ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

TÉZISFÜZETE

PALLAGI ANDRÁS

Kritikus infrastruktúrák védelmének vizsgálata

Témavezető: Prof. Dr. Rajnai Zoltán

Prof. Dr. Kovács Tibor

**BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA**

Budapest, 2023. december 10.

Tartalomjegyzék

1 Summary

Protecting critical infrastructure is of utmost importance since it forms the foundation for the uninterrupted functioning of social and economic activities. These essential infrastructure assets face growing internal and external threats, which can disrupt operations or result in significant damage. Consequently, the imperative of enhancing the resilience and security of these infrastructures has extended not only to the national level but also within the purview of the European Union.

Directive 2022/2557/EU, issued by the European Union, strongly emphasizes bolstering the resilience of critical infrastructures. This directive offers a structured framework for Member States to manage potential risks effectively, ensuring the ability of these infrastructures to swiftly recover and sustain their functions in the face of disruptions or threats.

It is essential to adopt a systematic approach to maintain the protection and security of critical infrastructures and address the challenges stemming from deficiencies in related legal regulations. Given the diverse nature of critical infrastructures, this approach involves identifying commonalities and applying a unified security strategy that can be tailored to each similarity individually. Establishing a defense zone system for critical infrastructures is the most effective means to achieve this.

The characteristics and nomenclature of these defense zones should be closely tied to the logical and physical unity of the access control system. This system should encompass minimum physical and organizational prerequisites determined based on domestic and international regulations and practical experience.

While the zone system aids in the practical design of other protection components, a well-designed access control system should be regarded as a primary protective technical solution to prevent intentional harmful activities. This system should follow a comprehensive practical guide rooted in a unified security professional approach.

Drawing from my research findings, the creation of effect-based defense zones emerges as a viable method for enhancing protection effectiveness. Utilizing a scale of 0 to 4, these zones lead to a multi-layered set of security measures aligned with defense-in-depth principles. By implementing fundamental physical and electronic security requirements for each zone according to its level of protection, critical infrastructures can be prepared for worst-case scenarios.

Through fulfilling and applying these conditions, an appropriate protection strategy and effective access control system can be established for any critical infrastructure. In conjunction with establishing and maintaining an appropriate legal framework, this approach promotes the long-term stability and secure operation of critical infrastructures.

2 A kutatás előzményei

A változó világban kiemelt figyelem irányul a létfontosságú kritikus infrastruktúrák védelmére. A globalizáció, a technológiai fejlődés és a növekvő népesség új kihívásokat és lehetőségeket teremt, amelyek befolyásolják ezeknek az infrastruktúráknak a biztonságát és védelmét.

Az egyre növekvő társadalmi egyenlőtlenségek mellett létfontosságúvá válik a kritikus infrastruktúrák zavartalan működése. Az energiaellátástól az információs és kommunikációs technológiákig, valamint a közlekedéstől az egészségügyig terjedően a kritikus infrastruktúrák hatékony működése és védelme nélkülözhetetlen a modern társadalmak stabilitása és jóléte szempontjából.

Eközben a szándékosan elkövetett cselekményekből fakadó fenyegetések folyamatosan nőnek, és egyre több támadás éri ezeket az infrastruktúrákat. A terrorizmus, az ipari kémkedés, a kiberbűnözés és a szabotázs jelentős veszélyt jelentenek a kritikus infrastruktúrákra. Ugyanakkor az éghajlatváltozás és a természeti katasztrófák is komoly kihívásokat jelentenek a védelem és biztonság terén.

A kritikus infrastruktúrák védelmének és biztonságának fenntartása érdekében a döntéshozóknak és szakembereknek összehangolt, innovatív és előrelátó megközelítésekre van szükségük. Hatékony védelmi stratégiák kifejlesztése és alkalmazása, valamint megfelelő jogi keretrendszer létrehozása és fenntartása kulcsfontosságú a kritikus infrastruktúrák hosszú távú biztonsága és stabilitása szempontjából.

Összefoglalva, a kritikus infrastruktúrák védelme és biztonsága napjainkban és a jövőben is kiemelt jelentőségű marad. A dinamikusan változó világhoz való alkalmazkodás és az új fenyegetések kezelése érdekében döntéshozók, szakemberek és érintett szervezeteknek együtt kell működniük annak érdekében, hogy biztosítsák a kritikus infrastruktúrák hosszú távú stabilitását és biztonságát.

3 Célkitűzések

Értekezésem célja az, hogy a kritikus infrastruktúrák, mint létfontosságú rendszerelemek védelmét hatékonyabbá tegyem. Ehhez szükséges, hogy megvizsgáljam a jelenlegi jogszabályi környezetet, feltárjam a hiányosságait és azok következményeit.

Célom egy olyan egységes zónabesorolási rendszer kifejlesztése, amely segítségével azonosíthatom az egyes zónák legnagyobb kockázatait. Ezáltal lehetővé válik a védelmi erőforrások hatékonyabb elosztása és a kritikus infrastruktúrák hatékonyabb védelme. Továbbá a zónarendszer segíthet a kockázatkezelési stratégiák kidolgozásában is, mivel a kockázatok pontos azonosítása, mérése és értékelése elengedhetetlen része a hatékony védelemnek.

Célom továbbá a zónabesorolás alapján meghatározni az egyes zónákhoz kapcsolódó minimális követelmények rendszerét, különös tekintettel az elektronikus beléptető rendszerek alkotóelemeire.

