ISSN 2676-9042

Vol 6, No 2, 2024.

2024, VI. évf. 2. szám

Safety and Security Sciences Review

international, peer-reviewed, professional and scientific journal of safety and security sciences

Biztonságtudományi Szemle

a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

https://biztonsagtudomanyi.szemle.uni-obuda.hu

On the cover can be seen | A borítón
BORS Györgyi
painter/festőművész
Touch painting | **Érintés** című festménye látható

The Military Science Committee of the 9th Department of Economics and Law of the Hungarian Academy of Sciences classified our journal as a "C" category.

Folyóiratunkat a Magyar Tudományos Akadémia IX. Gazdaság- és Jogtudományok Osztályának Hadtudományi Bizottsága „C" kategóriás folyóiratnak minősítette.

The Safety and Security Sciences Review is a classified journal by Hungarian Science Bibliography.

A Biztonságtudományi Szemle a Magyar Tudományos Művek Tára (MTMT) által minősített folyóirat.

Our journal is indexed by the following databases

Folyóiratunkat a következő adatbázisok indexelik

EBSCO

Electronic Periodicals Archive & Database | Elektronikus Periodika Adatbázis
https://epa.oszk.hu/04100/04186

Hungarian Periodicals Table of Contents Database | Magyar folyóiratok tartalomjegyzékeinek kereshető adatbázisa
https://matarka.hu/szam_list.php?fsz=2267&nyelv=hun

Digital Archives of Óbuda University | Óbudai Egyetem Digitális Archívum

National Széchenyi Library Digital Library | OSZK Digitális Könyvtár
https://oszkdk.oszk.hu/DRJ/39186

Global Serials Directory | Globális Sorozatok Könyvtára
http://ulrichsweb.serialssolutions.com/title/1678275514425/863974

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

COLUMNS	ROVATOK
Material Safety	Anyagbiztonság
Philosophy and History of the Safety and Security	Biztonságfilozófia és -történet
Security Policy	Biztonságpolitika
Security Systems	Biztonságtechnika
Security Awareness	Biztonságtudatosság
Domotics	Domotika
Health Security	Egészségbiztonság
Food Safety	Élelmiszer-biztonság
Economic Security	Gazdasági biztonság
War Security and Law Enforcement	Hadbiztonság és rendvédelem
Information Security	Információbiztonság
Industrial and Operational Safety	Ipar- és üzembiztonság
Legal and Social Security	Jog- és társadalombiztonság
Book Review	Könyvismertetés
Security of Environment	Környezetbiztonság
Traffic Safety	Közlekedésbiztonság
Facility Security	Létesítménybiztonság
Private Security	Magánbiztonság
Artificial Intelligence	Mesterséges intelligencia
Safety and Security in General	Munkabiztonság
Technical Security	Műszaki biztonság
Fire Safety and Disaster Management	Tűzbiztonság és katasztrófavédelem

The **aim** of the journal is to publish studies, research reports, book reviews for professionals working in the field of security science or related scinces, or for those interested in the subject of the broadly disciplinary framework of military technical sciences, and for security awareness and developing a safety culture. We know that the cultivation of security sciences includes the study of the history of military and law enforcement security, as well as the knowledge of the historical aspects of our field of science, and its development. We are working towards to present the latest theoretical models and empirical research findings in our journal. We believe that our Journal and our authors can contribute to the creation of a world that enables a (more) secure life for all the inhabitants of the Earth by knowing the historical past and examining the events of the present with precision and accuracy.

Published quarterly, typically in Hungarian, occasionally in a foreign language. Special and/or thematic issues related to conferences and topics are occasionally published in Hungarian or in foreign languages.

Only those papers will be published which reviewed by two independent reviewers and recommended suitable for publication in the Safety and Security Sciences Review. The submitted manuscripts must meet the requirements both of the form and the content which can be found in the journal's website. Please note: we will not return unapproved manuscripts.

The studies of the staff and students of Óbuda University, published in the Journal, are recorded by the staff of the University Library at the Hungarian Scientific Works Library (MTMT).

A **folyóirat célja** a biztonságtudomány területén, vagy ahhoz kapcsolódó területeken dolgozó szakemberek, vagy a téma iránt érdeklődők számára a katonai műszaki tudományok, s így a biztonságtudomány tágan értelmezett diszciplináris keretébe tartozó tanulmányok, kutatási jelentések, beszámolók, könyvismertetők megjelentetése, s ennek révén a biztonságtudatosság és a biztonsági kultúra fejlesztése. Tudjuk, hogy a biztonságtudományok művelésébe beletartozik a had-, rendészet- és biztonságtörténet vizsgálata, tudományterületünk történeti és történelmi vetületeinek, s így fejlődésének megismerése. Azon dolgozunk, hogy Folyóiratunkban bemutassuk jelenkorunk legújabb teoretikus modelljeit és empirikus kutatási eredményeit. Hiszünk benne, hogy Folyóiratunk és szerzőink a történelmi múlt ismeretével, a jelenkor eseményeinek precíz és akkurátus vizsgálatával hozzá tudunk járulni egy olyan világ megteremtéséhez, amelyik lehetővé teszi a Föld minden lakója számára a biztonságos(abb) életet.

Megjelenés negyedévente, jellemzően magyar, eseti jelleggel idegen nyelven. Konferenciákhoz és témákhoz kapcsolódóan különszámok, tematikus számok alkalmi jelleggel magyar, vagy idegen nyelven jelennek meg.

A Biztonságtudományi Szemle folyóiratban csak két független lektor által lektorált és megjelentetésre alkalmasnak tartott tanulmányok jelenhetnek meg. A beküldött kéziratoknak formai és tartalmi szempontból egyaránt meg kell felelnie a Folyóirat weboldalán közölt elvárásoknak. El nem fogadott kéziratokat nem áll módunkban visszaküldeni.

Az Óbudai Egyetem munkatársainak és hallgatóinak a Folyóiratban megjelent tanulmányait az Egyetemi Könyvtár munkatársai rögzítik a Magyar Tudományos Művek Tárában (MTMT).

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

ISSN 2676-9042
https://biztonsagtudomanyi.szemle.uni-obuda.hu

Editorial office | Szerkesztőség
Óbudai Egyetem
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
Biztonságtudományi Doktori Iskola
1081 Budapest, Népszínház utca 8.

Publisher | Kiadó
Óbudai Egyetem, 1034 Budapest, Bécsi út 96/B.

Responsible for publishing | A kiadásért felel
Prof. Dr. KOVÁCS Levente
Rector of the Óbuda University | az Óbudai Egyetem rektora

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

Vol 6, No 2, 2024. | **2024. VI. évf. 2. szám**

Authors of this issue | **E számunk szerzői**

BENDIÁK István

bendiak.istvan@uni-obuda.hu

I graduated in electrical engineering at the Kandó Kálmán Faculty of Electrical Engineering at the Óbuda University, specializing in control technology at the BSc and MSc level. My field of expertise is Electric machines and drives, rotary machine diagnostics, signal processing. I am currently a PhD student Doctoral School for Safety and Security Sciences Óbuda University. My workplace: University Óbuda Kandó Kálmán Faculty of Electrical Engineering Institute of Automation and Energy Systems Department of Automation, Budapest, Hungary. Subjects taught: Electrical machines BSc, MSc, electrical machines and drives BSc, electrical drives MSc. I have been dealing with electric machines since 2010 in various positions, maintenance, testing, design, diagnostics, education.

Az Óbudai Egyetem Kandó Kálmán Villamosmérnöki Karon végeztem villamosmérnök szakot BSc és MSc szinten irányítástechnika specializáción. Szakterületem a villamos gépek és hajtások, forgógép diagnosztika, jelfeldolgozás. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola hallgatója vagyok. Munkahelyem a Kandó Kálmán Villamosmérnöki Kar Automatizálási és Energiarendszerek Intézet Automatika Tanszéke. Oktatott tárgyak: Villamos gépek BSc, MSc, villamos gépek és hajtások BSc, villamos hajtások MSc. Villamos gépekkel 2010 óta foglalkozom különböző pozíciókban, karbantartó, tesztelő, tervező, diagnosztika, oktatás.

BEREK László

berek.laszlo@uni-obuda.hu

László BEREK graduated from Eötvös Loránd University as an informatics librarian, and later earned qualifications as a systems IT specialist and library expert. He defended his PhD dissertation at the Doctoral School of Safety Sciences at Óbuda University in 2024. Over the past 20 years, he has gained experience in academic and university libraries, and since 2015 he has been Director of the University Library of Óbuda University. His primary research areas include online scientific communication security, science ethics, plagiarism- and AI-generated text detection, university rankings, and related scientometrics fields. He is the author of three university textbooks, which are used in the doctoral programs of two doctoral schools at Óbuda University. He is also an instructor for the Research Publication Knowledge course at the Doctoral School of Innovation Management. He has developed several e-learning courses over the past few years. He is a member of five committees of the Óbuda University: the Scientific Council, the Ranking Committee, the Greenmetric Committee, the IT Committee, and the AI Transition Committee. He also serves as a member of the Technical Librarians Section Board of the Hungarian Librarians Association.

BEREK László az Eötvös Loránd Tudományegyetemen végzett informatikus könyvtárosként, majd rendszerinformatikusi és könyvtári szakértői képesítést is szerzett. Doktori disszertációját az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában védte meg 2024-ben. Az elmúlt 20 évben tudományos és egyetemi könyvtárakban szerzett tapasztalatokat, 2015. óta az Óbudai Egyetem Egyetemi Könyvtárának igazgatója. Elsődleges kutatási területei közé tartozik az online tudományos kommunikáció biztonsága, a tudományetika, a plágiumellenőrzés és a mesterséges intelligencia által generált szövegek detektálása, az egyetemi rangsorok és a kapcsolódó tudománymetriai területek. Három egyetemi tankönyv szerzője, amelyeket az Óbudai Egyetem két doktori iskolájának doktori programjában használnak. Emellett az Innovációmenedzsment Doktori Iskola Kutatási publikációs ismeretek kurzusának oktatója. Az elmúlt években több e-learning kurzust is kidolgozott. Az Óbudai Egyetem öt bizottságának tagja: Tudományos Tanács, Ranking Bizottság, Greenmetric Bizottság, Informatikai Bizottság és Mesterséges Intelligencia Átállási Bizottság. A Magyar Könyvtárosok Egyesülete Műszaki Könyvtáros Szekciójának elnökségi tagja.

BODOR Károly

bodor.karoly@ek.hun-ren.hu

I am Károly BODOR from the HUN-REN Centre for Energy Research (17 years) and ELI ALPS (12 years). I have been involved in the radiation protection design and implementation of ELI ALPS since 2008. It became immediately clear that in addition to traditional radiation protection knowledge, new procedures should be developed, and new knowledge and visions, an interdisciplinary approach, would be needed. To this end, I participated in the meetings and conferences held during the preparatory phase of ELI, and I mastered the so-called FLUKA Monte Carlo code. In the course of my work, I led several diploma topics with my colleague and supervisor Dr. Péter ZAGYVAI. As a radiation protection expert and designer, I support the implementation of radiation protection at ELI ALPS. Methods must be developed and practiced. The results of the research carried out in the HUN-REN EK Nuclear Security Department can be used to strengthen the radiation protection of ELI ALPS, which is one of the reasons why we started developing the virtual surface contamination system.

BODOR Károly vagyok a HUN-REN Energiatudományi Kutatóközpont (17 év) és az ELI ALPS munkatársa (12 év). Az ELI ALPS sugárvédelmi rendszerének tervezésébe és megvalósításába 2008-ban kapcsolódtam be. Rögtön világossá vált, hogy a hagyományos sugárvédelmi tudás mellett új eljárásokat kell kidolgozni, illetve új ismeretekre és látásmódra, interdiszciplináris megközelítésre lesz szükség. Ennek érdekében részt vettem az ELI előkészítési fázisában megtartott találkozókon, konferenciákon, valamint elsajátítottam az akkor még Magyarországon nem használt ún. FLUKA Monte Carlo kódot. Munkám során több diplomatémát vezettem Dr. ZAGYVAI Péter kollégámmal, témavezetőmmel. Sugárvédelmi szakértőként és tervezőként támogatom az ELI ALPS üzemelését. Ahhoz, hogy sugárvédelmi szempontból a lehető legbiztonságosabb legyen a tényleges üzemelés, meg kell értenünk az ELI-ben a lézeranyag kölcsönhatás során zajló folyamatokat. Módszereket kell kidolgozni, melyeket be kell gyakorolni. A HUN-REN EK Sugárbiztonsági Laboratóriumában folyó kutatás eredményei felhasználhatók az ELI ALPS sugárvédelmének megerősítésében, többek között ezért is kezdtük el megvalósítani a virtuális felületi szennyezettség mérő rendszert.

CSALÓTZKY Zsolt

csalotzky.zsolt@ek.hun-ren.hu

I'm a computer science graduate from Óbuda University of Budapest, Hungary. Currently I am working in software development at HUN-REN Centre for Energy Research. Within the institute, initially I was involved in programming user interface for a detector development project at Nanosensors Laboratory. At present I'm working on the development of embedded systems and server applications for a virtual radiation source system at the Nuclear Security Department.

Az Óbudai Egyetem Neumann János Informatikai Karának mérnökinformatikus alapképzésén végeztem 2020-ban. Jelenleg a HUN-REN Energiatudományi Kutatóközpontban foglalkozom szoftverfejlesztéssel. Az intézmény berkein belül, kezdetben a Nanoérzékelők Laboratóriumnál, detektorfejlesztéssel kapcsolatos projekt felhasználói felületének programozásában vettem részt. Jelenleg a Sugárbiztonsági Laboratóriumnál virtuális sugárforrás keresést támogató eszközök beágyazott rendszereinek és szerveralkalmazásának fejlesztésével foglalkozom.

DÉR Attila

der.attila@uni-obuda.hu

Attila DÉR is a student at the Doctoral School of Safety and Security Sciences at the Bánki Donát Faculty of Mechanical and Safety Engineering, University of Óbuda. He holds a degree in Certified electrical engineer from the Specialization in industrial surveillance and communication systems of Kandó Kálmán

DÉR Attila az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán lévő Biztonságtudományi Doktori Iskola hallgatója. Okleveles villamosmérnöki végzettségét a Kandó Kálmán Villamosmérnöki Karán szerezte Ipari felügyeleti és kommunikációs rendszerek specializációján. Kuta-

Faculty of Electrical of engineer. His research interests include cybersecurity, protection of critical infrastructures in particular energy supply.

tási területei a kiberbiztonság, kibervédelem, kritikus infrastruktúrák védelme különös tekintettel az energiaellátásra.

GUGOLYA László

gugolya.laszlo@uni-obuda.hu

My name is László GUGOLYA, and I am currently a master instructor at the Alba Regia Technical Faculty of Óbuda University. Additionally, I serve as the professional director and humanoid robot programmer at the Alba Innovár Digital Experience Center in Székesfehérvár. I graduated as a high school physics and mathematics teacher from József Attila University in Szeged in 1996, and I also obtained a degree as a certified programming mathematician from the same institution in 1998. In 2008, I earned a diploma as an educational evaluation expert (certified teacher) from Kodolányi College in Székesfehérvár. I am currently a correspondence student at the Doctoral School of Safety Sciences at Óbuda University. In the first half of my career, I mainly worked in secondary education, and my research was related to this field. Then, in 2012, I shifted my focus towards higher education and the teaching of programming. Initially, I dealt with pedagogical and methodological areas, and later I had the opportunity to work on the programming of robots, specifically humanoid robots. Currently, my research focuses on the introduction, integration, and safety aspects of humanoid robots in the educational field.

