszaki Főiskola, 1997.

[196] G. Lajtha, Fénytávközlő rendszerek és elemeik, Budapest: Akadémiai Kiadó, 1987.

[197] G. Ákos, P. Jani, S. Varró, L. Andor és J. Balázs, Lézerek tudományos és gyakorlati alkalmazása; Fényvezető szálak és fénytávközlés, Prosperitas Kft. nyomda, 1993.

[198] I. P. Antók, Fényvezető kábelhálózat építése;, Mackensen Kft. nyomba, 2008.

[199] I. P. Antók, Fényvezető Hálózatok Gyakorlat, Passzív és aktív elemek a gyakorlatban 2., Budakalász, 2011.

[200] A. Elek, Nyomvonalas hálózatépítési technológiák kézikönyve, Budapest: Magyar Elektrotechnikai és Infokommunikációs Szövetség, 2006.

[201] „TIA/EIA STANDARD; Commercial Building Telecommunications Cabling Standard; APRIL 12. 2001," [Online]. Available: http://www.nag.ru/goodies/tia/TIA-EIA-568-B.1.pdf. [Hozzáférés dátuma: Marc 2018].

[202] „Live Fiber Monitoring in CWDM Network Part2," [Online]. Available: http://www.exfo.com/corporate/blog/2010/live-fiber-monitoring-cwdm-networks-part-2. [Hozzáférés dátuma: September 2018].

[203] „3M™ Planar Light Circuit (PLC) Optical Splitters," [Online]. Available: http://multimedia.3m.com/mws/mediawebserver?66666UuZjcFSLXTtmxfcOXM6EVuQEcuZgVs6EVs6E666666--. [Hozzáférés dátuma: October 2018].

[204] „Active Fiber Monitoring," [Online]. Available: http://www.ntestinc.com/activefiber.html. [Hozzáférés dátuma: September 2018].

[205] „Optikai Kábelek; Sommerkábel 2011.05,” [Online]. Available: http://www.sommerkabel.hu/optikai-kabelek-leiras.html. [Hozzáférés dátuma: Oktober 2018].

[206] „Dark Fiber Monitoring; NTEST,” [Online]. Available: http://www.ntestinc.com/darkfiber.html. [Hozzáférés dátuma: Oktober 2018].

[207] „Live Fiber Monitoring in CWDM Networks, Olivier Plomteux, Senior Product Line Manager, Optical Business Unit,” [Online]. Available: http://www.ccontrols.ch/cms/upload/downloads/Telecom/1206EN_FiberGuardianApplicationNoteLiveFiberMonitoringCWDM.pdf. [Hozzáférés dátuma: September 2018].

[208] D. Kozischek és M. Bolick, „Planning Link-Loss Budgets Using Statistics; Broadband Propertier; June 2007.,” [Online]. Available: http://www.broadbandproperties.com/2007issues/jun07issues/corning_june.pdf. [Hozzáférés dátuma: July 2018].

[209] „Light Amplifiers;,” [Online]. Available: http://ftp.utcluj.ro/pub/users/cemil/dwdm/dwdm_Intro/8_5311715.pdf. [Hozzáférés dátuma: March 2018].

[210] „Fiber Optic Cable;,” [Online]. Available: http://www.lanshack.com/fiber-optic-tutorial-cable.aspx. [Hozzáférés dátuma: October 2018].

[211] „Fibre Formulas made simple,” [Online]. Available: http://www.tripleplay.co.za/uploads/Optical%20Fibre%20Formulas.pdf. [Hozzáférés dátuma: September 2018].

8 Publikációk

8.1 A tézispontokhoz kapcsolódó tudományos közlemények

Tudományos folyóirat közlemények [K] :

[K1] Bréda, Gábor; Védett helyiségek biztonságának szempontjai

KÖZTES EURÓPA: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI 8 : 1-2 pp. 157-167. , 11 p. (2016)

[K2] Bréda, Gábor ; Hajdu, Beáta; A társadalom és a védett helyiségek kapcsolata, valamint a védett helyiségek kialakításához kapcsolódó tudományterületek

KÖZTES EURÓPA: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT: A VIKEK KÖZLEMÉNYEI 9 : 1-2 pp. 89-96. , 8 p. (2017)

[K3] Bréda, Gábor; Védett tárgyaló kialakításának alapvető biztonsági kérdései

HADMÉRNÖK 13 : 3 pp. 9-17. , 9 p. (2018)

[K4] Gábor, Bréda; Security Challenges of Smart Meeting Rooms in Smart Cities

ÓBUDA UNIVERSITY E-BULLETIN 8 : 1 pp. 5-12. , 8 p. (2018)

[K5] Kiss, Miklos ; Breda, Gabor ; Muha, Lajos; Information security aspects of Industry 4.0

PROCEDIA MANUFACTURING 32 pp. 848-855. , 8 p. (2019)

[K6] Gábor, Bréda ; Péter, János Varga; Protected spaces in smart citiesandthe identification of new radio signalsin their environment usinga complexmeasurement method

INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS 17 : 1-A pp. 67-77. , 11 p. (2019)

[K7] Gábor, Bréda; Monitoring optical data connection between protected rooms in smart cities

INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS 17 : 3 pp. 444-457. , 14 p. (2019)

[K8] Breda, Gabor ; Kiss, Miklós; Overview of Information Security Standards in the Field of Special Protected Industry 4.0 Areas & Industrial Security

PROCEDIA MANUFACTURING 46 pp. 580-590. , 11 p. (2020)

Tudományos konferencia kiadvány, könyvrészlet közlemények [K] :

[K9] Bréda, Gábor; Dóka, László; Varga, Péter János;

The examination of the development of the communication devices on the commercial market In: Szakál, Anikó (szerk.) 17th IEEE International Symposium on Computational Intelligence and Informatics (CINTI 2016)

Budapest, Magyarország : IEEE Hungary Section (2016) 370 p. pp. 303-307. , 5 p.