Végül, célom egy olyan segédlet létrehozása, amely alapul szolgálhat az optimális beléptető rendszer kiválasztásához a kritikus infrastruktúrák tulajdonosai és üzemeltetői számára. Emellett támogatást nyújt a biztonsági rendszerek tervezőinek, kivitelezőinek, biztonsági összekötőknek és az auditoroknak is, így segítve az infrastruktúrák hatékonyabb védelmét és a biztonsági intézkedések megerősítését. Ezeknek a céloknak az elérésével hozzájárulhatok a társadalmunk biztonságának és stabilitásának megőrzéséhez.

4 Vizsgálati módszerek

A kutatásom során többféle kutatási módszertant alkalmaztam, amelyek mindegyike hozzájárult a kutatásom eredményeinek gazdagításához. Elsőként az általam preferált módszertan a hazai és nemzetközi kritikus infrastruktúrákkal kapcsolatos jogszabályok alapos elemzésén alapult. Ennek az alapos jogszabályelemzésnek célja az volt, hogy mélyebb betekintést nyerjek a kritikus infrastruktúrákkal kapcsolatos jogi keretrendszerbe, valamint, hogy megérthessem ezeknek a jogszabályoknak a kritikus infrastruktúrák védelmére és működésére gyakorolt hatását.

A második módszertanom az volt, hogy tanulmányoztam a nemzetközi kritikus infrastruktúrákkal kapcsolatos irányelveket és műszaki követelményeket. Ennek a kutatásnak a célja az volt, hogy mélyebb betekintést nyerjek a nemzetközi szabványokba és gyakorlatokba,

és hogy összehasonlítsam ezeket a magyarországi szabályozási keretrendszerrel. Ezáltal lehetőségem nyílt azonosítani a legkiválóbb nemzetközi gyakorlatokat, és megvizsgálni, hogy milyen mértékben alkalmazhatók ezek a normák a magyar jogrendszerben.

A harmadik módszertanom része volt a kritikus infrastruktúrákkal foglalkozó szakemberekkel folytatott interjúk készítése. Ezek az interjúk lehetőséget teremtettek a szakértőkkel való közvetlen párbeszédre, és mélyebb betekintést nyújtottak a "best practice" megoldásaikba. A szakértőkkel folytatott ilyen közvetlen interakciók révén tudtam megérteni a kritikus infrastruktúrák működési mechanizmusainak és védelmi kihívásainak gyakorlati aspektusait.

Az összesített kutatási módszertan lehetővé tette számomra, hogy átfogó képet alkossak a magyarországi kritikus infrastruktúrák fizikai és elektronikai védelmi szabályozásáról. A jogszabályelemzéstől kezdve a szakértői interjúkig minden módszertan hozzájárult ahhoz, hogy mélyebb betekintést nyerjek a kritikus infrastruktúrák védelmi helyzetébe és a fejlesztési irányokba. A kutatás eredményeképpen sikerült egy új irányelvet kidolgozni, amely segít a kritikus infrastruktúrák beléptető rendszereinek kiválasztásában tervezők, kivitelezők, megrendelők, üzemeltetők, biztonsági összekötők és auditorok számára. Mindezek alapján megállapítható, hogy a választott kutatási módszertanok kulcsfontosságú szerepet játszottak a kutatásom sikerében és a hipotéziseim megerősítésében.

5 Új tudományos eredmények

A kutatásom új tudományos eredményei:

1. tézis: Meghatároztam a kritikus infrastruktúrák védelmi zónáit, amely kulcsfontosságú a potenciális incidensek hatásainak kezelése során. [PA1], [PA2], [PA3]
2. tézis: A disszertációmban bizonyítottam, hogy meghatározhatók a kritikus infrastruktúrák beléptető rendszereihez társított alapkövetelmények. [PA1], [PA2], [PA3], [PA4]
3. tézis: A disszertációmban bizonyítottam, hogy az általam meghatározott alapkövetelmények alapján megalkotható egy olyan segédlet, amely komplex támogatást nyújt a kritikus infrastruktúrák beléptető rendszereinek tervezéséhez és kialakításához. [PA2], [PA3], [PA4]

.

6 Az eredmények hasznosítási lehetősége

A „Kritikus infrastruktúrák védelmének vizsgálata” című doktori értekezésem eredményeinek hasznosíthatósága alapján az alábbi javaslatokat fogalmazom meg a kutatási eredmények tükrében, az alábbi területeken:

1. Az elektronikus vagyonvédelmi rendszerek definíciójának egységesítését javaslom a magyarországi jogalkotók részére. Az egységes definíció segítene meghatározni és értelmezni az elektronikus vagyonvédelmi rendszereket, ezzel összehangolva a jogszabályokat és elősegítve a hatékonyabb és egységesebb szabályozást. Ezáltal javulna az elektronikus vagyonvédelmi rendszerek hatékonysága és alkalmazhatósága a különböző területeken és alkalmazási módokban.
2. Javaslom, hogy a disszertációban meghatározott védelmi zóna besorolási rendszert vegyék figyelembe a 2022/2557 irányelv magyarországi implementálásával kapcsolatos jogszabályok kidolgozásánál. Az egységes besorolási rendszer hatékonyan hozzájárulhat a kritikus infrastruktúrák hatékonyabb védelméhez, és az irányelv helyi alkalmazása ennek megvalósítására alkalmas lehetőséget teremt. Ezáltal fokozható az infrastruktúrák biztonsága és az ország védelmi rendszere.
3. Javaslom, hogy vegyék figyelembe a védelmi zónák követelményeit tartalmazó segédlet hasznosságát és vezessék be azt a kritikus infrastruktúrákkal foglalkozó biztonsági szakértők számára. Ez a segédlet segíthet a szakembereknek hatékonyabb beléptető rendszerek kialakításában és működtetésében, ezzel növelve a kritikus infrastruktúrák biztonságát és védelmét. Az ilyen iránymutatások bevezetése elősegítheti az optimális védelmi stratégiák alkalmazását és az esetleges biztonsági kockázatok minimalizálását.
4. Javaslom, hogy a disszertációmban kifejlesztett védelmi zónabesorolási rendszert, annak alapkövetelményeit, valamint az ezek alapján készített segédletet integrálják a kritikus infrastruktúra-védelmi biztonsági összekötő személy szakirányú továbbképzési szak tananyagába. Az integráció lehetővé tenné a szakértők számára az egységes és hatékony védelmi módszerek megismerését a kritikus infrastruktúrák védelmére, ezáltal növelve az ország kritikus infrastruktúráinak biztonságát és rugalmas ellenálló képességét.

7 Irodalmi hivatkozások listája/ Irodalomjegyzék

[1] A Tanács 2008/114/EK Irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről. (2008.12.23.) Az Európai Unió Hivatalos Lapja

[2] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

[3] 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről

[4] Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről

[5] Böröcz, M. Gy. (2022) Az Európai Unió biztonságpolitikája szerepének vizsgálata a kritikus infrastruktúrák védelmében Doktori (PhD) értekezés; Óbudai Egyetem

[6] Bonnyai, T. (2011). A kritikus infrastruktúra védelem fogalmi rendszere, hazai és nemzetközi szabályozása.

[7] Bonnyai, T. (2012). Kritikus infrastruktúra védelem az Európai Unióban – a kezdetektől napjainkig. Magyar rendészet, 12(1), 132–137.

[8] COM/2004/0702, A Bizottság közleménye a Tanács és az Európai Parlament részére, A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben

[9] COM/2005/0576, Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról

[10] COM/2006/0786, A Bizottság közleménye a létfontosságú infrastruktúrák védelmére vonatkozó európai programról

[11] COM/2006/0787, Javaslat A Tanács irányelve az európai létfontosságú infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről

[12] COM/2008/0676, Javaslat A Tanács határozata a létfontosságú infrastruktúrák figyelmeztető információs hálózatáról (CIWIN)

[13] Elavult Bizottsági javaslatok visszavonása. (2012.06.02) Az Európai Unió Hivatalos Lapja. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012XC0602(03)&qid=1683633307411 (Letöltve 2023.05.02.)

[14] COM/2020/829, Javaslat Az Európai Parlament és e Tanács irányelve a kritikus fontosságú szervezetek rezilienciájáról. (2020.12.16.)

[15] COM/2022/551, Javaslat A Tanács ajánlása a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről. (2022.10.18.

[16] ST/15623/2022/INIT. A Tanács ajánlása a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről (2022.12.9.)

[17] Bognár, B. (2014). A létfontosságú rendszerek és létesítmények védelmének nemzeti szabályozása. In A terrorizmus Rubik-kockája, avagy a fenyegetések komplex megközelítése: Nemzetközi tudományos-szakmai konferencia (pp. 46–50).

[18] Károlyi L. (2007) A kritikus infrastruktúrák védelme és az operatív erők tevékenységirányítása a honi katasztrófavédelemben, különös tekintettel az EU konformitásra Doktori (PhD) Értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar Katonai Műszaki Doktori Iskola

[19] 2112/2004. (V. 7.) Kormány határozat a terrorizmus elleni küzdelem aktuális feladatairól

[20] A Kormányzati Koordinációs Bizottság 1/2007. (III. 29.) számú határozata a katasztrófavédelemmel összefüggő 2007. évi feladatokról. https://jogkodex.hu/doc/6808616 (Letöltés ideje 2023.05.02.)

[21] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

[22] 1249/2010. (XI. 19.) Kormány határozat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról

[23] 295/2010. (XII. 22.) Kormány rendelet a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól

[24] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról1

[25] Bognár, B., Bonnyai, T., Görög, K., Katai-Urban, L. & Vass, Gy. (2015). Létfontosságú rendszerek és létesítmények védelme Kézikönyv a katasztrófavédelmi feladatok ellátására. Nemzeti Közszolgálati Egyetem. ISBN 978-615-5057-50-2.

[26] 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

[27] 62/2011. (XII. 29.) BM rendelet a katasztrófák elleni védekezés egyes szabályairól

[28] 65/2013. (III. 8.) Kormány rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

[29] Ciekanowski, Z., Żurawski, S., & Wyrębek, H. (2023). Critical infrastructure threats. In Studia Administracji i Bezpieczeństwa (Köt. 13, Issue 13, o. 263–272). Index Copernicus. https://doi.org/10.5604/01.3001.0016.2902

[30] Bonnyai, T. (2014). A kritikus infrastruktúra védelem elemzése a lakosságfelkészítés tükrében Doktori (PhD) Értekezés. Nemzeti Közszolgálati Egyetem

[31] Bonnyai, T. (2013). Létfontosságú rendszerek és rendszerelemek katasztrófa-érzékenysége. Műszaki katonai közlöny, 23(1), 204–223.