GUGOLYA László vagyok jelenleg az Óbudai Egyetem Alba Regia Műszaki Karának mestertanára. E mellet a székesfehérvári Alba Innovár Digitális élményközpont szakmai vezetője, humanoidrobot programozója. A szegedi József Attila Tudományegyetemen végeztem fizikai-matematika középiskolai tanárként 1996-ban, majd szintén itt okleveles programozó matematikus diplomát szereztem 1998-ban. A székesfehérvári Kodolányi Főiskolán szereztem pedagógiai értékelési szakértő (szakvizsgázott pedagógus) diplomát 2008-ban. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola levelező hallgatója vagyok. Pályafutásom első felében főleg középiskolába tevékenykedtem, kutatásaim is ehhez kapcsolódtak. Majd 2012-ben a felsőoktatás és a programozás oktatása felé vettem az irányt. Eleinte itt is pedagógiai, módszertani területekkel foglalkoztam, majd lehetőségem nyílt a robotok, a humanoid robotok programozására. Jelenleg a humanoid robotok oktatási területen való bevezetését, megjelenését és biztonságtechnikai vetületét kutatom.

KISS Gábor

kiss.gabor@bgk.uni-obuda.hu

Dr. habil. Gábor KISS is associated professor and the Head of the Security Science and Cyber Defense Institute of Óbuda University. He received the PhD degree in Mathematics and Computer Science from Debrecen University in 2013 and the Habilitation in Safety and Security Science from Óbuda University in 2020. Dr. KISS was guest scientist in the Faculty of Computer Science Freie Universität Berlin in 2003 and Universität Paderborn in 2006. Dr. KISS has published more than 200 refereed papers in Journals and Proceedings. He serves as an Editorial board member more Journals. He has been a Keynote speaker, Panelist speaker, Publicity chair, Program Committee or Organizing Committee member for more than 200 International Conferences. Dr. KISS is a member of the Hungarian Academy of Sciences, and more Hungarian and International Societies in Computer Science. Dr. KISS is an external expert of Bureau of Education, Hungary, National Research, Development and Inno-

Dr. habil. KISS Gábor egyetemi docens Óbudai Egyetem Biztonságtudományi és Kibervédelmi Intézetének vezetője. A Debreceni Egyetemen 2013-ban szerzett PhD fokozatot Matematika és Számítástudományból, 2020-ban pedig az Óbudai Egyetemen habilitált Katonai Műszaki Tudományból. 2003-ban a Freie Universität Berlin Informatikai Karán, 2006-ban az Universität Paderborn Informatikai Karán volt vendégkutató. Több mint 200 referált tanulmány szerzője folyóiratokban és konferencia kiadványokban, valamint több folyóirat szerkesztő bizottsági tagja. Több mint 200 nemzetközi konferencián töltött be Keynote speaker, Panelist speaker, Publicity chair, Program Committee or Organizing Committee member tisztségeket. Dr. KISS Gábor tagja a Magyar Tudományos Akadémiának, valamint több magyar és nemzetközi számítástechnikai társaságnak. Dr. KISS Gábor külső szakértője az Oktatási Hivatalnak, a Nemzeti Kutatási, Fejlesztési és Innovációs Hiva-

vation Office of Hungary. His research interests include computer science education, information security awareness, AI in self-driving vehicles and healthcare.

talnak. Kutatási területe az informatika oktatás, információbiztonság-tudatosság, mesterséges intelligencia alkalmazása az önvezető járművekben és az egészségügyben.

KOLLÁR Csaba

kollar.csaba@uni-obuda.hu

Csaba KOLLÁR is a communications engineer, certified communications specialist, electronic information security manager, doctor of economics (PhD), habilitated doctor (Dr. habil.) of military engineering, cybernetic, consultant, coach, mediator. His research interests include the social aspects and economic impacts of the digital age, with a focus on the human aspects of information security, information security awareness, human-robot interaction, smart city, artificial intelligence, social credit systems, domotics. He is a senior research fellow at the Óbuda University, head of the training courses for the specialized courses of Domotics engineer and Domotics consultant, head of the Artificial Intelligence Workshop, scientific secretary of the Editorial Board of the Safety and Security Sciences Review, which is classified by the Military Science Committee of the 9th Department of Economics and Law of the Hungarian Academy of Sciences. Chairman of the professional qualification exams. Senior consultant and coach of PREMA Consulting, expert of the Hungarian Society of Military Science and the National Association of Human Professionals. Member of the Artificial Intelligence Consortium since Q4 2018.

KOLLÁR Csaba kommunikációtechnikai mérnök, okleveles kommunikációs szakember, elektronikus információbiztonsági vezető, a közgazdaságtudományok doktora (PhD), a katonai műszaki tudományok habilitált doktora (Dr. habil.), kibernetikus, tanácsadó, coach, mediátor. Kutatási területe a digitális kor társadalmi vetületei és gazdasági hatásai, kiemelten az információbiztonság humán aspektusa, az információbiztonság-tudatosság fejlesztése, az ember-robot interakció, az okosváros, a mesterséges intelligencia, a társadalmi kredit rendszere, az intelligens épületek (domotika rendszerek) üzemeltetése és gazdálkodása. Az Óbudai Egyetem tudományos főmunkatársa, a domotika szakmérnök és a domotika szaktanácsadó továbbképzési szakok képzésvezetője, a Mesterséges Intelligencia Műhely vezetője, az MTA IX. Osztály Hadtudományi Bizottsága által minősített Biztonságtudományi Szemle szerkesztőbizottságának tudományos titkára, az Egyetem Biztonságtudományi Doktori Iskolájának és a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolájának az oktatója, témavezetője. Elnök a szakmai képesítő vizsgákon. A PREMA Consulting vezető tanácsadója és coacha, a Magyar Hadtudományi Társaság és a Humán Szakemberek Országos Szövetsége szakértője. 2018. negyedik negyedévétől a Mesterséges Intelligencia Konzorcium tagja.

MANDIĆ Dorottya

mandic.dorottya@uni-obuda.hu

My name is Dorottya MANDIĆ. I graduated from the Technical College of Applied Sciences in Bachelor of Management Engineering in Subotica, Serbia. I received my master's degree in Mechatronical Engineering from the Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering. I am currently a doctoral student in Safety and Security Sciences at the Óbuda University Doctoral School. My research area is the analysis of the security of smart devices.

MANDIĆ Dorottyának hívnak és a Műszaki Szakfőiskolán fejeztem be a tanulmányaimat Szabadkán, Szerbiában, mint mérnök menedzser. A mesterképzést az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnika Mérnöki Karán szereztem meg, mint okleveles mechatronikai mérnök. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusz hallgatója vagyok. A kutatási témám az okoseszközök biztonságának az elemzésével foglalkozik.

MORVAY László

morvay.laszlo@phd.uni-obuda.hu

László MORVAY (1967) electrical operating engineer in the medical technology sector (KKVMF, 1989) and MSc in safety engineering (ÓE-BGK, 2023). He is currently the managing director of HOLL & MOOR Health Service and Consulting Ltd. He specializes in soft laser therapy, as well as compiling professional material for research and development projects supported from EU and domestic funds, and monitoring and documenting the professional progress of projects. Contract tender assessor and mentor of the National Research, Development and Innovation Office. Continuous learning is the key to professional development, so he is currently a doctoral student at Óbuda University's Doctoral School on Safety and Security Sciences. His field of research is the investigation of medical devices used in musculoskeletal disorders, which covers the safety issues of soft laser therapy (light), ultrasound therapy (mechanical) and electrotherapy (electric current).

MORVAY László (1967) villamos-üzemmérnök orvostechnikai ágazaton (KKVMF, 1989), biztonságtechnikai mérnök-tervező MSc (ÓE-BGK, 2023). Jelenleg a HOLL & MOOR Egészségügyi Szolgáltató és Tanácsadó Kft ügyvezetője. Szakterülete a lágylézer terápia, valamint uniós és hazai forrásból támogatott kutatás-fejlesztési projektek szakmai anyagának összeállítása, a projektek szakmai előrehaladásának ellenőrzése, dokumentálása. A Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal szerződéses pályázati bírálója és mentora. A szakmai fejlődés kulcsa a folyamatos tanulás, ezért jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusza. Kutatási területe a mozgásszervi megbetegedések során alkalmazott orvostechnikai eszközök vizsgálata, amely a lágylézer terápia (fény), az ultrahang terápia (mechanikai) és az elektroterápia (elektromos áram) biztonsági kérdéseire terjed ki.

NAGY Csaba Norbert

nagy.csaba@inf.unideb.hu

Csaba Norbert NAGY, a graduate student of Computer Science Engineering at the Faculty of Informatics of the University of Debrecen. Besides his student research, he hold a technical position at the Department of Data Science and Visualization. His interests include blockchain technology, cryptographic solutions, information and cyber security. He is a member of the Data Security Section of the György Hajós Data Science Colloquium and the Talent Management Program of the University of Debrecen. He participated in the Scientific Student Conference of the Faculty of Informatics of the University of Debrecen with his thesis "Blockchain based security framework for IoT devices", where he won the EPAM special prize and advanced to the National Scientific Student Conference. He submitted his thesis to the "Information Security Thesis of the Year - 2023" announced by the Hétpecsét Information Security Association, where he won the "Other" category and the "Margaret" special prize of Noreg Information Protection Ltd, beyond that New National Excellence Program of the Ministry of Human Capacities scholarship.

NAGY Csaba Norbert a Debreceni Egyetem Informatikai Karának végzős alapszakos mérnökinformatikus hallgatója. Hallgatói pályája mellett technikus pozíciót lát el az Adattudomány és Vizualizációs Tanszéken. Érdeklődési köre a blokklánc-technológia, a kriptográfiai megoldások, az információ és kiberbiztonság. Tagja a Hajós György Adattudományi Szakkollégium Adatbiztonsági tagozatának és a Debreceni Egyetem Tehetséggondozási Programjának. Debreceni Egyetem Informatikai Karának Tudományos Diákköri Konferenciáján a vett részt „Blokklánc alapú biztosági keretrendszer IoT eszközökre” című szakdolgozattal, ahol EPAM különdíjat nyert és továbbjutott Országos Tudományos Diákköri Konferenciára. Szakdolgozatával pályázatot nyújtott be a Hétpecsét Információbiztonsági Egyesülete által meghirdetett „Az év információbiztonsági dolgozata – 2023” címre, ahol az „egyéb” kategória címet nyerte el, valamint a Noreg Információvédelmi Kft. „Margaréta” különdíj, ezentúl az Újnemzeti Kiválóság Program ösztöndíjának elismerésében részesült.

NAGY Rudolf

nagy.rudolf@uni-obuda.hu

Dr. habil. Rudolf NAGY, retaired firefighter Colonel, is currently senior lecturer at Óbuda University. He studied in foreign educational institutions. He served as a CBRN defence officer, and took part in industrial safety tasks. He gained experience as an operations officer in the NATO SFOR mission. After that he became Deputy Head of the Emergency Management Department of Hungarian National Directorate General for Disaster Management. Summa cum laude earned a PhD degree in field of Critical Infrastructure Protection. Later he was appointed Deputy Head of the Disaster Management Training Centre. In civilian life, he worked as an EHS manager. He has been teaching subjects of safety and security sciences since 2015, and is responsible for the fire protection engineering specialization. He obtained a habilitated doctorate in the scientific study of self-ignition.

Dr. habil. NAGY Rudolf nyugalmazott tűzoltó ezredes, jelenleg az Óbudai Egyetem adjunktusa. Külföldi oktatási intézményekben tanult. Vegyivédelmi tisztként szolgált, és részt vett iparbiztonsági feladatokban. A NATO SFOR misszióban műveleti tisztként szerzett tapasztalatokat. Ezt követően az Országosl Katasztrófavédelmi Főigazgatóság Veszélyhelyzetkezelési Főosztályának helyettes vezetője lett. Summa cum laude minősítéssel szerzett PhD fokozatot a kritikus infrastruktúrák védelme területén. Később a Katasztrófavédelmi Oktatási Központ vezetőjének helyettesévé nevezték ki. A polgári életben EHS vezetőként dolgozott. 2015 óta oktatja a biztonságtudományok tantárgyakat, a tűzvédelmi mérnöki specializáció felelőse. Habilitált doktori címet szerzett az öngyulladások tudományos vizsgálatából.

NÉGYESI Imre

negyesi.imre@uni-nke.hu

Dr habil. Colonel Imre NÉGYESI, Head of the Department of Informatics, Faculty of Military Science and Military Officer Training, National University of Public Service. His research interests include the legal issues, social impact, human and ethical aspects of the application of Artificial Intelligence, and the possibilities of military applications of VR technology. In 1986 he graduated from the Zalka Máté Military Technical College as a radiochemistry engineer. From 1986 to 1998 he served in various chemical defence units. In 1998, he joined the staff of the Department of Informatics of the Zrínyi Miklós National Defence University as a teaching assistant. He obtained his PhD degree in 2006 (Military Science) and habilitated in 2011 (Military Engineering). He is currently Associate Professor at the Department of Informatics of the Faculty of Military Science and Military Training of the National University of Public Service.

Dr. habil. NÉGYESI Imre honvéd ezredes, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Informatikai Tanszék tanszékvezetője. Kutatási területe a Mesterséges Intelligencia alkalmazásának jogi kérdései, társadalmi hatásai, humán és etikai vonatkozásai, valamint a VR-technológia katonai alkalmazásának lehetőségei. 1986-ban végzett a Zalka Máté Katonai Műszaki Főiskolán radiokémia mérnökként. 1986-tól 1998-ig különböző alakulatoknál szolgált vegyivédelmi beosztásokban. 1998-ban került a Zrínyi Miklós Nemzetvédelmi Egyetem Informatikai tanszék állományába tanársegédként. PhD fokozatát 2006-ban szerezte (Hadtudomány), majd 2011-ben habilitált (Katonai műszaki tudományok). Jelenleg a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Informatikai tanszékének tanszékvezető egyetemi docense.

OLÁH Norbert

olah.norbert@inf.unideb.hu

Norbert OLÁH is an Assistant Professor at the Faculty of Informatics, University of Debrecen. He holds a PhD in Theoretical computer science, data security and cryptography in secure authentication scheme design in distributed systems. His interests include security issues in cloud computing and IoT ecosystems, including the implementation of user authentication. The topic is one of the most dynamically developing

OLÁH Norbert a Debreceni Egyetem Informatikai Karának adjunktusa. Az elméleti számítástudomány, adatvédelem és kriptográfia programban szerzett doktori fokozatot a biztonságos autentikációs sémák tervezése elosztott rendszerekben témakörében. Érdeklődési köre a felhő alapú számítások és az IoT ökoszisztémák biztonsági kérdései, azon belül is a felhasználó hitelesítés megvalósítási lehetőségei. A

areas in IT today and raises several problems to be solved. He has been involved in several scientific projects focused on the secure design and study of various communication systems, including TKP 2019: Thematic Program of Excellence 2019, where his tasks included the design and analysis of V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure) secure communication protocols. He also participated in the SETIT - IoT Systems Enhancement Technologies project, where he researched lightweight cryptographic primitives and contributed to the study "Lightweight Cryptographic Algorithms and Security Features". During my PhD studies, he has been awarded the Universitas Foundation PhD Student Scientific Award and the New National Excellence Program of the Ministry of Human Capacities scholarship.

témakör napjainkban az informatika egyik legdinamikusabban fejlődő területe, számos megoldandó problémát vet fel. Több tudományos projektben is részt vett, amely a különböző kommunikációs rendszerek biztonságos kialakítására és tervezésére fókuszált, többek között a TKP 2019: Thematic Program of Excellence 2019 programban, ahol feladatai közé tartozott a V2V (Vehicle to Vehicle) és V2I (Vehicle to Infrastructure) biztonságos kommunikációs protokoll tervezése és elemzése. Emellett részt vett a SETIT - IoT Systems Enhancement Technologies projektben, ahol könnyűsúlyú kriptográfiai primitíveket tanulmányozott, és részt vett a "Lightweight Cryptographic Algorithms and Security Features" tanulmány kidolgozásában. A PhD tanulmányai során többször elismerésben részesült, melynek során megkapta az Universitas Alapítvány Hallgatói tudományos eredmény elismerését, illetve az Új Nemzeti Kiválósági Program ösztöndíját.