[K10] Bréda, Gábor; Védett helyiségek biztonságának szempontjai - Safety acpects of protected areas

In: Rajnai, Zoltán (szerk.) Kiberbiztonság - Cyber Security : Tanulmánykötet a Biztonságtudományi Doktori Iskola kutatásaiból

Budapest, Magyarország : Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, (2018) pp. 185-198. , 14 p.

[K11] Gábor, Bréda ; Péter, János Varga ; Zsolt, Illési; Forensic Functional Profile of IoT Devices: Based on Common Criteria

In: Anikó, Szakál (szerk.) 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY) : Proceedings

Budapest, Magyarország : IEEE Hungary Section (2018) 344 p. pp. 261-264. , 4 p.

[K12] Bréda, Gábor; Designing a protected room from information security aspect, a personal approach

In: Rajnai, Zoltán (szerk.) Kiberbiztonság – Cybersecurity 2.

Budapest, Magyarország : Óbudai Egyetem, Biztonságtudományi Doktori iskola (2019) 247 p. pp. 147-154. , 8 p.

[K13] Gábor, Bréda; Design a Protected Room from Information Security Aspect, a Personal Approach

In: Rajnai, Zoltán; Schmidt, Péter; Jurik, Pavol (szerk.) Eight International Scientific Web-conference of Scientists and PhD. students or candidates

Budapest, Magyarország : Óbuda University (2020) 224 p. pp. 145-152. , 8 p.

[K14] Bréda, Gábor; A villamosenergia ellátás biztonságának növelése a meddő villamos energia kompenzációja révén

In: Rajnai, Zoltán (szerk.) Kiberbiztonság – Cybersecurity 2.

Budapest, Magyarország : Óbudai Egyetem, Biztonságtudományi Doktori iskola (2019) 247 p. pp. 30-46. , 17 p.

[K15] Bréda, Gábor; Védett helyiségek jelene és jövője

In: Rajnai, Zoltán; Fregán, Beatrix; Marosné, Kuna Zsuzsanna (szerk.) Tanulmánykötet a 7. BBK előadásaiból

Budapest, Magyarország : Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, (2016) pp. 677-682. , 6 p.

Szóbeli előadás és absztrakt kötetben megjelent közlemények [K] :

[K16] Bréda, Gábor; Védett helyiségek és azok elhelyezése

In: Keresztes, Gábor (szerk.) Tavaszi Szél 2016 Konferencia. Nemzetközi Multidiszciplináris Konferencia : Absztraktkötet

Budapest, Magyarország : Doktoranduszok Országos Szövetsége (DOSZ) (2016) 485 p. pp. 303-303. , 1 p.

[K17] Bréda, Gábor; Védett helyiségek biztonságának szempontjai (2016)

X. Régiók a Kárpát-medencén innen és túl nemzetközi tudományos konferencia, Kaposvár, Kaposvári Egyetem, 2016 október 14.,

[K18] Bréda, Gábor; Az elhangzott szó védelme, védett tárgyaló, Protecting the spoken word, protected meeting room

In: Óbudai, Egyetem (szerk.) XXXIII. KANDÓ KONFERENCIA 2017: „Kandó a tudomány hajóján" Absztrakt kötet

Budapest, Magyarország : Óbudai Egyetem, (2017) pp. 31-32. , 2 p.

[K19] Bréda, Gábor; Okos város okos tárgyalóinak biztonsági kihívásai, The security challenges of smart meeting rooms in Smart Cities

In: Tokody, Dániel; Mgr. Ing. Gabriela Sopková, PhD. (szerk.) Smart City Konferencia 2017 Absztraktkötet : Smart City 2017 Conference Abstract Book

Budapest, Magyarország : Doktoranduszok Országos Szövetsége, (2017) p. 17 , 1 p.

[K20] Bréda, Gábor ; Varga, Péter János; Protected Spaces in Smart Cities and The Identification New Radio Signals in Their Environment Using a Complex Measurement Method

In: Tokody, Dániel; Tokodyné, Szabadi Nikolett (szerk.) Smart, Sustainable and Safe Cities Conference 2018 Abstract Book

Budapest, Magyarország : Doktoranduszok Országos Szövetsége (DOSZ) (2018) 40 p. pp. 30-30. , 1 p.

[K21] Kiss, Miklós ; Muha, Lajos ; Bréda, Gábor; Information Security Aspects of Industry 4.0 p. & (2018)

The 12th International Conference INTER-ENG 2018 Interdisciplinarity in Engineering, Konferencián elhangzott előadás,

[K22] Bréda, Gábor; Védett helyiségek információbiztonsága p. & (2018)

Doktoranduszok interdiszciplináris kutatásai a belügyi nemzetbiztonsági szférában, Előadás, Nemzeti Közszolgálati Egyetem,

[K23] Miklós, Kiss ; Gábor, Bréda; Overview of Information Security Standards in the Field of Special Protected Industry 4.0 Areas & Industrial Security (2019)

Szóbeli előadás, The 13th International Conference INTER-ENG 2019 Interdisciplinarity in Engineering, 3 - 4 October 2019, Târgu Mureș, Romania,

[K24] Gábor, Bréda; Designing a protected room from information security aspect, a personal approach (2020)

Trends and Innovations in E-business, Education and Security 2020, előadás a webkonferencián,

[K25] Bréda, Gábor; Védett helyiségek komplex biztonsága

In: Bárdos, Szabolcs (szerk.) Doktoranduszok Interdiszciplináris kutatásai a belügyi nemzetbiztonsági szférában

(2021) p. & , 1 p.