[32] NIPP 2013, Partnering for Critical Infrastructure Security and Resilience. (2013). U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf (letöltés ideje: 2023.05.02.)

[33] National Risk Register. (2020). HM Goverment. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/952959/6.6920_CO_CCS_s_National_Risk_Register_2020_11-1-21-FINAL.pdf (letöltés ideje: 2023.05.02.)

[34] Risk Management Guide for Critical Infrastructure Sectors. (2010). Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rsk-mngmnt-gd/rsk-mngmnt-gd-eng.pdf (letöltés ideje: 2023.05.02.)

[35] Pallagi, A., Pető, R., & Hronyecz, E. (2023). Increasing the resilience of critical infrastructures with defense zone system. In SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics (pp. 549–554).

[36] McMillan, D. (2014) Disruption at Gatwick Airport. https://www.gatwickairport.com/globalassets/publicationfiles/business_and_community/all_public_publications/2014/mcmillan_report_feb14.pdf (letöltve: 2023.05.02.)

[37] Mufson, S. (2012) 3 nuclear power reactors shut down during Hurricane Sandy. Washington Post. https://www.washingtonpost.com/business/economy/3-nuclear-power-reactors-shut-down-during-sandy/2012/10/30/7ddd3a94-22b6-11e2-8448-81b1ce7d6978_story.html (leöltve: 2023.05.02.)

[38] DesRoches, R., Comerio, M., Eberhard, M., Mooney, W., & Rix, G. J. (2011). Overview of the 2010 Haiti Earthquake. In Earthquake Spectra (Köt. 27, Issue 1_suppl1, o. 1–21). SAGE Publications. https://doi.org/10.1193/1.3630129

[39] Fukushima accident summary. (2011). https://www.britannica.com/summary/Fukushima-accident (letöltve:2023.05.02.)

[40] 2023 Turkey-Syria Earthquake. (2023). https://disasterphilanthropy.org/disasters/2023-turkey-syria-earthquake/?gclid=Cj0KCQjwmtGjBhDhARIsAEqfDEfgjdIwtJJ4yPNZdAAU5vpJ2k4GKewg7BJjLERYgpDQWEbyeByRcQgaAhEYEALw_wcB (letöltve: 2023.05.02.)

[41] 2011. Report on Eyjafjallajokull (Iceland). In R. Wunderman (Szerk.), Bulletin of the Global Volcanism Network (Köt. 36, Issue 4). Smithsonian Institution. https://doi.org/10.5479/si.gvp.bgvn201104-372020

[42] Soma, S. (1975). In Journal of Geography (Chigaku Zasshi) (Köt. 84, Issue 4, o. 204–217). Tokyo Geographical Society. https://doi.org/10.5026/jgeography.84.4_204

[43] Tarik, M. (2022). The worst solar storms in history. https://www.space.com/12584-worst-solar-storms-sun-flares-history.html#section-2022-a-very-expensive-storm (letöltve: 2023.05.02.)

[44] Case Study: St. Francis Dam (California, 1928) https://damfailures.org/case-study/st-francis-dam-california-1928/ (letöltve: 2023.05.02.)

[45] Chernobyl Accident 1986. https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx (letöltve: 2023.05.02.)

[46] How the Ohio Train Derailment and Its Aftermath Unfolded. (2023). The New York Times. https://www.nytimes.com/article/ohio-train-derailment-timeline.html (letöltve: 2023.05.02.)

[47] Byers, M., Wright, E., Boley, A., & Byers, C. (2022). Unnecessary risks created by uncontrolled rocket reentries. In Nature Astronomy (Köt. 6, Issue 9, o. 1093–1097). Springer Science and Business Media LLC. https://doi.org/10.1038/s41550-022-01718-8

[48] Nagy, R. (2010). A klímaváltozás hatása a kritikus infrastruktúrák védelmére. NEMZET ÉS BIZTONSÁG: BIZTONSÁGPOLITIKAI SZEMLE, 3(2), 35–44.

[49] Krista, C. (2021) Uttarakhand flood was caused by rare rock and glacier avalanche. https://www.newscientist.com/article/2280645-uttarakhand-flood-was-caused-by-rare-rock-and-glacier-avalanche/ (letöltve: 2023.05.02.)

[50] Tomalska, A. (2022). Preparing critical infrastructure for the future: Lessons learnt from the Covid-19 pandemic. In Security and Defence Quarterly. War Studies University. https://doi.org/10.35467/sdq/146603

[51] European Commmossion. (2022). https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/statistics-migration-europe_en (letöltve: 2023.05.02.)

[52] A tervezett üzemidő lejártát követő üzemeltetés engedélyezése a paksi atomerőmű 4. Számú blokkján (2017). Országos Atomenergetikai Hivatal. https://www.haea.gov.hu/web/v3/oahportal.nsf/96CD56566A00C7D9C12581230024CB74/$File/OAH_k%C3%B6z%C3%A9rthet%C5%91_%C3%B6sszefoglal%C3%B3%204.bl_05.08_v%C3%A9gl.pdf (letöltve: 2023.05.02.)