OPOR Csaba Barnabás

csabaopor@gmail.com

Csaba Barnabás OPOR, born in Budapest, currently resides with his family in Üröm, Pest County. In 2015, he graduated from the Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering, specializing in Military and Safety Engineering. He has nearly ten years of experience working in various areas of law enforcement, including as an occupational safety supervisor, allowing him to become acquainted with the specialized field of occupational safety in law enforcement. Later, he worked for two years as the head of the occupational safety department at the National Tax and Customs Administration, where he had to map out the legal background. In 2024, he also graduated as an Occupational Safety Engineer from Óbuda University. In addition to his expertise in occupational safety, he also holds qualifications in fire safety and armament. In his spare time, he volunteers as a firefighter. Currently, he serves as the occupational health and safety manager at ANY Security Printing Company.

OPOR Csaba Barnabás, született Budapesten, jelenleg a Pest vármegyei Ürömön él családjával. 2015-ben végzett az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki kar Had- és Biztonságtechnikai mérnök szakon. Közel tíz évet dolgozott a rendvédelem különböző területein, többek között munkavédelmi felügyelőként is, így a munkavédelem a rendvédelmekre vonatkozó speciális területével is megismerkedhetett. Később kettő évig dolgozott a Nemzeti Adó- és Vámhivatal munkavédelmi osztályvezetőjeként, ahol muszáj volt feltérképeznie a jogszabályi hátteret. 2024-ben Munkavédelmi szakmérnökként szintén az Óbudai Egyetemen végzett. A munkavédelem mellett tűzvédelmi, illetve fegyverzeti végzettségei vannak. Szabadidejében önkéntes tűzoltóként tevékenykedik. Jelenleg az ANY Biztonsági Nyomda munka- és tűzvédelmi vezetője.

PÁL Anita

pal.anita@phd.uni-obuda.hu

Over the past 15 years, I have served as an interpreter and IT developer for law firms, economic entities, and commercial organizations, acquiring deep understanding of corporate dynamics within both English and German-speaking environments. For the last four years, I have been serving my country as a soldier at

Az elmúlt 15 évben ügyvédi irodák, gazdasági cégek és kereskedelmi vállalatok angol és német nyelvű képviseletében tolmácsként és technikai-informatikai fejlesztőként dolgoztam, mélyreható betekintést nyerve a cégvezetés dinamikájába. A legutóbbi 4 évben katonaként szolgálom hazámat a HM Védelem-

the MoD Defence Economic Bureau's International Directorate. I earned my bachelor's degree in International Relations, then completed a master's degree in International Security and Defense Policy at the National University of Public Service. During my studies, I deepened my knowledge in optimizing defense organizations and administrative processes. My thesis explored the art of deterrence, examining the role of the defense industry in the arms race. Currently, I am continuing my studies at the Óbuda University Doctoral School of Safety Sciences, where my research focuses on the impact of artificial intelligence on both military and civilian security, emphasizing the importance of AI development and the reduction of associated security risks.

gazdasági Hivatal Nemzetközi Igazgatóságán. Nemzetközi Kapcsolatokból szereztem alapdiplomámat, majd a Nemzeti Közszolgálati Egyetem Hadtudományi Karán végeztem el mesterképzést Nemzetközi Biztonság- és Védelempolitikai szakon. Itt tudásomat a védelmi szervezetek és a védelmi közigazgatás optimalizálására mélyítettem el. Diplomamunkámat az elrettentés művészetéről írtam, vizsgálva a hadiipar szerepét. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában folytatom tanulmányaimat, ahol kutatásom középpontjában a mesterséges intelligencia katonai és polgári biztonságra gyakorolt hatása áll, kiemelve az MI fejlesztésének és a biztonsági kockázatok csökkentésének fontosságát.

SZABÓ Lajos

szabo.lajos@uni-obuda.hu

Dr. Lajos SZABÓ PhD. of security and safety sciences, certified security engineer, security management engineer, retired police Lieutenant Colonel, Chairman of the Board of Trustees of the Law Enforcement and Private Security Education and Research Foundation (REMOK), lecturer at the Faculty of Law Enforcement of the National University of Public Service and the Bánki Donát Faculty of Mechanical and Security Engineering of Óbuda University. During the first half of his three decades in the police service he was a senior investigator and during the second half he was the chief police and team services officer. During this time, I planned and implemented the securing of routes and destinations for various sporting, cultural and religious events, transport and delegations. I was responsible for planning the secure guarding of various facilities.I was one of the first to obtain the Diploma in Security Engineering, I was an expert in the accreditation of the MSC Chartered Security Engineers course and subsequently graduated from the MSC. Since retirement I have been teaching, researching and publishing.

Dr. SZABÓ Lajos PhD., a biztonságtudományok doktora, okleveles biztonságtechnikai mérnök, biztonságszervező mérnök, nyugállományú rendőr alezredes, kuratóriumi elnöke a Rendészeti és Magánbiztonsági Oktatási és Kutatási Alapítványnak (REMOK), a Nemzeti Közszolgálati Egyetem Rendészeti Karán és az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán óraadó tanár. A rendőri szolgálatban töltött három évtized első felében kiemelt főnyomozó, a második felében kiemelt főelőadó közrendvédelmi és csapatszolgálati területen. Ez idő alatt terveztem és végrehajtottam különféle sport, kulturális és egyházi rendezvények helyszínének biztosítását, szállítmányok és delegációk útvonalainak és célállomásainak biztosítását. Felelős voltam különféle létesítmények biztonságos őrzésének megtervezéséért. Az elsők között szereztem meg a biztonságszervező szakmérnöki diplomát, bolognai szakértőként vettem részt az okleveles biztonságtechnikai mérnök MSC képzés akkreditálásában, majd ott is diplomát szereztem. Tanítok, kutatok és publikálok nyugdíjba vonulásom óta.

SZŰCS Attila

szucs.attila@uni-nke.hu

Attila SZŰCS, Lieutenant Colonel of the National University of Public Service, Assistant Professor of the Department of Military Studies and Military Officer Training. He is currently a doctoral student at the Security Sciences Doctoral School of the University of Óbuda. His research interests include legal issues, social impact, human and ethical aspects of the application of Artificial Intelligence. He graduated from the

SZŰCS Attila honvéd alezredes, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Híradó Tanszék tanársegédje. Öt gyermek édesapja Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusz hallgatója. Kutatási területe a Mesterséges Intelligencia alkalmazásának jogi kérdései, társadalmi hatásai, humán és etikai vonatkozásai. 1997-ben végzett a Bolyai János Katonai

Bolyai János Military College in 1997 as a locator engineer. He served 3 years in an air defence missile battery as a reconnaissance locator station commander. In the meantime, he graduated from the Kandó Kálmán Technical College with a degree in Engineering teacher. In 2002, he was transferred to Szentendre to study at the Central Non-commissioned officer Training School, where he served for 18 years, and was promoted from instructor to head of the Technical and Military Informatics Training Division. During this time, he obtained a Master's degree in Engineering teacher from the University of Óbuda and a teaching qualification in Faith and Morals from the Esztergom College of Faith and Morals.

Főiskolán lokátorüzemmérnökként. 3 évet szolgált egy légvédelmi rakétaütegnél mint felderítő lokátor állomás parancsnok. Közben a Kandó Kálmán Műszaki Főiskolán Mérnöktanári oklevelet szerzett. 2002-ben került Szentendrére a Központi Tiszthelyettes Szakképző Iskola állományába, ahol 18 éven át szolgálta a tiszthelyettes majd altisztképzést és lett oktatótisztből a Műszaki és Katonaiinformatikai Oktatási Alosztály vezetője. Ezalatt az Óbudai Egyetemen Mérnöktanári mesterdiplomát, valamint az Esztergomi Hittudományi Főiskolán Hit és Erkölcstan oktatói képesítést szerzett.

SZŰCS Endre

szucs.endre@bgk.uni-obuda.hu

Endre SZŰCS (1963) PhD degree in military science, certified security engineer, mechanical engineer, engineering teacher. Currently, he is a doctoral supervisor and advisor at Óbuda University's Doctoral School on Safety and Security Sciences, Instructor of the course "Review and analysis of the history and events of security technology", and he is also a lecturer at the Institute of Mechanical Engineering and Technology and Institute of Safety Science and Cybersecurity at Óbuda University, Bánki Donát Faculty of Mechanical and Security Engineering. His research interests are "The possibilities of the use of renewable energy sources in safety and security technology", "Investigation of the history of safety and security technology".

SZŰCS Endre (1963) a hadtudomány PhD fokozatosa, okleveles biztonságtechnikai mérnök, gépészmérnök, mérnök tanár. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában témavezető és témakiíró, „A biztonságtechnika történetének, eseményeinek áttekintése, elemzése” című tantárgyat oktató, illetve az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Gépészeti és Biztonságtudományi és Kibervédelmi Intézet óradója. Kutatási területe A megújuló energiaforrások alkalmazásának lehetőségei a biztonságtechnikában. A biztonságtechnika történetének vizsgálata.

VÖLGYESI Péter

volgyesi.peter@ek.hun-ren.hu

Péter VÖLGYESI (MSc and PhD in Environmental Science, Loránd Eötvös University, Budapest), joined the Nuclear Security Department at the HUN-REN Centre for Energy Research, Hungary in 2014, as a young researcher. He was nominated as the head of the detector testing laboratory in 2016. Since 2018 he has been the head of the Nuclear Security Department. In the end of 2020, he became the head of the nuclear forensics laboratory as well. The activities of the Nuclear Security Department cover research and practical application in the field of nuclear security and nuclear safeguards, as well as scientific support for domestic and international organizations and companies. One of the main activities of the department is to participate in combating illicit trafficking of nuclear materials and nuclear terrorism (misuse of radioactive

VÖLGYESI Péter az Eötvös Loránd Tudományegyetemen szerzett környezettudományi MSc és PhD diplomát. 2014-ben fiatal kutatóként csatlakozott a HUN-REN Energiatudományi Kutatóközpont Sugárbiztonsági laboratóriumához (EK SBL), ahol 2016-ban a Detektortesztelő laboratórium vezetőjének nevezeték ki. 2018 óta a Sugárbiztonsági Laboratórium, majd 2020 végétől a Nukleáris törvényszéki analitikai laboratórium vezetője. A Sugárbiztonsági Laboratórium tevékenysége a nukleáris védettség (nuclear security) és a nukleáris biztosítéki rendszer (safeguards) területén végzett kutatásokra és ezek gyakorlati alkalmazására, illetve hazai és nemzetközi szervezetek és cégek szakmai támogatására terjed ki. Az SBL egyik fő tevékenysége a nukleáris anyagok illegális forgalmazása (illicit traf-

materials). The professional on-site analysis and laboratory measurement of unknown nuclear or other radioactive materials found or seized (ie. nuclear forensic examination), is delegated to the HUN-REN Centre for Energy Research by a Governmental Decree (490/2015 (XII.30). The NSD maintains a mobile expert support team and a preparedness service to carry out the activities described by this Decree and, if necessary, to perform on-site investigations and to transport radioactive materials with unknown origin to the KFKI site. As a result of this, in 2016, HUN-REN Centre for Energy Research was nominated to the Collaborating Centre of the International Atomic Energy Agency for Nuclear Forensics.

ficking), illetve a nukleáris terrorizmus (sugárzó anyagokkal való visszaélés, pánikkeltés) elleni küzdelemben való részvétel. A talált, vagy lefoglalt nukleáris és egyéb radioaktív anyagok helyszíni elemzését és laboratóriumi szakértői vizsgálatát, azaz nukleáris törvényszéki elemzését a 490/2015 (XII.30.) Kormányrendelet delegálja a HUN-REN Energiatudományi Kutatóközponthoz. Az SBL állandó készenlétet tart fenn a 490/2015-ös rendelet tevékenységének ellátásához és szükség esetén helyszíni vizsgálatokhoz, továbbá az ismeretlen anyagoknak a HUN-REN EK telephelyére történő beszállításához. A nukleáris törvényszéki területen az intézet 2016 óta a Nemzetközi Atomenergia Ügynökség kinevezett együttműködő központja.

ZAGYVAI Péter

zagyvai.peter@ek.hun-ren.hu

I am Péter ZAGYVAI. I graduated as a chemical engineer at the Budapest University of Technology (BME) in 1976. I dealt with radioanalysis even during my diploma thesis period, and I remained in this area. Between 1990 and 2010 I was the head of the radiation protection department of the training reactor of the Institute of Nuclear Techniques at BME. From 2010 my major workplace has been the HUN-REN Centre for Energy Research. I am senior research associate of the Environmental Physics Laboratory. I retired in 2021, but still, I hold the position of the radiation protection officer of the campus. As a part-time job I have lectures at BME with BSc and MSc subjects for the faculties of Natural Sciences, Mechanical and Energetic Engineering and Chemical and Bioengineering. In addition, I support the work of the ELI ALPS laser centre at Szeged, and occasionally I am invited as a lecturer or consultant of working units of the International Atomic Energy Agency (IAEA) in relation to emergency management and response and decommissioning of facilities.

ZAGYVAI Péter vagyok, okleveles vegyészmérnökként végeztem 1976-ban a Budapesti Műszaki Egyetemen (BME). Már a diplomázás alatt is radioanalitikával foglalkoztam, és utána is ezen a tudományterületen maradtam. 1990-től 2010-ig a BME Nukleáris Technikai Intézetéhez tartozó oktatóreaktor sugárvédelmi vezetője voltam, 2010-től fő munkahelyem a jelenlegi HUN-REN Energiatudományi Kutatóközpont lett. A Környezetfizikai Laboratórium tudományos főmunkatársaként dolgozom, 2021 óta nyugdíjasként, emellett ellátom a telephelyi sugárvédelmi megbízott feladatait. Másodállásban megmaradtam a BME-n, a Természettudományi Kar, a Gépészmérnöki és Energetikai Kar, valamint a Vegyész- és Biomérnöki Kar BSc és MSc képzésein tartok előadásokat. Ezek mellett sugárvédelmi szakértőként segítem a szegedi ELI ALPS lézerközpont munkáját, és alkalmanként tanfolyami előadóként és konzulensként részt veszek az International Atomic Energy Agency (IAEA) baleset-elhárítással és létesítmények leszerelésével foglalkozó munkacsoportjaiban.

ZS. SZABÓ Kitti

Kitti.szabo@smartopert.com

ZS. SZABÓ Kitti graduated from the Budapest University of Technology and Economics as a certified biomolecular engineer in 2012. In addition to her diploma, she completed the Quality Management program at the BME Faculty of Chemical Engineering and Biotechnology. Since 2013, she has been involved in quality management, and since 2017, in process improvement and efficiency enhancement. While her expertise lies in quality management, she also has experience in preparing a diagnostics company for

ZS. SZABÓ Kitti 2012-ben végzett a Budapesti Műszaki és Gazdaságtudományi Egyetemen okleveles biomérnökként. Diplomáját kiegészítve elvégezte a BME Vegyészmérnöki és Biomérnöki Kar minőségügy programját. 2013 óta foglalkozik minőségirányítással, 2017 óta folyamat fejlesztéssel és hatékonyság növeléssel. Bár minőségirányítás tekintetében az ISO 9001 szabvány a szakterülete, van tapasztalata orvosdiagnosztikai cég ISO13485 szabványra való felkészítésében és egészségügyi vállalat ISO27001

ISO 13485 compliance and establishing ISO 27001 compliance for healthcare enterprises. In 2019, she co-founded Smartopert Kft. with Péter ZSÁK and launched the Okosotthon Guru® ("Smart home guru") brand with the aim of building internationally recognized smart home installation training that promotes the widespread adoption of high-quality smart homes. Her research topic is smart home for assisted livings – the harmonization of home medical diagnostic tools and information security for user protection.

megfelelőségének kialakításában is. ZSÁK Péterrel 2019-ben alapították meg a Smartopert Kft.-t majd az Okosotthon guru® brandet azzal a céllal, hogy egy olyan nemzetközileg elismert okosotthon telepítő képzést építsenek fel, amely elősegíti a magas színvonalú okosotthonok elterjedését. Kutatási témája a gondoskodó okosotthonok – az otthoni orvosi diagnosztikai eszközök és az informatikai biztonság összehangolása a felhasználók védelméért.

ZSÁK Péter

Peter.zsak@smartopert.com

Peter ZSÁK graduated in 2005 from the Faculty of Science and Informatics at the University of Szeged as a chemist. In 2011, he completed his studies in economics at the Faculty of Economics and Business Administration at the University of Szeged. From 2012 to 2019, he was involved in chemical and physical occupational safety, gaining experience in chemical safety and fire protection. Since 2019, he has been educating professionals in the field about the operation and installation peculiarities of smart homes and building automation systems under the name Okosotthon guru®, brand of Smaropert Kft. His expertise lies in the application of wireless IoT protocols. He is the chair of the Z-Wave Alliance EMEA TaskForce and the founding president of the Hungarian Smart Home and Buildingautomation Association. His research focuses on the safety of smart homes, within which he investigates IT security challenges and solutions related to the Z-wave protocol.

ZSÁK Péter 2005-ben végzett a Szegedi Tudományegyetem Természettudományi és Informatikai Karán vegyészként. 2011-ben a Szegedi Tudományegyetem Gazdaságtudományi Karán elvégezte a közgazdász szakot. 2012-től 2019-ig kémiai és fizikai munkavédelemmel fogalkozott, tapasztalatot szerzett a kémiai biztonság és tűzbiztonság területén. 2019-től okosotthonok és épületautomatizálási rendszerek működésével és telepítési sajátosságaival ismerteti meg a szakmában dolgozókat a Smartopert Kft. Okosotthon guru® márkaneve alatt. Szakterülete a vezeték nélküli IoT protokollok alkalmazása. A Z-Wave Alliance EMEA TaskForce vezetője, a Magyar Okosotthon és Épületautomatizálási Szövetség alapító elnöke. Kutatási témája az okosotthonok biztonsága, mely területen belül az IT-biztonsági kihívásokat és megoldásokat kutatja a Z-wave protokoll tekintetében.

Creator of the cover image | **A borítón látható kép alkotója**

BORS Györgyi

borsgyorgyi77@gmail.com

She was born in 1977 in Tapolca, Hungary. The tragic early death of his mother was decisive in her life because she was then raised in state care until she was 18 years old. During her years there, she realized that she found the greatest pleasure in art. She studied graphic art for several years at the Railway School of Music and Fine Arts in Budapest with the painter and sculptor György BENEDEK, and later with Árpád "Pika" NAGY and Zoltán SEBESTYÉN. In 2007 she graduated from the King Zsigmond College with a degree in Cultural Management. From 2017, her master is Kálmán GASZTONYI, from whom she learned the different techniques of oil painting. She is narrative

Magyarországon, Tapolcán született 1977-ben. Édesanyja tragikus korai halála meghatározó volt az életében, mert ezt követően 18 éves koráig állami gondozásban nevelkedett. Az ott töltött évek alatt jött rá, hogy a művészetben leli a legnagyobb örömet. Grafikai tanulmányokat folytatott több évig Budapesten a Vasutas Zene- és Képzőművészeti Iskolában BENEDEK György festő és szobrászművésznél, majd később NAGY Árpád „Pika"-nál és SEBESTYÉN Zoltánnál is tanult. 2007-ben diplomázott a Zsigmond Király Főiskola Művelődésszervező szakán. 2017-től Mestere GASZTONYI Kálmán, akitől elsajátította az olajfestés különböző technikáit. Narratív

painter. It is important for her to be creative about something, a feeling, an idea, an impression, or even a human quality. She creates using the tools of abstract painting. With her innovative style, she brings experiences, feelings and thoughts with the tools of painting to a universal level that we have all known or experienced in some form. Her work has been successfully featured in various domestic and international competitions and exhibitions (Budapest, London, New Jersey, Hong Kong) and has appeared in several contemporary art albums and art magazines. One of her works can also be found in the public collection of the Hungarian Museum of Circus Art. Her expression is geometric and lyrical abstract, which are side by side yet reinforce her art organically intertwined.

festő. Fontos számára, hogy alkotási szóljanak valamiről, egy érzésről, egy gondolatról, egy benyomásról, vagy akár egy emberi tulajdonságról. Az absztrakt festészet eszközeit felhasználva alkot. Innovatív stílusával olyan tapasztalatokat, érzéseket és gondolatokat emel a festészet eszközeivel egyetemes szintre, melyeket mindnyájan ismerünk vagy megéltünk már valamilyen formában. Munkái sikeresen szerepeltek különféle hazai és nemzetközi versenyeken és kiállításokon. (Budapest, London, New Jersey, Hong Kong) Több kortárs művészeti albumban, art magazinban jelentek meg munkái. Egyik alkotása a Magyar Cirkuszművészeti Múzeum közgyűjteményében is megtalálható. Kifejezésmódja a geometriai- és lírai absztrakt, melyek egymás mellett, de mégis szervesen összefonódva erősítik művészetét.

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

Vol 6, No 2, 2024. | **2024. VI. évf. 2. szám**

CONTENT | **TARTALOM**

Philosophy and History of the Safety and Security column | Biztonságfilozófia és -történet rovat

Domotics column | Domotika rovat

Health Security column | Egészségbiztonság rovat

Information Security column | Információbiztonság rovat

Safety and Security Sciences Review	Biztonságtudományi Szemle
international peer-reviewed, professional and scientific journal of safety and security sciences	a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

PREDATORY JOURNALS AND MISLEADING METRICS – DON'T LET THEM DECEIVE YOU!

PREDÁTOR FOLYÓIRATOK ÉS FÉLREVEZETŐ MÉRŐSZÁMOK – NE HAGYD, HOGY BECSAPJANAK!

BEREK László[1]

Abstract

The predatory phenomenon that poses the greatest threat to the security of online scientific communication has emerged primarily due to the proliferation of open-access publishing, along with associated article processing charges, driven by the development of information technology and the internet. Predatory journals bypass professional evaluation, plagiarism checks, and quality assessments of publications, with their sole objective being to publish as many articles as possible to maximize profit. Over the past decade, a portion of predatory journals, perfecting their arsenal of deceptive tactics, has become increasingly difficult to distinguish not only for young researchers but also for experienced ones from reputable journals. Examining the scholarly literature of the last 10 years reveals that predatory journals and publishers present an increasingly serious threat to online scientific communication. What are the consequences of publishing in predatory journals, and how can predatory journals be identified?

Keywords

predatory publishers, predatory journals, scientometrics, career of researc-hers, university rankings, science ethics, bogus metrics

Absztrakt

Az online tudományos kommunikáció biztonságát leginkább veszélyeztető predátor jelenség az open access publikálás - valamint a kapcsolódó cikkeljárási díjak - elterjedésével, illetve az informatika és az internet fejlődésének hatására jelent meg. A predátor folyóiratok mellőzik a szakmai bírálatot, a plágiumellenőrzést és a publikációk minőségi vizsgálatát, az egyetlen céljuk, hogy minél több cikket jelentessenek meg, így minél nagyobb profitra tegyenek szert. Az elmúlt egy évtized során a predátor folyóiratok egy része - tökéletesítve a megtévesztés eszköztárát - nem csak a fiatal, de a tapasztalt kutatók számára is nehezen különböztethető meg a hiteles folyóiratoktól. Az elmúlt 10 év szakirodalmát vizsgálva megállapítható, hogy a predátor folyóiratok és kiadók egyre komolyabb veszélyt jelentenek az online tudományos kommunikációra. Milyen következményei lehetnek a predátor folyóiratban történő publikálásnak és milyen módon ismerhetők fel a predátor folyóiratok?

Kulcsszavak

predátor kiadók, predátor folyóiratok, tudománymetria, kutatói életpálya, egyetemi világranglista, tudományetika, hamis metrika

[1] berek.laszlo@uni-obuda.hu | ORCID: 0000-0002-4126-1528 | könyvtárigazgató, Óbudai Egyetem | Library director Óbuda University

BEVEZETÉS

A tudományos kommunikáció az évszázadok során nagyon sokat változott és természetesen – mint az élet bármelyik területén – a változás üteme folyamatosan gyorsult. Ha csak az utolsó bő két évtizedet vesszük alapul, a tudományos kommunikáció olyan egyértelműen jutott az online térbe, hogy mára túlnyomó részt itt van jelen. Ez a folyamat érthető is, mivel a tudományos kommunikáció elsődleges „szükségleteit", ezek a felületek, ez a publikálási forma elégíti ki leginkább. Ebből a szempontból is a legfontosabb kulcsszó a gyorsaság.

A tudományos kutatómunka is felgyorsult, a publikálás folyamatában a kézirat benyújtásáig tartó út így jelentősen lerövidült. A különböző tudományos, szakirodalmi adatbázisok, akár automatikus témafigyeléssel szolgálják ki a kutatókat, kutatóhelyeket. A szakirodalom szűrése, feldolgozása, kategorizálása, sőt a kéziratba történő hivatkozás szintű felhasználása is megoldható a reference manager – hivatkozáskezelő – szoftverek segítségével. Túlzás nélkül állíthatjuk, hogy a publikálás ezen munkafolyamataira felhasznált idő az elmúlt 10 évben sokszorosan csökkent.

PUBLIKÁCIÓS KÉNYSZER

A publikációs kényszer (Publish or Perish) a tudományos kommunikáció minden résztvevőjénél megtalálható tényező. A doktorandusz hallgató a kutatási beszámoló alkalmával a megjelent publikációk után kapja a kreditpontokat, a kutatói és egyetemi oktatói előmenetel minden egyes lépcsőfokán megtalálhatók a publikációs és hivatkozási elvárások. Az intézmény szintjén (akár kutatóhely, akár felsőoktatási intézmény) ugyanúgy jelen vannak a publikációs, mennyiségi – és persze minőségi – elvárások a különböző teljesítményértékelő indikátoroknak vagy az egyes nemzetközi rangsorok elvárásainak megfelelően. Ezek az intézményi publikációs célok természetesen tovább rakódnak az ott dolgozó kutatók, oktatók vállára. Ha konkrét ösztöndíjak, támogatások szempontjából vizsgáljuk a kérdést, ugyanúgy fennáll a „kényszer-publikálás" jelensége.

Két pontos definíció a jelenségre a szakirodalomból:

„A "Publish or perish" kifejezés az akadémiai intézményeken belüli hozzáállásra vagy gyakorlatra utal, amely szerint a kutatókra publikációs nyomás nehezedik annak érdekében, hogy megtarthassák pozíciójukat, vagy hogy sikeresnek tartsák őket."[2][1]

„A Publish or perish (POP) kifejezés a kutatókra gyakorolt nyomást írja le, hogy publikáljanak gyorsan és folyamatosan, mert ez a munkahely elvárása, az előléptetés, de még a munkahely megtartásának is a feltétele."[3][2]

A "publish or perish" nyomás és az online tudományos kommunikáció felgyorsulása magával hozta a predator kiadók és folyóiratok megjelenését. A jelenség természetesen sok összetevőből áll össze, de ez a két tényező a legfontosabb. Világunk felgyorsult, bármely területet is vesszük górcső alá.

[2] *„Publish or perish" used to refer to an attitude or practice existing within academic institutions, whereby researchers are under pressure to publish material in order to retain their positions or to be deemed successful."* [1]

[3] *„Publish or perish (POP) is a phrase that describes the pressure put on academics to publish in scholarly journals rapidly and continually as a condition for employment (finding a job), promotion, and even maintaining one's job."* [2]

A tudományos kommunikáció egyik alapja, hogy a nem dokumentált és nem közölt kutatómunka azt jelenti, hogy egyszerűen meg sem történt. Tehát bármilyen kutatás közlése, publikálása alapkövetelmény. Itt természetesen nem elsősorban a láthatóságon van a hangsúly, hanem a tudományos közeg, a szűkebben vett szakma bírálata. A folyóiratok esetében ezért is fontos a minőségi és dokumentált lektorálási folyamat. A minősített folyóiratok esetében ez alap elvárás, nem csak a legmagasabb tudományos szinteken (pl. Web of Science, Scopus indexált folyóiratok esetében) de a Magyar Tudományos Művek Tárában is.

A legfontosabb kutatási eredmények minél gyorsabb publikálása mindig is fontos volt, az elmúlt években a technológia fejlődése ezt az igényt egyre inkább kiszolgálja. Lényeges kérdés vetődik fel ezen a ponton, hogy a publikálás gyorsasága meddig fokozható úgy, hogy az ne menjen az érdemi, minőségi bírálat rovására? Esetleg már túl is léptük ezt a határt? A publikált kutatási eredmények fontos indikátorok a kutatói előmenetel, kutatói támogatások, egyéb ösztöndíjak szempontjából.

A szerzők, kutatók és természetesen az egyetemek/kutatóhelyek azt szeretnék, hogy…

- a kutatási eredmények minél gyorsabban eljussanak a közönséghez;
- a kutatási eredmények minél gyorsabban megjelenjenek – kapcsolódva a kutatói/oktatói előmeneteli folyamatokhoz;
- az eredmények minél korábban hivatkozhatók legyenek;
- minél jobb minőségű, tudományos hivatkozások jelenjenek meg;
- a szerzői / intézményi hivatkozások minél egyszerűbben naplózhatók legyenek.

A nagy online tudománymetriai adatbázisok a hivatkozások, publikációk és különböző tudománymetriai mérőszámok aktuális állását prezentálják. A szerzőknek és az intézményeknek – és természetesen a különböző egyetemi és kutatói ranking szolgáltatóknak is - valamint az országok részére is gyors, könnyen elérhető és automatizálható adatforrást jelentenek a tudományos világban. A nagyobb cégek ezen adatbázisokon alapuló tudománymetriai és kutatás-elemző platformokat alakítottak ki az elmúlt években, amelyekkel lehetőség van a kutatók, intézmények régiók és országok tudományos kutatási teljesítményének vizualizálására, speciális teljesítményértékelések összeállítására, kutatási trendek beazonosítására és intézmények/kutatók összehasonlítására. (SciVal, InCites) Mindezekhez jönnek még a különböző folyóirat rangsorok és minősítő források. A legismertebbek ezek közül a Scopus adatbázis adatait használó Scimago Journal Rank, illetve a Clarivate aktuális IF értékeket is tartalmazó Journal Citation Reports adatbázisa és a Master Journal List felülete.