[53] Nagy, R. (2016). A kritikus infrastruktúrák elleni lehetséges radiológiai terrortámadások. MAGYAR RENDÉSZET, 16(6), 145–153.

[54] Nagy R. (2011) A kritikus infrastruktúra védelme elméleti és gyakorlati kérdéseinek kutatása. Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem Bolyai János Katonai Műszaki Kar Hadmérnöki Doktori Iskola, Budapest

[55] Palicz, T., Sas, T., Tisóczki, J., Bencsik, B., & Joó, T. (2020). „Pénzt vagy életet!” – Zsarolóvírusok az egészségügyi informatikai rendszerekben. In Orvosi Hetilap (Köt. 161, Issue 36, o. 1498–1505). Akademiai Kiado Zrt. https://doi.org/10.1556/650.2020.31788

[56] Nguyen, H. P. D., Ruiz, L., & Rajnai, Z. (2021). Industrial Control System (ICS): The General Overview of the Security Issues and Countermeasures. In Informatics and Cybernetics in Intelligent Systems (o. 412–419). Springer International Publishing. https://doi.org/10.1007/978-3-030-77448-6_39

[57] Miranda, B. (2023) Key details behind Nord Stream pipeline blasts revealed by scientists https://www.theguardian.com/business/2023/sep/26/nord-stream-pipeline-blasts-key-details-revealed-by-scientists (letöltve 2023.10.01.)

[58] Pocskai, Á. (2012) Gondolatok a kritikus infrastruktúrák terrortámadással szembeni védelmének szabályozásáról. Terrorelhárítási Központ. https://www.epa.oszk.hu/02900/02932/00001/pdf/EPA02932_terror_elharitas_2012_1_02.pdf (letöltve: 2023.05.02.)

[59] Terror Profile Hungary. (2021). Council of Eupean Committee on Counter-terrorism. https://rm.coe.int/profile-hungary-may-2021-2767-7286-2979-v-2/1680a2b116 (letöltés ideje: 2023.05.02.)

[60] Global Terrorism Index 2023. (2023). Institute for Economics & Peace. https://www.economicsandpeace.org/wp-content/uploads/2023/03/GTI-2023-web.pdf (letöltve: 2023.05.02.)

[61] Szabo, A., & Rajnai, Z. (2017). The review of the external risk factors during the operation training plan of the security guards. In 2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY). IEEE. https://doi.org/10.1109/sisy.2017.8080583

[62] 1997. évi CLIX. törvény a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról.

[63] Bederna, Z., Rajnai, Z., & Szadeczky, T. (2020). Attacks against energy, water and other critical infrastructure in the EU. In 2020 IEEE 3rd International Conference and Workshop in Óbuda on Electrical and Power Engineering (CANDO-EPE). IEEE. https://doi.org/10.1109/cando-epe51100.2020.9337751

[64] List of conflicts in Europe. Wikipedia. https://en.wikipedia.org/wiki/List_of_conflicts_in_Europe (letöltés ideje: 2023.05.02.)

[65] Beckvard, H. P. (2022). Protecting critical infrastructure and critical information infrastructure. In contemporary military challenges (Köt. 2022, Issue 2, o. 15–28). Walter de Gruyter GmbH. https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.1

[66] Muha, L. (2007). A Magyar Köztársaság kritikus információs infrastruktúráinak védelme Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem

[67] Haig, Zs. & Kovács, L. (2012) Kritikus infrastruktúrák és kritikus információs infrastruktúrák. Tanulmány. Nemzeti Közszolgálati Egyetem. https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf (letöltés ideje: 2023.05.02.)

[68] Őszi, A. (2019). A biometrikus azonosítás helye és szerepe az e-kereskedelemben PhD (Disszertáció), Óbudai Egyetem

[69] Nyikes, Z., & Rajnai, Z. (2015). Big data, as part of the critical infrastructure. In 2015 IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY). IEEE. https://doi.org/10.1109/sisy.2015.7325383

[70] James, F. B. & Eugene, T. (2012). Risk Analysis and the Security Survey Fourth Edition. Elseiver Inc. ISBN 978-0-12-382233-8

[71] Rehak, D., Markuci, J., Hromada, M., & Barcova, K. (2016). Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system. In International Journal of Critical Infrastructure Protection (Köt. 14, o. 3–17). Elsevier BV. https://doi.org/10.1016/j.ijcip.2016.06.002

[72] Pataki, J. (2020). A terrorizmus, mint biztonsági probléma, a kritikus infrastruktúra védelmi szabályai tükrében Doktori (PhD) értekezés. Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtudományi Doktori Iskola

[73] Muha, L., & Tóth, G. N. (2011). A bankbiztonság vizsgálata kockázatelemzéssel. HADMÉRNÖK, 6(4), 204–215. http://www.hadmernok.hu/2011_4_muha_toth.pdf (letöltve: 2023.05.02.)

[74] Rajnai, Z., & Fregan, B. (2016). Kritikus infrastruktúrák védelme (jogi szabályozás). In Műszaki Tudományos Közlemények (Köt. 5, o. 349–352). Muszaki Tudomanyos Kozlemenyek. https://doi.org/10.33895/mtk-2016.05.78

[75] Nagy, R. (2006). A kritikus infrastruktúravédelme és annak katasztrófavédelmi aspektusai a terrorizmus tükrében. Kard És Toll: Válogatás A Hadtudomány Doktoranduszainak Tanulmányaiból, (3), 56–64.