A predátor folyóiratok és kiadók kapcsán természetesen az open access filozófia elterjedése is fontos tényező. A gombamód szaporodó online folyóiratok sokaságából egy kezdő, de néha még a tapasztaltabb kutatók számára is kihívást jelenthet egyértelműen megállapítani egy-egy folyóirat értékét. A predátor kiadók és folyóiratok megjelenésével és folyamatos fejlődésével ez a kihívás egy újabb szintre lépett.

A PREDÁTOR FOLYÓIRATOK JELLEMZŐI

Több, korábbi publikációmban foglalkoztam a predátor folyóiratok legfontosabb jellemzőivel, felismerhetőségükkel és osztályozásukkal is. Ezekre a folyóiratokra együttesen jellemző a megtévesztés és a félretájékoztatás is. A következőkben sorra veszem azokat a gyanús jeleket, amelyek esetén jogosan merülhet fel kétség a folyóirattal kapcsolatban.

Szakmai bírálat / lektorálás hiánya

Gyanús jel, ha a folyóirat honlapján nem található információ a lektorálás folyamatára. Ebben az esetben – kifejezetten a predátor folyóiratok esetében – jogosan merülhet fel, hogy az összes beküldött kéziratot elfogadják a folyóiratban.

Indexelés

Az egyik leginkább feltűnő jel, ami alapján azonosíthatók a predátor folyóiratok. A folyóiratok honlapjukon feltüntetik azokat a tudományos adatbázisokat és regisztereket, amik indexelik a tartalmukat, a leközölt, befogadott folyóiratcikkeket. Ez az egyik fontos szempont, ami alapján a szerző kiválasztja a folyóiratot kézirata megjelentetésére. A korábban már említett publikációs kényszer és az előmenetel elvárásai ezen a ponton érvényesülnek leginkább. (*Ha például az egyetemi docensi elvárások között szerepel, hogy legyen a pályázónak legalább 5 Web of Science által indexelt publikációja, akkor egy ennek a követelménynek megfelelő folyóiratot keres a kéziratának.*)

A predátor folyóiratok sokszor olyan adatbázisokat is megjelentethetnek honlapjukon, amelyek valójában nem indexelik a tartalmukat. Ezeket érdemes ellenőrizni a konkrét adatbázisok felületén, amennyiben gyanús a kiadvány. Érdemes ellenőrizni például az adatbázist, ha a folyóirat honlapján annak logója nem linkelt, nem vezet egy kattintással az adatbázis megfelelő felületére.

Bírálat, lektorálás időtartama

A tudományos folyóiratok hagyományosan nagy gondot fordítanak a leközölt cikkek minőségi, tudományos szintű ellenőrzésére. A magas IF értékkel rendelkező, rangos tudományos folyóiratok esetében ez akár 6-8 hónap is lehet. A korábban leírt publikációs kényszer és a tudományos kommunikáció gyorsulása miatt természetesen kecsegtető lehet, ha egy folyóirat gyors bírálattal hirdeti magát. A predátor folyóiratok esetében ez az idő jelentősen lecsökken, akár egy hétre. Ebben az esetben nem is kérdés, hogy minőségi bírálatról nem beszélhetünk, ha a folyóirat 7 napos bírálatot ígér. Ezek a folyóiratok sokszor még a publikációs díj mellett felkínálnak un. „Fast track" szolgáltatást. Egy újabb összeg fejében még gyorsabb bírálatot ígérnek, akár „2-5" nap alatt bírálják el a cikket.

Székhely

A szerkesztőség irodája vagy székhelye nyilvános adat a folyóirat honlapján. Amennyiben ez nincs feltüntetve, az már gyanúra ad okot. Sok esetben a folyóirat honlapján megtalálható ez az adat, ami legtöbbször az Egyesült Államokban működő irodára utal. Ha a gyanú fennáll, akkor mindenképp megér egy ellenőrzést, hogy a google térképen mit mutat ez a cím. Sokszor belefuthatunk egy-egy meghökkentő eredménybe: autópálya lehajtó vagy egy raktártelep.

Hamis tudományos metrikák

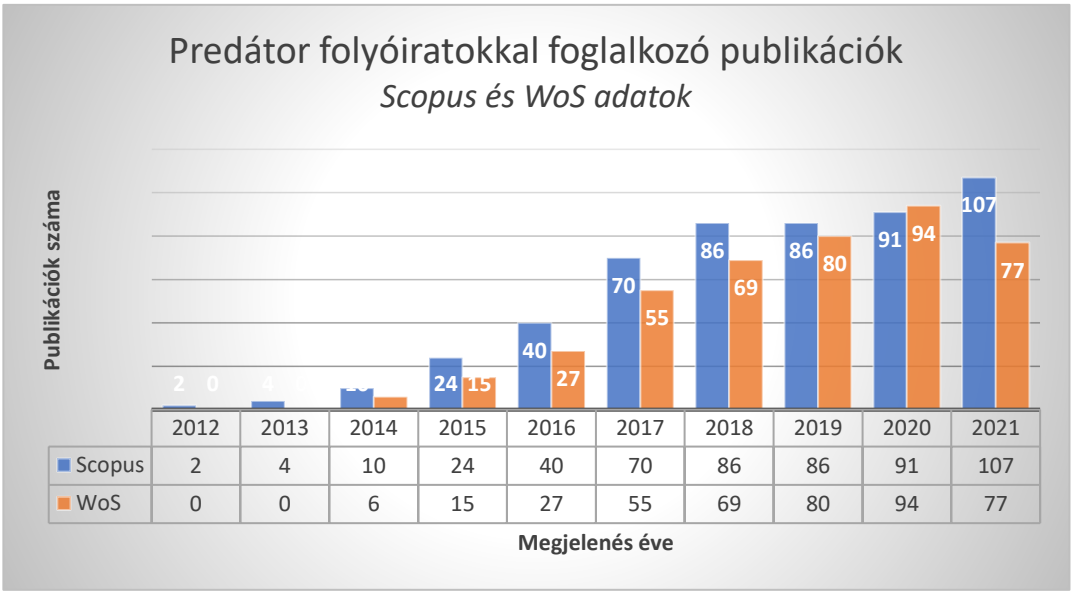
A folyóirat félrevezető, hamis "impakt faktor" vagy egyéb tudománymetriai értékeket tüntet fel magáról. Ha egy folyóirat honlapján Impact Factor értéket látunk, akkor mindenképp ellenőrizzük a Clarivate Journal Citation Reports adatbázisában. Ha nem szerepel az adatbázisban a folyóirat, akkor már nincs is több kérdés. (Az Impact Factor egyébként levédett márkaneve a Clarivate cégnek.) Viszont a predátor jelenség egyik fontos területe a

hamis metrikák létrejötte. Sok olyan „tudományos mérőszám” található ezeken a honlapokon, amelyek kísértetiesen hasonlítanak a hiteles tudományos metrikákhoz. (Universal Impact Factor, CiteFactor, Cosmos IF, General Impact Factor…)

Ezen jellemzők alapján jól látszik, hogy a predátor folyóiratok felismeréséhez a kutatóknak tisztában kell lenniük a jelenleg elérhető, hivatalos tudományos rangsorokkal, a hiteles tudománymetriai mérőszámokkal, illetve a tudományos adatbázisokat is ismerniük kell. A predátor folyóiratok ezeket a rangsorokat és a tudománymetriai értékeket is meghamisítják. [3]

A PREDÁTOR JELENSÉG VIZSGÁLATA

Több szempontból is vizsgálják a predátor folyóiratok működését a különböző szakterületen dolgozó kutatók. A téma aktualitását mutatja, hogy az elmúlt 10 évben a predátor kiadók és folyóiratok problémájával kapcsolatban évről-évre egyre több publikáció jelent meg. Ezt egy korábbi kutatásom során be is mutattam. A vizsgálat a Scopus és a Web of Science adatbázisok információin alapult, ahol a 2012 és 2021 között megjelent, kapcsolódó publikációk vizsgálata történt meg. Az eredmény egyértelmű, a predátor folyóiratok problémája egyre jobban foglalkoztatja a tudományos közösséget (1. ábra). [4]



	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Scopus	2	4	10	24	40	70	86	86	91	107
WoS	0	0	6	15	27	55	69	80	94	77

1. Ábra. Predátor folyóiratokkal foglalkozó publikációk. (2012-2021 / Scopus és WoS) Saját szerkesztés.

Mind a két adatbázisban lekérdezhető a felhasznált adathalmaz, bármikor reprodukálható a keresés a következő CCL keresőkifejezésekkel:

Scopus

(TITLE-ABS-KEY ("predatory journal") OR TITLE-ABS-KEY ("pseudo journal*") OR TITLE-ABS-KEY ("fraud journal*") OR TITLE-ABS-KEY ("hijacked journal*") OR TITLE-ABS-KEY ("predatory publis*")) AND PUBYEAR > 2012 AND PUBYEAR < 2022.*

Web of Science

(((TI=("predatory journal" OR "pseudo journal*" OR "fraud journal*" OR "hijacked journal*" OR "predatory publis*")) OR AB=(("predatory journal*" OR "pseudo journal*" OR "fraud journal*" OR "hijacked journal*" OR "predatory publis*"))) OR AK=(("predatory journal*" OR "pseudo journal*" OR "fraud journal*" OR "hijacked journal*" OR "predatory publis*"))) OR KP=(("predatory journal*" OR "pseudo journal*" OR "fraud journal*" OR "hijacked journal*" OR "predatory publis*")).*

A találati lista további elemzése megmutatta azt is, hogy mely szakterületeken van leginkább jelen az online tudományos kommunikációban a predátor jelenség. A megjelent publikációk kapcsán vizsgáltam, hogy a publikációk milyen folyóiratokban jelentek meg szakterület szempontjából. Ez alapján mind a Scopus, mind a Web of Science eredmények esetében kirajzolódtak azok a tudományterületek, amelyeken a legnagyobb problémát okozzák a kétes folyóiratok. Látható, hogy mind a két adatbázis esetében 30% körüli azon publikációk száma, amelyek a probléma egészével foglalkoznak (Social sciences és Information sciences), a többi publikáció valamely szakterületi folyóiratban jelent meg (1. táblázat). [5]

Subject Area *Scopus*	Pub. (%)	WoS Categories *Web of Sciences*	Pub. (%)
Social Sciences	30,4%	Information Science Library Science	32,1%
Medicine	25,1%	Medicine General Internal	13,0%
Computer Science	9,8%	Computer Science Interdisciplinary Applications	6,6%
Nursing	5,0%	Nursing	5,4%
Business, Management and Accounting	4,9%	Multidisciplinary Sciences	4,7%
Engineering	4,7%	Education Educational Research	4,0%
Biochemistry, Genetics and Molecular Biology	3,7%	Ethics	3,5%
Arts and Humanities	3,3%	Communication	3,3%
Agricultural and Biological Sciences	1,6%	Computer Science Information Systems	2,8%
Multidisciplinary	1,7%	History Philosophy Of Science	2,8%

1. Táblázat: Predátor folyóiratokkal foglalkozó publikációk aránya tudományterület szerint. Saját szerkesztés.

Az általánosan, a probléma feltérképezésével és esetleges megoldásával foglalkozó kutatásokban felmerül a kérdés, hogy kik és miért publikálnak a predátor folyóiratokban.[6] Kijelenthető, hogy természetesen nem csak a tapasztalatlan, átvert kutatók jelentetik meg kéziratait ilyen folyóiratokban. A publikációs nyomás és az elvárásoknak való megfelelési kényszer rávihet kutatókat, hogy éljenek a predátor kiadók adta „lehetőségekkel". [7] A probléma, hogy amint kiderül egy predátor folyóiratról a valódi minősége, tudományos értéke, ez megbélyegzi az ott publikáló vagy a szerkesztőbizottságba „beválogatott" kutatót is.

Az elmúlt 10 évben több kutatás próbálkozott a predátor jelenség körülírásával, meghatározásával, fogalmi definíciójával.[8] Jól mutatja a terület érzékenységét, hogy 10 évet kellett várni egy elfogadott definícióra: „*A predátor folyóiratok és kiadók olyan szereplők, amelyek az önérdekeket helyezik előtérbe a tudományosság rovására, és jellemző*

rájuk a hamis vagy félrevezető tájékoztatás, a legjobb szerkesztési és publikálási gyakorlatoktól való eltérés, az átláthatóság hiánya és/vagy az agresszív és válogatás nélküli beszervezési gyakorlatok alkalmazása."[4] [9]

A szakterületi folyóiratokban megjelent publikációkat vizsgálva meghatározhatók azok a területek, amelyeken a lenagyobb problémát okozzák a predátor kiadók. Ezeken a területeken jelent meg a legtöbb olyan publikáció, amely a predátor folyóiratok felismerhetőségével, veszélyeivel és az ilyen folyóiratokban történő publikálás következményeivel foglalkozik. Kimagasló százalékban szerepelnek az ilyen publikációk az orvostudományi és a kapcsolódó szakterületi folyóiratokban. [10-12]

PREADÁTOR FOLYÓIRATOK HATÁSA A TUDOMÁNYOS KOMMUNIKÁCIÓ SZEREPLŐIRE

A predátor kiadók email-ek küldésével és erőszakos marketingstratégiát alkalmazva kecsegtetnek a gyors megjelenés lehetőségével. A predátor folyóiratokban megjelent publikációk száma évről-évre nő. Ilyen mennyiségű megjelent cikkre nem lehet magyarázat az, hogy a kutatókat megtévesztették, tapasztalatlanok voltak és nem voltak jártasok az online publikálás világában. Más okok is szerepet játszanak abban, hogy a kutatók, oktatók ilyen kiadványokban publikálnak.

Az online tudományos kommunikáció predátor jelensége több szinten veszélyezteti a tudományos közösség résztvevőit. Érdemes megvizsgálni a résztvevőket, illetve veszélyeztetettségüket.

Milyen résztvevők lehetnek?

- Szerző, kutató, oktató
- Egyetemi kar, szervezeti egység, intézet, tanszék
- Egyetem, kutatóhely, tudományos intézmény
- Ország, nemzet, társadalom

Szerző, kutató, oktató

Első megközelítésben leginkább a kommunikációban résztvevők legkisebb elemét, a kutatói motivációt kell feltérképezni. Fel kell tenni a kérdést: miért publikál valaki predátor folyóiratban?

- A tudományos előmenetellel járó, elvárt követelmények teljesítése
- Tudományos kutatói díjak, teljesítmény díjak megszerzése
- A munkahely elvesztésétől való félelem / Publish or Perish nyomás
- Kutatói/oktatói rangsorok
- Tájékozatlanság a tudományos publikálás világában

A kutató, oktató oldaláról a predátor kiadványokban történő publikálás komoly következményekkel járhat. Ha a kutató nincs tudatában annak, hogy a kéziratát egy predátor folyóiratnál jelentette meg és a korábbiakban valamilyen szintű elvárásoknak megfelelt az

[4] *„Predatory journals and publishers are entities that prioritize self-interest at the expense of scholarship and are characterized by false or misleading information, deviation from best editorial and publication practices, a lack of transparency, and/or the use of aggressive and indiscriminate solicitation practices."* [9]

a publikációja, akkor azt gondolhatja, hogy más területeken is „beválthatók" ezek a publikációk. Ha a tudományos karrier során a kutató eljut egy olyan lépcsőfokhoz vagy egy olyan nemzetközi pályázat kapcsán adja be jelentkezését, ahol komolyabban vizsgálják a feltételeket, akkor kiderülhet, hogy valójában nem felel meg. Sőt, azáltal, hogy ilyen kiadványokban publikált korábban, akár megbélyegezhetik az adott kutatót a tudományos életben. A kézirat visszavonására pedig szinte esélytelen.