[76] Marina, M., Toni, M. & Robert, M. (2019). Critical infrastructure: Concept and security challenges. Friedrich Ebert Foundation, office Skopje. ISBN 978-9989-109-93-5

[77] Nunes-Vaz, R., & Lord, S. (2014). Designing physical security for complex infrastructures. In International Journal of Critical Infrastructure Protection (Köt. 7, Issue 3, o. 178–192). Elsevier BV. https://doi.org/10.1016/j.ijcip.2014.06.003

[78] Pallagi, A., & Kovács, T. (2019). Kritikus infrastruktúrák komplex biztonságvédelmi rendszereinek tervezése, kialakítása, különös tekintettel a beléptetőrendszerek alkalmazására. In Hadmérnök (Köt. 14, Issue 4, o. 35–45). Hadmérnök. https://doi.org/10.32567/hm.2019.4.2

[79] Pető, R. (2017). Protection of Borders and Installation against vehicle-based. ÓBUDA UNIVERSITY E-BULLETIN.

[80] Ronyecz, L., Bognár, B., & Révai, R. (2018). A létfontosságú rendszerelemek közötti interdependencia kockázatainak elemzése, különös tekintettel az egészségügyi ágazat rendszerelemeire és létesítményeire. Hadmérnök, 13(1), 133–142.

[81] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

[82] Bognár, B., Bonnyai. T. & Vámosi, Z. (2019). Kritikus infrastruktúrák védelme I.. Dialóg Campus Kiadó. ISBN 978-615-5945-28-1

[83] Chen, X. (2023). Risk-based Access Control Model for Hospital Information Systems. In Frontiers in Computing and Intelligent Systems (Köt. 2, Issue 3, o. 82–84). Darcy & Roy Press Co. Ltd. https://doi.org/10.54097/fcis.v2i3.5315

[84] Biringer, B., & Danneels, J. J. (2001). Risk Assessment Methodology for Protecting Our Critical Physical Infrastructures. In Risk-Based Decisionmaking in Water Resources IX. Ninth United Engineering Foundation Conference on Risk-Based Decisionmaking in Water Resources. American Society of Civil Engineers. https://doi.org/10.1061/40577(306)4

[85] Garcia, M. L.. (2007) Design and Evaluation of Physical Protection Systems, 2nd Edition. Butterworth-Heinemann. ISBN: 9780080554280

[86] Horváth-Kálmán, E., & Elek, B. (2023). Risks and the management of construction in the environment of nuclear facilities. ACTA TECHNICA JAURINENSIS, 0–8. http://doi.org/10.14513/actatechjaur.00707

[87] Chouinard, P., & Giddings, J. (2023). A Systems Approach to Critical Infrastructure Resilience. In Safety and Security Science and Technology (o. 37–52). Springer International Publishing. https://doi.org/10.1007/978-3-031-21530-8_3

[88] Filkorn, J. (2009). Beléptető rendszerek. Seawing Kft. https://doksi.hu/get.php?lid=6516 (Letöltve: 2023.05.10.)

[89] Berek, L., Berek, T. & Berek, L.. (2016). Személy- és vagyonbiztonság. Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar. ISBN 978-615-5460-94-4

[90] Berek, L.. (2014). Biztonságtechnika. Nemzeti Közszolgálati Egyetem.

[91] Lukács, Gy., Gábor, L. (2002.). Új Vagyonvédelmi Nagykönyv. CEDIT 2000 Kft.. ISBN: 963-8180-39-0

[92] Ferraiolo, H., Mehta, K., Ghadiali, N., Mohler, J., Johnson, V., & Brady, S. (2018). Guidelines for the use of PIV credentials in facility access. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-116r1

[93] Electronic Access Control. (2017). Elsevier. https://doi.org/10.1016/c2015-0-04450-1

[94] András, P., & Éva, B. (2019). Plan and design of complex security systems for critical infrastructures, with particular regard to the use of access control systems. In Kiberbiztonság – Cybersecurity 2. (Vol. 2, pp. 240–246).

[95] Dan M. Bowers. (1988) Access Control and Personal Identification Systems. Elsevier. https://doi.org/10.1016/c2013-0-04278-8

[96] The evolution of credential technologies. (2021). HID Global Corporation. https://www.hidglobal.com/doclib/files/resource_files/pacs-card-evolution-ig-en.pdf (letöltés ideje:2023.01.02.)

[97] Camilla, A. (2023) The history of door access control systems. https://www.2n.com/en_US/blog/the-history-of-door-access-control-systems (letöltés ideje: 2023.05.05.)

[98] Wang, X., Wang, X., Yan, Y., Liu, J., & Zhao, Z. (2022). RF-Access: Barrier-Free Access Control Systems with UHF RFID. In Applied Sciences (Köt. 12, Issue 22, o. 11592). MDPI AG. https://doi.org/10.3390/app122211592

[99] Abid, A., Cheikhrouhou, S., Kallel, S., Tari, Z., & Jmaiel, M. (2022). A Smart Contract-Based Access Control Framework For Smart Healthcare Systems. In The Computer Journal. Oxford University Press (OUP). https://doi.org/10.1093/comjnl/bxac183

[100] Pallagi, A. & Persely, A. (2023). Methodological and Health Reasons for Unsuccessful Biometric Identification. Interdisciplinary Description of Complex Systems, 21 (2), 206-213. https://doi.org/10.7906/indecs.21.2.10

[101] Fialka, G., & Kovács, T. (2016). The vulnerability of biometric methods and devices. Annals of faculty of engineering hunedoara: international journal of engineering, 14(3), 45–48.