Sokszor felmerülő kérdés a kutatók felől, hogy milyen módon vonható vissza a cikk, illetve publikációs etikai szabályszegést követnek-e el, ha benyújtják ugyanazt a kéziratot más folyóirathoz? Ha egy cikket egyszer már benyújtott a szerző predátor folyóirathoz, akkor alig van remény arra, hogy sikeresen visszavonja a cikkét. Az ilyen kéréseket a folyóiratok vagy figyelmen kívül hagyják, vagy nem tesznek eleget neki. Miután a predátor folyóirat közzétette a cikket, ami gyakran értesítés nélkül történik, a kutatók azt kockáztatják, hogy a kettős publikációra vonatkozó publikációs etikai szabályokba ütköznek, ha a cikket egy másik folyóirathoz nyújtják be, függetlenül attól, hogy a szerzői jogokat átadták-e vagy sem.

Még rosszabb a helyzet, ha egy ilyen folyóirat a kutatót szerkesztőbizottsági tagnak kéri fel. Sokszor ez hasonló módon történik, mint ahogy a kéziratok esetében küldött kéretlen levelekben is. A kutatóhoz érkezik egy levél, amiben méltatják az eddigi tudományos teljesítményét és leírják, hogy mennyire nagy megtiszteltetés lenne a folyóirat számára, ha a szerkesztőbizottságban tudnák őt. Sok kutató egy ilyen lehetőséget büszkén fogad, ha nem ismeri a folyóirat minőségét. Ráadásul a kutatói előmenetel, karrier különböző lépcsőfokainál plusz pontot jelenthet az, ha valaki nemzetközi folyóirat szerkesztőbizottságában van benne. Ezzel a predátor folyóirat máris szintet lépett, mivel egy hiteles – létező – kutató neve (és persze intézménye) fényképe jelenhet meg a folyóirat honlapján. Ez pedig természetesen további megtévesztésre ad lehetőséget. Az ilyen esetekben talán könnyebb valamivel a szerkesztőbizottsági tagság visszavonása, de sokszor az ilyen jellegű kérésekkel sem foglalkoznak a predátor folyóiratok.

Egyetemi kar, szervezeti egység, intézet, tanszék

A predátor kiadók és folyóiratok negatív hatása nem csak a kutatók szintjén jelenik meg, a negatív publikációs eredmények és a presztízs veszteség tovább adódik a szervezeti egység, egyetemi kar szintjére. A kar vagy kutatóhely esetében folyamatosan vannak megmérettetések. Akár egyetemen belüli rangsorok, teljesítmény összehasonlítások formájában, akár akkreditációs folyamatok során az egység összteljesítménye meghatározó. A szervezeti egységek, karok tudományos teljesítményének – legalább – negyedéves monitorozása ma már elengedhetetlen. Gyakran kutatói, oktatói szinten év elején meghatározzák a teljesítendő publikációs kibocsátást. Ezekkel az eredményekkel természetesen számol a kar vagy szervezeti egység vezetése is. Amennyiben az elszámoláskor derül ki, hogy valójában „értéktelen" a publikáció a megjelenés szempontjából, az már késő. Ez pedig már nem csupán presztízs veszteséggel jár, hanem költségvetési szempontból is negatívan érintheti például egy egyetemi kar következő évét. A karon belül is rangsorolhatják a szervezeti egységeket a tudományos teljesítmény alapján, ha a költségvetés bizonyos része ilyen feltételhez kötött.

Egyetemi kar, szervezeti egység, intézet, tanszék

Ahogy a kutatók teljesítménye a szervezeti egységénél meghatározó, úgy természetesen az egyetemi kar felé is tovább adódik a kutató predátor folyóiratokkal való kapcsolatának hatása. Az egyetemek, tudományos intézmények esetében külön követelmények elvárások érkeznek a tudományos publikációk számára, azok minőségére, illetve a hivatkozásokra vonatkozóan. Ezeket az indikátorokat évről-évre teljesíteni kell, mert az intézmény költségvetése függ ezektől. A magyar felsőoktatási rendszerben jelenleg szinte 95% körüli a modellváltó egyetemek aránya. A térségben ez a felsőoktatási finanszírozási forma nem szokatlan, Lengyelországban, Csehországban és Szlovákiában is hasonló módon működnek az egyetemek.

Ebben a rendszerben az állam és a felsőoktatási intézmény szerződésben fekteti le, hogy milyen követelményeknek kell megfelelni az adott évben például az oktatás és a tudományos eredmények tekintetében. Témám szempontjából a tudományos indikátorok meghatározók. A modellváltó egyetemek éves teljesítményére vonatkozóan teljesíteniük kell a szerződésben szereplő publikációs és citációs vállalásokat. Ezekben a Scimago Journal Rank D1-Q1-Q2, illetve a Clarivate/InCites Top10% publikációk kompozit értéke, illetve a Web of Science és Scopus adatbázisokban szereplő, az egyetem publikációira kapott hivatkozások száma szerepel.

Ebben a rendszerben az egyetemnek folyamatosan monitorozni kell a tudományos kibocsátást. Nem megengedhető, hogy kétes folyóiratokban jelenjenek meg olyan publikációk, amelyek esetleg egy az indikátoroknak megfelelő folyóiratban is megjelenhettek volna.

Az egyetemek és a felsőoktatás számára a másik nagy megmérettetés a különböző, nemzetközi felsőoktatási rangsorokban történő részvétel. Természetesen ezek a szervezetek eltérő módszertannal, különböző számítási arányokkal vizsgálják az egyetemeket és ez alapján aktualizálják az adott évi rangsort. Témám szempontjából természetesen a tudományos kibocsátás, illetve a hivatkozások vizsgálata a legérdekesebb a rangsorok esetében is. Bármelyik – hiteles – egyetemi rangsort vesszük, mindegyiknél elmondható, hogy a Web of Science vagy a Scopus adataival dolgozik a tudományos indikátorok vizsgálatakor. Így a predátor folyóiratokban történő publikálás megint csak negatívan érinti az egyetem egészét.

Az egyetemek és tudományos intézmények költségvetésében komoly helyet foglalnak el a különböző nemzeti és európai uniós, kutatásra irányuló pályázati források. Ezen forrásokra szigorú elszámolás és többször teljesítési mérföldkövek vonatkoznak. A legtöbb ilyen pályázat esetében a teljesítésigazolás meghatározott szintű publikálással történik a kutatási eredmények bemutatásával. Amennyiben a pályázatban résztvevő kutatók nem megfelelő kiadványban publikálnak, az akár a támogatás visszafizetési kötelezettségével is járhat.

Az egyetemek oldaláról a kutatóknál említett presztízs veszteség természetesen az egyetemet, illetve a tudományos intézményt is érinti. A szerző affiliációja ott szerepel a megjelent cikken, a folyóirat weboldalán pedig gyakran fel is tűntetik, hogy milyen intézményből publikáltak náluk kutatók. Az egyetem működése szempontjából a reputáció, amelynek része természetesen az egyetemi rangsorokban való minél magasabb helyezés elérése is, nagyon fontos, akár a beiskolázást, akár a nemzetközi szintű kutatókkal történő közös kutatást vagy esetleges szerződtetésüket nézzük.

Ország, nemzet, társadalom

A témám szempontjából legmagasabb szinten ugyanúgy elmondható a kutatói szinten meghatározott predátor folyóiratok hatása. A magyar kutatók összesített teljesítménye mutatja az ország, a nemzet teljesítményét. a kutatások finanszírozása, az egyetemi modellváltás rendszere erre hatással van. Az országok vonatkozásában is évről-évre készülnek kimutatások és rangsorok. Ilyen például a folyóiratok minősítésében ismertebb Scimago esetében a Country Rank, ahol a publikációs kibocsátás alapján rangsorolják az országokat.

Az eddigiekben a predátor folyóiratok hatását a tudományos kommunikáció szempontjából jellemeztem, de nem lehet figyelmen kívül hagyni a tömegkommunikációra és így a társadalomra gyakorolt hatásokat sem. Áttekintve az eddigi kutatási eredményeket és a témával kapcsolatosan megjelent publikációkat, kevés információt találunk a jelenség és a tömegkommunikáció kapcsolatáról. Az eddigi kutatások főként a tudományos kommunikáció szintjén vizsgálták a problémát: milyen veszélyei vannak egy predátor folyóiratban történő publikálásnak a kutató előmenetele, pályázati lehetőségei szempontjából vagy akár egy intézmény milyen károkat szenvedhet el, ha nem vizsgálja tudományos kibocsátását ebből a szemszögből is.

Az elmúlt években viszont egyre inkább látható, hogy a predátor folyóiratokban megjelenő tartalmak a média, a közösségi média felületein is megjelennek, de közvetetten. A közösségi médiában, különböző csatornákon az összeesküvés elméletek és a megtévesztés, a dezinformáció könnyedén hitelessé tehető egy hivatkozott tudományosnak vélt tartalommal. A predátor folyóiratainak tartalma – amennyiben a közösségi média eszközeit „megfelelően” használják – éppen olyan gyorsan is terjedhet, mint a hiteles, tudományos folyóiratoké. Ez pedig egyenesen vezethet a megbízhatatlan információk terjedéséhez. Egy friss kutatás szakterületi szinten vizsgálta a fogászati folyóiratokban megjelent publikációk terjedését a közösségi médiában. (Instagram, Facebook és Twitter) A folyóiratokat predátor és hiteles besorolással látták el a rendelkezésre álló információk alapján. Az eredményül kapott adatok alapján elmondható, hogy a szakterületen mind a predátor, mind a hiteles folyóiratokban megjelent publikációk terjedése a vizsgált közösségi média felületeken szinte megegyezett. [13]

Ahogy láthattuk, ezek a folyóiratok sokszor megtévesztésig hasonlítanak egy elfogadott, tudományos folyóirathoz, természetesen a hasonlóság csak a külsőségek szintjén értelmezhető. Tartalmilag viszont a tudományos ellenőrzés, bírálat, a lektorálás hiánya azt eredményezi, hogy egy látszólag tudományos kutatás eredményét olvassuk publikációként. Ezek a publikációk pedig tökéletesek egy-egy manipulatív-, megtévesztő- vagy álhír tudományos alátámasztásához. Gondoljunk csak bele, hogy a jelenleg beazonosítható sok ezer predátor folyóirat akár tapasztalt kutatókat is megtéveszt, olyan szerzőket, akik ebben a szférában élnek, dolgoznak, publikálnak. Hogyan várható el a hétköznapi embertől, hogy felismerje a hír mögötti, hivatkozott „tudományos” alátámasztást?

Napjaink közösségi média felületei a legalkalmasabb területek az összeesküvés elméletek és a megtévesztő hírek terjesztésére. A hétköznapi ember pedig a médiából kapott információknak nagyon ritkán néz utána. Ha pedig esetleg mélyebben utánajárna a forrásnak, akkor is nagyon nehezen tudná beazonosítani a forrás minőségét. A problémát ebből a szemszögből nézve a predátor kiadók akaratlanul is terjesztői, alátámasztói lehetnek a különböző konteóknak és persze a dezinformációnak is. Ha pedig bármelyik népszerű videómegosztó platform hiteltelen, összeesküvés elméleteket terjesztő csatornáját nézzük, ahol

a hivatkozott „tudományos" publikáció csak felvillan a jobb felső sarokban, akkor még messzebb kerülünk a valóságtól.

ÖSSZEGZÉS

A predátor folyóiratok és kiadók jelenléte a tudományos világban, az online tudományos kommunikációban az elmúlt 10 évben egyre erősödött. A predátor folyóiratokkal foglalkozó kutatások, publikációk száma az elmúlt évtizedben évről-évre nőtt. Az online tudományos kommunikáció egyes szereplőire gyakorolt hatást vizsgálva megállapítható, hogy a predátor folyóiratokban történő publikálás negatív hatásai „átöröklődnek" a szintek között.

Az eddigi kutatások és publikációk leginkább a tudományos világra gyakorolt hatások szemszögéből vizsgálták a jelenséget. A legtöbb kutatás a predátor folyóiratok jellemzőit gyűjtötte össze, kategorizálta azokat, ellenőrző listákat (fehér és fekete listákat) hozott létre és magát a problémát csak a tudományos közegbe helyezve elemezte. Az elmúlt években a médiában és leginkább a közösségi médiában megjelenő dezinformációk, megtévesztések és manipulációk nyomán egyre inkább felmerül a kérdés: a predátor jelenség biztos, hogy csak a tudományos világban okoz károkat? Véleményem szerint ezeket a hatásokat vizsgálni kell, mert az elmúlt 10 évben a tudományos szférában sem sikerült megnyugtató megoldást találni a problémára. Társadalmi szinten, az információfogyasztási szokások várható alakulását figyelembe véve, ezen a területen még nehezebb lesz kiszűrni a megtévesztő tartalmakat.

FELHASZNÁLT IRODALOM

[1] E. Knowles, Ed. „*Oxford Dictionary of Phrase and Fable*." Oxford University Press. 2006.
DOI: 10.1093/acref/9780198609810.001.0001

[2] I. A. Moosa, „*Publish or Perish - Perceived Benefits versus Unintended Consequences*." Edward Elgar Publishing. 2018.
DOI: 10.4337/9781786434937

[3] L. Berek, „Predátor kiadók és folyóiratok az online tudományos publikálás világában" in, Muhi Béla (szerk) *Vajdasági Magyar Tudóstalálkozó 2020 – Konferenciakötet*. B. Muhi Ed. Újvidék, Vajdasági Magyar Akadémiai Tanács. 2021. pp. 74-80.

[4] L. Berek, „Az online tudományos kommunikáció hitelességét veszélyeztető tényezők." *Biztonságtudományi Szemle*. Vol 4(2se.), pp. 35-41., 2022.
https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/286

[5] L. Berek, „A Decade of Predatory Journals with an Overview of the Literature : literature analysis, the first step of a systematic review" *Transactions On Internet Research - IPSI BGD.*. Vol. 18.(1.) pp. 4-8., 2022.

[6] S. Kurt, „Why do authors publish in predatory journals?" *Learned Publishing*, 31(2), pp. 141-147., 2018.
DOI: 10.1002/leap.1150

[7] S.B. Demir, „Predatory journals: Who publishes in them and why?" *Journal of Informetrics*, 12(4), pp. 1296-1311., 2018.
DOI: 10.1016/j.joi.2018.10.008

[8] K.D. Cobey et al, „What is a predatory journal? A scoping review” *F1000Research*, 7., 2018.
DOI: 10.12688/f1000research.15256.1
[9] A. Grudniewicz et al, „Predatory journals: No definition, no defence.” *Nature*, 576(7786), pp. 210-212. 2019.
DOI: 10.1038/d41586-019-03759-y
[10] A. Cortegiani et al: „Predatory open-access publishing in anesthesiology” *Anesthesia and Analgesia*, 128(1), pp. 182-187., 2019. https://10.1213/ANE.0000000000003803
[11] A. Cortegiani et al, „Predatory open-access publishing in critical care me-dicine.*”* *Journal of Critical Care*, 50, pp. 247-249., 2019. https://10.1016/j.jcrc.2018.12.016
[12] G. Richtig et al, „Problems and challenges of predatory journals” *Journal of the European Academy of Dermatology and Venereology*, 32(9), pp. 1441-1449., 2018.
https://10.1111/jdv.15039
[13] D. Al-Moghrabi et al, „An analysis of dental articles in predatory journals and associated online engagement” *Journal of Dentistry*, 129., 2023. 10. 25.
https://10.1016/j.jdent.2022.104385

APPEARANCE OF SAFETY AND SECURITY IN THE HUMANITIES (PART 1)

A BIZTONSÁG MEGJELENÉSE A HUMÁN TUDOMÁNYOKBAN (1. RÉSZ)

KOLLÁR Csaba[1]

Abstract

The study, which is the first part of a three-part series, examines the emergence of the concept of safety and security in the humanities, with particular attention to ethology, evolutionary biology, and sociology. It analyzes the instinctual pursuits of safety and social behaviors in animals, which fundamentally determine the survival and evolution of species. By comparing human behavior and societal structures, the author highlights how the demand for safety significantly shapes human groups and societal institutions, including legal systems and political decision-making. The study also elaborates on how modern societies adapt to changing security challenges.

Keywords

safety and security, humanities, ethology, evolutionary biology, sociology, social adaptation

Absztrakt

A tanulmány – mely egy háromrészes sorozat első része – a biztonság fogalmának megjelenését vizsgálja a humán tudományokban, különös tekintettel az etológia, az evolúciós biológia és a szociológia területére. Az állatok biztonság iránti ösztönös törekvései és társas viselkedése kerül elemzésre, amelyek alapvetően meghatározzák a fajok fennmaradását és fejlődését. Az emberi viselkedés és társadalmi struktúrák összehasonlításával a szerző rámutat arra, hogy a biztonság iránti igény milyen mértékben formálja az emberi csoportokat és társadalmi intézményeket, beleértve a jogrendszereket és a politikai döntéshozatalt is. A tanulmány azt is kifejti, hogy a modern társadalmak hogyan alkalmazkodnak a változó biztonsági kihívásokhoz.

Kulcsszavak

biztonság, humán tudományok, etológia, evolúciós biológia, szociológia, társadalmi adaptáció

[1] kollar.csaba@uni-obuda.hu | ORCID: 0000-0002-0981-2385 | senior research fellow and leader, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering Artificial Intelligence Workshop | tudományos főmunkatárs és vezető, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mesterséges Intelligencia Műhely

BEVEZETÉS

A „Biztonság megjelenése a humán tudományokban” című tanulmánysorozat első részében a biztonság fogalmának különböző megközelítéseit vizsgálom meg a humán tudományok területén, különös tekintettel az etológia, az evolúciós biológia és a szociológia diszciplináira. A biztonság, mint alapvető szükséglet és motiváció, minden élőlény életében jelen van, azonban az emberi társadalmakban különösen összetett jelenségeket eredményez. A tanulmány először az állatvilág biztonság iránti törekvéseit elemzi, melyek az ösztönös viselkedésminták és a társas interakciók révén a fajok fennmaradását és fejlődését szolgálják. Ezt követően a figyelem az emberi viselkedés felé terelődik, ahol a társadalmi struktúrák, normák és intézmények fejlődését vizsgálom a biztonság iránti igény tükrében. Az emberi csoportok és társadalmak formálódnak és alakulnak a biztonság iránti igény mentén, beleértve a jogrendszereket és a politikai döntéshozatalt is. A tanulmány továbbá megvizsgálja, hogy a modern társadalmak hogyan alkalmazkodnak a változó biztonsági kihívásokhoz, amelyek a globalizáció és a technológiai fejlődés következményei. Ez a rész a biztonság multidiszciplináris megközelítését hivatott bemutatni, rávilágítva arra, hogy a biztonság fogalma milyen mélyen gyökerezik a biológiai alapoktól kezdve az összetett társadalmi szerkezetekig. A tanulmány célja, hogy átfogó képet adjon a biztonság tudományos megközelítéseiről, és bepillantást nyújtson abba, hogy ezek a megközelítések hogyan kapcsolódnak össze az egyéni és közösségi jólét kérdéseivel. Ezen keresztül írásművem hozzájárul a biztonság jobb megértéséhez és annak társadalmi, biológiai és szociológiai dimenzióinak feltárásához.

ETOLÓGIA ÉS EVOLÚCIÓS BIOLÓGIA

A biztonság fogalmának tartalmi értelmezésének sokféle megközelítés közül elsőként az etológia és az evolúciós biológia biztonság interpretációját adom meg. Tinberger [1] állatok viselkedésével foglalkozó munkájában kiemeli, hogy az állatok viselkedése, az örökölt, illetve tanult viselkedésminták erősen biztonság-fókuszúak. Az adott faj, vagy egyed biztonság-fókuszú viselkedése a záloga ugyanis a faj fennmaradásának. Tinberger [1], [2] mellett többek között Lorenz [3], Hinde [4], Bekoff [5] rámutatott arra, hogy az állatok alapvető életstratégiái, mint a reprodukció, a táplálkozás, a védekezés, a társadalmi viselkedés a biztonság irányába kongruálnak. Részletesebben: a fajfenntartás alapja a szaporodás, a génállomány továbbvitele, hiszen a reprodukció – pontosabban a sikeres reprodukció – a biztosítéka annak, hogy legyenek utódok, akik majd szüleikhez hasonlóan cselekszenek. Az egyed fejlődése szempontjából fontos a táplálkozás. Vannak állatok, akik születésüktől fogva magukra maradnak (pl.: teknősök), vagyis alapvető ösztöneikre vannak utalva, hogy a táplálékot megszerezzék, míg másokat (pl.: madarak, emlősök) születésük után szüleik táplálnak, illetve tanítanak meg a táplálékszerzésre. Miután a fiatal egyedek az önfenntartásukhoz szükséges ismereteket elsajátítják, felnőtté válnak, s fajtól függően vagy elhagyják (pl.: medvék), vagy a többi fajtársukkal közösen alkotott közösségekben maradnak (pl.: elefántok, majmok). Az állatok fizikai felépítése és képességei (pl.: (kitin)páncél, méregmirigyek, illetve méregfog, szárnyak – repülés), valamint egyéb lehetőségeik, mint az elrejtőzés, az ügyesség, a védekező testtartás, a védekező viselkedés, illetve a szimbolikus viselkedés biztosítják a számukra, hogy megvédjék magukat a ragadozóktól, illetve a környezeti veszélyektől. Az ember társas lény – ahogy arról többek között Mead [6], illetve

Aronson [7] is írt – de hasonló figyelhető meg bizonyos állatok között is. Az állatok társas viselkedése jó stratégiának bizonyul a túlélésben – vélekedik Wilson [8] – hiszen a csorda, falka, boly, stb. lehetővé teszi, hogy eredményesebben vadásszanak (szerezzenek táplálékot) és hatékonyabban tudják megvédeni magukat. Hiba lenne azt gondolni, hogy csak a nagyobb, fejlettebb agyi kapacitással rendelkező állatokra jellemző a társas viselkedés. Wilson [8] a hangyák, míg Waal [9] a méhek esetében írta le, hogy a kolónia egyaránt jelenti az egyénnek és magának a kolóniának is a legeredményesebb túlélési stratégiát. A jól működő kolónia túlélési „filozófiája" az egyént gyakran altruistává teszi, vagyis feláldozza magát azért, hogy a kolónia, s tágabban értelmezve a faj túléljen. Társas közösségben élő állatoknál, ha az egyén nem talál vissza a kolóniába, vagy a kolónia kiközösíti, akkor az rendszerint az egyén halálát jelenti.

Az etológia és az evolúciós biológia vizsgált témái között nem csak az állatok, hanem (akár összehasonlítás jelleggel) az emberek is szerepelnek. Waal [10] az emberi viselkedést hasonlítja össze a majmok viselkedésével a „Belső majmunk" című könyvében. A majmok társas viselkedése a szerző szerint eklatáns példája a közösség biztonságra való törekvésének, s rámutat arra, hogy a közösségen belüli együttműködés hogyan szolgálja az egyén és a közösség biztonságát. A majmoknál megtapasztalt együttműködés az emberi közösségekre is jellemző, s többek között az emberi kapcsolatokban, a családban, s tágabban értelmezve akár a nemzetközi kapcsolatokban is megnyilvánul. Az egyének és csoportok közötti együttműködés – vélekedik a szerző – hozzá tud járulni a biztonság növekedéséhez a társadalmakban, ami révén elkerülhetőek a biztonsági konfliktusok (legalábbis társadalomtudományi megközelítés szerint). Csányi [82 p. 13] nem feltétlenül csak előnyként tekint a csoporttagok közötti együttműködésre, bár ő is a csoport által nyújtott biztonság mellett foglal állást. Ahogy a csoportszerkezettel kapcsolatban írja „Az egyedül történő táplálékszerzés csökkenti a felesleges vetélkedéseket, de biztonsági problémákat okoz: a ragadozókat valahogyan el kell kerülni. A csoportos gyűjtögetés biztonságossá teszi ugyan az egyed életét, de ilyen esetben megnő a csoporton belüli versengés a közös erőforrásokért, és kialakulnak a csoportviselkedést, a versengést szabályozó viselkedési mechanizmusok". Waal [10] munkájában a társas kapcsolatok, illetve a biztonság hiányából eredő negatív következményeket vizsgálva megállapítja, hogy ezek hozzájárulnak a stressz, a szorongás és a félelem kialakulásához és fenntartásához, ami véleményem szerint – ahogy arról még később a téma pszichológiai aspektusánál írni fogok – elősegítheti az egyén (akár ember, akár állat) sebezhetőségét, fizikai és mentális bántalmazhatóságát, szélsőséges esetben akár halálát is. Babelcombe [12] a félelem és a biztonság érzetét állítja szembe egymással, elsősorban az állati viselkedést tanulmányozva. Ahhoz, hogy az állatok jól érezzék magukat, élvezzék az életet, s ne legyenek frusztráltak a félelem miatt, szükségük van arra, hogy biztonságban érezzék magukat. Bekoff [13] Babelcombe-hoz [12] hasonlóan úgy gondolja, hogy a biztonságérzet az alapja annak, hogy az állatok jól érezzék magukat. Az állatok jó érzelmi állapota, jó közérzete, s általános jólléte erősen pozitívan korrelál a biztonsággal. A (majom)közösségen/kolónián belüli kommunikáció, s a (nonverbális) kommunikáció révén megosztott információk, jelzések a kolónia tagjai számára nagyfokú biztonságot jelentenek. A kommunikáció hiteles, tartalma valós, a környezet pillanatnyi állapotáról szolgál információkkal akkor is, amikor például egy fiatal egyed ezt egyébként még nem venné észre, vagy nem tudná megfelelően értelmezni/értékelni, így idősebb fajtársai jelzéseire hagyat-

kozik. A majmok biztonságérzetét – vélekedik Cheney és Seyfarth [14] – alapvetően befolyásolja társaik jelenléte, a közöttük levő kapcsolatok minősége, a kapcsolat fenntartását (is) szolgáló kommunikáció. Véleményem szerint Babelcome [12], Bekoff [13], Cheney és Seyfarth [14] meglátásai az emberi biztonságérzetre is igazak. Az állatok és az emberek fenyegetésekre adott viselkedési válaszai között megannyi hasonlóság figyelhető meg Abbas [15] szerint. A félelem, a szorongás, a pánik (vagyis a biztonságérzet hiánya) az állatoknál és az embereknél pozitív és negatív mentális folyamatokat indít el. A pozitív folyamatok a biztonsági hiányosságok pótlására, javítására, kiküszöbölésére sarkallják az állatokat és az embereket annak érdekében, hogy elkerüljék a biztonság hiányából eredő még nagyobb kockázatokat és az esetleg bekövetkező káros eseményeket, a negatív folyamatok ugyanakkor rombolják az egyént, s veszélybe sodorhatják a közösséget is. Az egyén sebezhetőbbé válik, áldozatszerepbe kerül, feladja a küzdeni-, illetve élni akarást (ez egyébként igaz a beteg, öreg állatokra is). Könnyebben válik prédává, vagy szenved el balesetet. Az állati és emberi közösségek reakciója hasonló lehet: a sebezhető egyént feláldozzák, hátra hagyják, kiközösítik, vagy épp ellenkezőleg: megvédik, ápolják, gyámolítják, nem hagyják magára. A közösségben élő állatoknál az első stratégiát rendszerint akkor követik, ha az egyén hátráltatja, veszélyezteti a közösséget, vagy feláldozásával a közösség erősebb, egészségesebb, s így értékesebb tagjai megmenthetőek, vagy nem éri meg, vagy kockázatot jelentene az áldozat, amit a közösség az ilyen egyén érdekében hozna. Az első stratégiával akkor él az emberi közösség – erről részletesebben írok majd a téma későbbi részében – ha az egyén vét a közösségi/társadalmi normák ellen. A kiközösítés lehet(ett) többek között a faluból elkergetés, az egyházból történő kiátkozás, a boszorkányvád, a munkahelyi elbocsátás, a törvény szerinti börtönbe zárás, vagy egy (szűk) erőforráshoz való hozzáférés megtagadása, vagy korlátozása.

Wilson [8] és Mealey [16] hasonlóan vélekednek a társadalmi evolúció tekintetében. Az emberi társadalmak alakulása, s ennek részeként a társas kapcsolatok fejlődése, a társadalmi hierarchia kialakulása, a kollektív döntéshozatal, valamint a társadalmon belüli együttműködés a társadalmakat sikerre viheti, s minél inkább sikeresnek vélünk/gondolunk egy társadalmat, annál inkább mondható az biztonságosnak és békésnek is. Az ilyen társadalmak polgárai – írják a nevezett szerzők – boldogabbak, életük nyugodtabb, jövőjük kiszámíthatóbb. A béke állapota és a biztonság állapota közé egyenlőségjel tehető, ami a gyakorlatban azt jelenti – s erre az adott országról és társadalomról szóló narratívákban megannyi példa található – hogy az adott ország békés kapcsolatokat ápol a környező országokkal, ugyanakkor olyan keretet, mint szabályozó rendszert tart fenn és működtet (akár fizikai határ, akár jogi szabályozás), melyben arra törekszik, hogy a béke állapota fennmaradjon, s ezáltal a lakosságnak ne kelljen félnie, s maximális biztonságban érezze magát. A társadalom nem csak a fizikai fenyegetés miatt félhet, sőt sokszor alaptalan félelmek miatt lesz mentálisan beteg a társadalom. Ennek okait az amerikai társadalom vizsgálatában Glassner [24] a szórakoztatóiparban, a médiában és a politikában látja. A média nem csak jogi értelemben tekinthető tehát (a negyedik) hatalmi ágnak, hanem a társadalomra gyakorolt hatásában is. A médiatartalmak fogyasztása, s eleve a társadalom mediatizálódása azt jelenti, hogy az egyén egyre több információt szerez a médiából, ez jelentősen hat értékítéletére, szocializációjára. A média által közvetített és felnagyított erőszak, ami gyakran nem is valós tényeket mutat be, vagy az eltúlzott veszélyek bemutatása károsak az ember életére és döntéseire. A szerző [24] a megoldást abban látja, hogy az egyénnek kellően kritikusan kellene

fogadnia és fogyasztania a médiatartalmakat, hogy megőrizhesse valós, reális alapokon nyugvó biztonságérzetét. Ugyan az ember biztonságtudatosságának fejlesztése – ahogy arról még később bővebben írni fogok – egyéni, családi, munkahelyi, társadalmi szinten egyaránt hasznos lehet, de a hamis félelmekre épülő hamis biztonságérzet legalább annyira káros lehet, mint a hanyag, a reális biztonsági kihívásokkal nem törődő attitűd. Humánetológiai aspektusból a biztonságos társadalom fogalma egyenesen korrelál a csoport méretével, a csoport felépítésével, valamint a csoporton belüli (esetleg csoportok közötti) együttműködéssel – írja Moffett [25]. Meglátása szerint a nagyobb és összetettebb társadalmak rendszerint nagyobb biztonságot és védelmet nyújtanak az egyénnek, hiszen egy ilyen jól szervezett társadalom hatékonyabban tudja elhárítani a külső fenyegetéseket. Tévedés lenne azonban azt állítani, hogy a nagyobb és összetettebb társadalmak az egyénnek minden biztonsági dimenzióban biztonságot jelentenek, hiszen a társadalom méretének növekedése és rétegződése társadalmi konfliktusok forrása lehet, a városon belül kialakulhatnak saját törvényeik szerint működő gettók, a népsűrűség kedvez a fertőző betegségek és járványok terjedésének, növekszik a tömeges erőszak kockázata, s a bűnözői csoportok és a bűnüldözés szervei közötti együttműködés is tetten érhető. Erre megannyi példát lehet olvasni többek között Hinton [26], McInerney [27] tényfeltáró munkáiban.