[102] Ikponmwosa, O., S., O., Jeffrey Okieke, U., E. E., E., B. P., D., D. I., A., U.G., A., A. O., O., A.O., O., O.J., E., G. I., E., … K. U, O. (2023). Face recognition system for automatic door access control. In Engineering and Technology Journal (Köt. 08, Issue 02, o. 1981–1985). Everant Journals. https://doi.org/10.47191/etj/v8i2.03

[103] Shi, W., Li, G., Li, X., & Mitrouchev, P. (2023). Intelligent Access Control System Base on Face Recognition. In Advanced Manufacturing and Automation XII (o. 399–405). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-9338-1_49

[104] Tóth, A., & Tóth, L.. (2014) Biztonságtechnika. Nemzeti Közszolgálati Egyetem. ISBN 978-615-5305-56-6

[105] MSZ EN 50133-1:2000 Riasztórendszerek. Hozzáférés-ellenőrző rendszerek biztonságtechnikai alkalmazásokhoz. 1. rész: A rendszerrel szemben támasztott követelmények.

[106] MSZ EN 50133-7:2000 Riasztórendszerek. Beléptetőrendszerek biztonságtechnikai alkalmazásokhoz. 7. rész: Alkalmazási irányelvek

[107] MSZ EN 50133-2-1:2001 Riasztórendszerek. Beléptetőrendszerek biztonságtechnikai alkalmazásokhoz. 2-1. rész: Részegységek általános követelményei

[108] MSZ EN 50133-1:1996/A1:2003 Riasztórendszerek. Hozzáférés-ellenőrző rendszerek biztonságtechnikai alkalmazásokhoz. 1. rész: A rendszerrel szemben támasztott követelmények

[109] MSZ EN 50133-1:2006 Riasztórendszerek. Beléptetőrendszerek biztonságtechnikai alkalmazásokhoz. 1. rész: Rendszerkövetelmények

[110] MSZ EN 50130-4:2011 Riasztórendszerek. 4. rész: Elektromágneses összeférhetőség. Termékcsalád-szabvány: Tűzjelző, behatolásjelző, támadásjelző, zárt láncú (CCTV) televíziós megfigyelőrendszerek, beléptető és személyi segélyhívó rendszerek egységeinek zavartűrési követelményei

[111] MSZ EN 60839-11-1:2013 Riasztórendszerek és elektronikus biztonsági rendszerek. 11-1. rész: Elektronikus beléptető rendszerek. A berendezésekre és készülékekre vonatkozó követelmények (IEC 60839-11-1:2013)

[112] MSZ EN 50130-4:2011/A1:2015 Riasztórendszerek. 4. rész: Elektromágneses összeférhetőség. Termékcsaládszabvány: Tűzjelző, behatolásjelző, támadásjelző, zárt láncú (CCTV) televíziós megfigyelőrendszerek, beléptető és személyi segélyhívó rendszerek egységeinek zavartűrési követelményei

[113] MSZ EN 60839-11-2:2015 Riasztórendszerek és elektronikus biztonsági rendszerek. 11-2. rész: Elektronikus beléptető rendszerek. Alkalmazási irányelvek (IEC 60839-11-2:2014)

[114] MSZ EN 60839-11-31:2017 Riasztórendszerek és elektronikus biztonsági rendszerek. 11-31. rész: Elektronikus beléptető rendszerek. A webszolgáltatásokon alapuló alaprendszer interoperabilitási protokollja (IEC 60839-11-31:2016)

[115] MSZ EN 60839-11-32:2017 Riasztórendszerek és elektronikus biztonsági rendszerek. 11-32. rész: Elektronikus beléptető rendszerek. A webszolgáltatásokon alapuló beléptetés monitorozása (IEC 60839-11-32:2016)

[116] MSZ EN IEC 60839-11-5:2021 - Riasztórendszerek és elektronikus biztonsági rendszerek. 11-5. rész: Elektronikus beléptetőrendszerek. Nyílt felügyelt eszközprotokoll (OSDP) (IEC 60839-11-5:2020)

[117] MSZ EN IEC 60839-11-33:2022 - Riasztórendszerek és elektronikus biztonsági rendszerek. 11-33. rész: Elektronikus beléptetőrendszerek. A webszolgáltatásokon alapuló beléptetés konfigurálása (IEC 60839-11-33:2021)

[118] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól

[119] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[120] 169/2010. (V. 11.) Korm. rendelet a polgári légiközlekedés védelmének szabályairól és a Légiközlekedés Védelmi Bizottság jogköréről, feladatairól és működésének rendjéről

[121] 53/2015. (IX. 24.) BM rendelet az egységes elektronikuskártya-kibocsátási keretrendszerről szóló 2014. évi LXXXIII. törvény végrehajtásához szükséges kapcsolódási, műszaki, technológiai, biztonsági előírásokról, követelményekről és a hitelesítési rendről

[122] 33/2021. (IX. 15.) MNB rendelet a fizetési rendszer működtetése tevékenységre vonatkozó részletes szabályokról

[123] 78/2015. (XII. 23.) BM rendelet az arcképelemző rendszer működtetésének részletes szabályairól

[124] 62/2009. (XII. 17.) IRM rendelet a Közjegyzői Levéltár tevékenységével összefüggő szakmai követelményekről

[125] 8/2021. (XI. 18.) OBH utasítás a bírósági épületek fizikai védelmi rendszereinek feltételeiről

[126] Osei-Kyei, R., Tam, V., Ma, M., & Mashiri, F. (2021). Critical review of the threats affecting the building of critical infrastructure resilience. In International Journal of Disaster Risk Reduction (Köt. 60, o. 102316). Elsevier BV. https://doi.org/10.1016/j.ijdrr.2021.102316

[127] Pallagi, A., & Kovács, T. (2019). Kritikus infrastruktúrák komplex biztonságvédelmi rendszereinek tervezése, kialakítása, különös tekintettel a beléptetőrendszerek alkalmazására. In Hadmérnök (Köt. 14, Issue 4, o. 35–45). Hadmérnök. https://doi.org/10.32567/hm.2019.4.2

[128] Pallagi, A., Pető, R., & Hronyecz, E. (2023). The fundamental requirements of the defense zones of critical infrastructures. In ICCECIP 2023 5th International Conference on Central European Critical Infrastructure Protection

[129] Puskas, B., & Rajnai, Z. (2015). Requirements of the Installation of the Critical Informational Infrastructure and Its Management. In Interdisciplinary Description of Complex Systems (Köt. 13, Issue 1, o. 48–56). Croatian Interdisciplinary Society. https://doi.org/10.7906/indecs.13.1.7

[130] Bruce, S.. Schneier a biztonságról. (2008). HVG Könyvek. ISBN: 978-963-304-026-3

[131] Lee, B., & Amanda, B. (2017). Defensive Security Handbook. O'Reilly Media Inc.. ISBN: 9781491960332

[132] Berek, L., & Hódosi, V. (2019). Veszélyes objektumok biztonsági rendszereinek ellenőrzése. In Hadmérnök (Köt. 14, Issue 3, o. 5–11). Hadmernok. https://doi.org/10.32567/hm.2019.3.1

[133] MSZ EN 1627:2021 Bejárati ajtók, ablakok, függönyfalak, rácsok és redőnyök. Betörésállóság. Követelmények és osztályba sorolás

[134] MSZ EN 356:2000 Építési üveg. Biztonsági üvegezés. Kézi támadással szembeni ellenálló képesség vizsgálata és osztályozása

[135] MSZ EN 60529:2015 Villamos gyártmányok burkolatai által nyújtott védettségi fokozatok (IP-kód) (IEC 60529:1989)

[136] MSZ IEC 62262:2023 Villamos gyártmányok burkolatai által nyújtott védettségi fokozatok külső mechanikai hatások ellen (IK-kód)

[137] EN 1522:1998 Ablakok, ajtók, redőnyök és árnyékolók - Lövedékállósága - Követelmények és besorolás

[138] Pandey, S. K. &, Mustafa, K. (2012). Access Control and Rights related Risk Assessment. International Journal of Engineering Research and Applications (IJERA). pp.1174-1178. https://www.ijera.com/papers/Vol2_issue1/GG2111741178.pdf (letöltve: 2023.01.04.)

[139] Krishna Khanth, N., Jain, S., & Madan, S. (2023). Sentinel: An Enhanced Multimodal Biometric Access Control System. In Big Data Analytics in Astronomy, Science, and Engineering (o. 95–109). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-28350-5_8

8 Publikációk

8.1 A tézispontokhoz kapcsolódó tudományos közlemények

PA1. Pallagi, A., & Kovács, T. (2019). Kritikus infrastruktúrák komplex biztonságvédelmi rendszereinek tervezése, kialakítása, különös tekintettel a beléptetőrendszerek alkalmazására. In Hadmérnök (Köt. 14, Issue 4, o. 35–45). Hadmérnök. https://doi.org/10.32567/hm.2019.4.2

PA2. András, P., & Éva, B. (2019). Plan and design of complex security systems for critical infrastructures, with particular regard to the use of access control systems. In Kiberbiztonság – Cybersecurity 2. (Vol. 2, pp. 240–246).

PA3. Pallagi, A., Pető, R., & Hronyecz, E. (2023). Increasing the resilience of critical infrastructures with defense zone system. In SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics (pp. 549–554). https://doi.org/10.1109/SISY60376.2023.10417949

PA4. Pallagi, A., Pető, R., & Hronyecz, E. (2023). The fundamental requirements of the defense zones of critical infrastructures. In ICCECIP 2023 5th International Conference on Central European Critical Infrastructure Protection

8.2 További tudományos közlemények (opcionális)

PA5. Pallagi, A. & Persely, A. (2023). Methodological and Health Reasons for Unsuccessful Biometric Identification. Interdisciplinary Description of Complex Systems, 21 (2), 206-213. https://doi.org/10.7906/indecs.21.2.10

PA6. Pallagi, A. (2019). Az optimális/ideális beléptető rendszer kiválasztása. DETEKTOR PLUSZ, 26(6), 18–18.

PA7. Pallagi, A. (2019). A biztonságtudatosság fejlesztésének szerepe az oktatási rendszerben. In Mobilitás (pp. 653–660).

PA8. Andras, P. (2020). Security awareness in the education system. In Mérnöki Szimpózium a Bánkin Előadásai (pp. 101–112).