SZOCIOLÓGIA

A szociológiában a biztonság fogalmának tartalmi feldolgozása során többféle, egymással nem, vagy csak részint kongruáló elképzeléssel találkozhatunk. Az elképzeléseket a feldolgozott szakirodalom alapján tanulmányomban három fő csoportba osztom: (1) társadalmi szinten értelmezett biztonság, (2) közösségi szinten értelmezett biztonság, illetve (3) egyéni szinten értelmezett biztonság.

A társadalmi szinten értelmezett biztonságot a gazdasági-politikai rendszer, a társadalmi szerkezet, a társadalmi interakciók, valamint a normák és elvárások alakítják elsősorban. Felelősség terheli e konstrukció megalkotásában, fenntartásában és fejlesztésében a politikai döntéshozókat, akik törvényekkel és azok betartatásával törekednek szavatolni az állampolgárok (jog)biztonságát, illetve a gazdasági szereplőket is, akik a munkavállalók számára munkahelyeket teremtenek, fizetést adnak, így biztosítva számukra a gazdasági biztonságot, a megélhetést. Foucault [17] a büntetőrendszerek történetét és fejlődését elemezve megállapítja, hogy a büntetőrendszerek fejlődése hogyan hat a társadalomra, s annak szabályozására. Az alapvető kérdés az, hogy az egyén kapjon-e, s ha igen, akkor milyen mértékű büntetést, ha a társadalom biztonsága ellen vét, vagyis bűnt követ el. Kérdéses a büntetés formája, ami a figyelmeztetéstől, megrovástól, a pénzbirságon, felfüggesztett és letöltendő szabadságvesztésen keresztül az életfogytiglani szabadságvesztésig, illetve (országoktól függően) a halálbüntetésig terjedhet. Az is kérdéses, hogy a törvények és a társadalmi normák ellen vétő egyén a büntetést követően felhagy-e a bűnismétléssel, s ha igen, akkor ezt miért teszi (pl.: félelem az újabb büntetéstől, a büntetés hatására megváltozott, szeretne a társadalom hasznos tagja lenni, stb.) [18]. A modern technológiák megjelenése, illetve a globalizáció – állítja Beck [19] – állandó fenyegetést jelent a társadalomra, mivel az ezek révén előidézett társadalmi változások, illetve a hozzájuk való alkalmazkodás sok erőforrás-allokációt követel meg az egyéntől. A biztonság ugyan nagyobb hangsúlyt kap (ami meglátásom szerint is jó), de e hangsúly magával hozza a biztonság fogalmának frag-

mentálódását (pl.: környezeti biztonság, közlekedésbiztonság, gazdasági biztonság, iparbiztonság) és kiterjesztését számos területre, s az ezeken a területeken beazonosított kockázatok és fenyegetések tudatosítása révén az egyén és a társadalom egyaránt azt érezheti, hogy állandó fenyegetettségnek van kitéve. A demokratikusan működő kormányoknak, a politikai hatalom gyakorlóinak, a kormányzati szerveknek és intézményeknek, a munkáltatóknak olyan megoldásokat kell kidolgozniuk és hihetően kommunikálniuk, amelyek a társadalom fenyegetettségérzetét úgy csökkentik, hogy közben az említett [20], [21] diktatúra-csapdákat elkerülik.

Ahogy arra korábban is utaltam, az emberi társadalmakat rendszerint a közösségekben való élet, illetve a közösségi aktivitások jellemzik. Tilly [22] munkájában 250 év társadalmi mozgalmait elemezve azt állapítja meg, hogy a társadalmi mozgalmak voltak a változások erőforrásai és katalizátorai, s e mozgalmak révén alakult, formálódott és fejlődött a társadalom, a demokrácia, a jogállam, s olyan fogalmak is értelmezést és hasznosulást nyertek, mint például a szolidaritás, az igazságosság és az egyenlőség. E fogalmak gyakorlati alkalmazása alapvetően növelni tudta a társadalom tagjainak biztonságtudatát, hiszen a környezeti és akár a társadalmon belüli politikai, gazdasági változásokkal szemben védelmet nyújthattak. Bauman [20] a modern társadalmak és a holokauszt közötti kapcsolatot elemezve rámutat arra, hogy miközben a 20. századra, mint modern társadalomra tekinthetünk – amelynek társadalmi védelmi mechanizmusai az egyénnek számos területen védelmet nyújthatnak, vagy legalábbis nem hagyja teljesen magára egy vesztes háború után sem – mégis szemtanúi vagyunk, hogy a modern társadalom racionális rendszerében is felépíthető egy népcsoporttal szemben olyan narratíva, amelyik a társadalmi egyenlőtlenségekért e népcsoportot felelőssé téve, annak ellehetetlenítésére törekszik. A Frankfurti Iskola – mely meglehetősen kritikusan viszonyult a náci Németországhoz – tagjai Németországra, mint a modern társadalom pozitív értékeinek ellenpéldájára tekintettek. A pozitív értékek hamar újfajta, negatív értelmezést kaptak, melyben az irányított és központosított propaganda, a kritikai gondolkodás elnyomása, a másképp gondolkodók üldözése, a jól körülhatárolt és definiált (belső) ellenség képének sulykolása, a társadalom homogenizálódásának, valamint a személyes és kollektív kreativitás elvetésének az irányába mutatott. Aki származása, vagy nézetei révén nem tudott, vagy nem volt alkalmas, hogy a homogén társadalom tagja legyen, azt a rendszer kivetette magából. A rendszer tehát önhatalmúlag meghúzta a határokat, melyeken belül gyakran a látszatbiztonság illúzióját tartotta fent, s akik a határokon kívül rekedtek, azokat, mint veszélyforrást aposztrofálta. A frankfurti iskolába tartozó Horkheimer és Adorno [21] azt vizsgálta, hogy milyen veszélyeket rejt magában az, ha a modern társadalom túlzottan is a biztonságra törekszik. Megállapították, hogy ha a biztonság túlzott ellenőrzéssel párosul, akkor a kreativitás beszűkül és az élet minősége romlik. Vagyis: miközben a modern társadalom biztosíthatja polgárainak a fizikai síkon a biztonságot (pl.: védik az ország határait, a rendőrség ellátja bűnüldöző feladatait, ha az egyén megbetegszik, orvosi kezelést kap, magánvagyonát törvények védik), addig – különösen az értelmiség – bezárva érezheti magát, ami mentális, illetve pszichoszomatikus betegségek kialakulásához vezethet. A szépirodalmi műként számon tartott 1984 [28], illetve a kínai Társadalmi Kredit Rendszere, mellyel többek között Kollár [29] [30] [31] is foglalkozott, a művészet és a realitás szemszögéből egyaránt azt mutatja, hogy a technikai fejlődés (pl.: a mesterséges intelligencia használata) a posztmodern társadalmakban is lehetővé teszi egy olyan társadalmi

biztonsági rendszer kiépítését, melyben ha az egyén elfogadja és betartja a rendszer elvárásait, akkor biztonságban, békében érezheti magát, hozzá tud férni a szűk/korlátos erőforrásokhoz, s „jó állampolgárként" előnyöket élvez, ellenkező esetben azonban rendszeridegen elemmé válik, s megannyi problémával kell megküzdenie, ami komoly hatást gyakorol biztonságtudatára és -érzetére egyaránt, s növekszik félelme a biztonságának hiánya miatt. A szociológia tudományterületén megjelenő, egyéni szinten értelmezett biztonsággal többek között Durkheim [23] foglalkozott. Véleménye szerint a munkamegosztás javítja a társadalmi integrációt, ami erősíti a társadalmi kohéziót, s ez elvezet a személyes biztonság növeléséhez. A társadalmi szerepek és a munkatevékenységek átgondolt és tudatos elosztása révén növelhető a társadalmi együttműködés, ami a szociális feszültségek csökkentésének az irányába hat. A munkamegosztás révén nem csak hatékonyabbá válik a munkavégzés, de a siker érdekében az egyéneknek kooperálniuk kell egymással, ahelyett, hogy versenyeznének. Az együttműködő attitűd fenntartása és erősítése pozitívan hat az egyén személyes biztonságára, különösen akkor, ha az egyes szereplők egy kölcsönös előnyökön alapuló kommunikációt folytatnak egymással.

Az egyéni szinten értelmezett biztonság szociológiai megközelítésénél célszerűnek tartom bemutatni, hogy az egyén születésétől haláláig tartó (biztonság)szocializációjában milyen csoportok játszanak szerepet. Egy lehetséges felosztás szerint létezik elsődleges és másodlagos csoport [32] [33] illetve aspirációs és aszociális csoport [32], formális és informális csoport [34], illetve nyílt és zárt (szélsőséges esetben karcerszervezet [35]) csoport. Az elsődleges csoport (informális csoport) az, amelyiknél az egyének közötti kölcsönhatások, interakciók folyamatosak. Ide sorolhatóak a család, a barátok, a szomszédok (nagyvárosi kultúrában rendszerint nem jellemző) és a közvetlen munkatársak. Az interakciók folyamatossága – ha annak célja a párbeszéd és a kapcsolatok ápolása – azt eredményezheti, hogy leginkább ezek azok a csoportok, illetve ennek tagjai azok, amelyek a csoportok közül a legnagyobb hatást tudják gyakorolni az egyénre, alakítják értékrendjét, formálják kultúráját, így biztonságtudatosságát is. A család, mint a gyermeki szocializáció első terepe alapvetően meghatározza az egyén alap biztonsági beállítódását, s későbbi személyiségét is. Csányi [36 p. 147] így ír erről: „A baba számára az ismeretlen világban az anya az egyetlen biztonságos pont, ha ezt elveszti, ősi félelmek keletkeznek benne, hogy ő maga is elveszik". Majd így folytatja: „Az a gyermek, aki az első három évében megtanulta a biztonságot, aki tudja, hogy ha szükséges, ha hívja, akkor az anya mindig jön, az idegen környezetben is vállalkozik felderítő utakra, szívesen keres kapcsolatot másokkal, mert nem fél örökösen attól, hogy elveszik". A másodlagos csoportok formálisabbak, a kommunikáció formalizált módon (séma) történhet, kevesebb egyénieskedést enged meg. Ide tartozhatnak a vallási, munkahelyi, iskolai, szakszervezeti csoportok, illetve a szakmai szövetségek. Ezeknél a csoportoknál az egyén a saját, illetve a csoport biztonságos élete/működése érdekében a biztonsággal kapcsolatban parancsolatokat kap (egyház: tízparancsolat, mely betartása a túlvilági élet záloga lehet), utasításokat ismer meg, s ezekről jobb esetben számot is ad (pl.: munkahelyi információbiztonsági szabályzat, majd vizsga), házirendet fogad el (mely szabályozza az iskolai viselkedési szabályokat), etikai szabályzat szerint viselkedik (pl.: a szakmai szervezet etikai szabályzata szerint nem kelti rossz hírét a konkurensnek, s így a szervezet tagjai biztonságban érezhetik jó hírnevüket). A másodlagos csoportoknál is megfigyelhetőek olyan személyek (véleményvezérek), akikre az egyén jobban hallgat, illetve ki-

alakulhatnak baráti kapcsolatok, de akkor azok már nem a formalizált kommunikáció szabályait fogják követni. Ezek a csoportok – állítja Kotler [32] – mint referenciacsoportok az egyént újfajta magatartás és életmód felvételére késztetik, hatnak egyéni viselkedésére és énképére. Vannak olyan csoportok, amelyeken az egyén kívül helyezkedik el. Ezekhez tartozni szeretne (aspirációs csoport), mert a csoporthoz tartozás a számára előnyöket, elismerést, presztízst, stb. jelent. A csoportnak rendszerint kialakult értékrendje van, mely jelentősen befolyásolja az egyén biztonságattitűdjét. Ez egyaránt lehet negatív és pozitív. Negatív, amikor a „beavatási szertartás" részeként az egyénnek (élet)veszélyes feladatokat kell végrehajtania, vagyis ahhoz, hogy a csoporttagságból fakadó előnyöket (így a csoporthoz tartozás biztonságát) élvezze, először ki kell lépnie saját biztonsági komfortzónájából. S lehet pozitív, amikor az „elitklub" csak olyan tagokat fogad be, akik például egy adott tudományterületen kimagasló ismeretekkel rendelkeznek, s ezáltal a csoport elismertsége is növekszik (pl.: MTA). A csoport/szervezet az egyén biztonságérzetét növeli, de az egyén is növeli a csoport biztonságérzetét azzal, hogy erősíti azt. Külön belső szabályok szerint működnek a karcer-, vagy kvázikarcer-szervezetek, mint a börtönök, a bentlakásos iskolák, az elmegyógyintézetek, vagy a katonaság. Ezeknél a szervezeteknél a szervezeti működést törvényi, rendeleti, tehát hatalmi utasítással tartják fenn, de magán a szervezeten belül is kialakulnak az íratlan szabályok. Az egyénnek kettős játékstratégiát kell folytatnia, ha egy látszólagos biztonságos életet akar magának megteremteni: egyfelől meg kell felelnie az elöljárók, felügyelők által betartatott szabályoknak, másfelől a csoporton belüli normáknak is.

ÖSSZEFOGLALÁS

Tanulmányom első részében részletesen foglalkoztam a biztonság megjelenésével a humán tudományokban, különösen az etológia, az evolúciós biológia és szociológia területén. A biztonság fogalmát állatok és emberek viselkedésének kontextusában vizsgáltam, kiemelve, hogy az ösztönös és tanult viselkedésminták milyen mértékben összpontosultak a biztonságra, ezzel biztosítva a fajok túlélését. Az állatok társas viselkedését és az emberek közötti társadalmi együttműködés formáit összehasonlítva rávilágítottam a biztonság központi szerepére a társadalmi struktúrák és intézmények kialakulásában. Elemeztem a modern társadalmak adaptációs stratégiáit a változó biztonsági kihívásokhoz, amelyek között szerepelt a politikai döntéshozatal, a jogi szabályozások fejlődése, és a közösségi normák átalakulása. A tanulmányomban arra is kitértem, hogy a médiának és a szórakoztatóiparnak milyen szerepe volt a biztonságérzet alakításában, kritikusan megközelítve a hamis biztonságérzet veszélyeit és annak társadalmi következményeit.

FELHASZNÁLT IRODALOM

[1] TINBERGER, N.: *Animal behavior*. New York: Time Inc, 1965.
[2] TINBERGEN, N.: *The Study of Instinct*. Oxford: Oxford University Press, 1951.
[3] LORENZ, K.: *King Solomon's Ring*. London: Methuen Publishing, 1952.
[4] HINDE, R. A.: *Animal Behavior: A Synthesis of Ethology and Comparative Psychology*. New York: McGraw-Hill Book Company, 1970.
[5] BEKOFF, M.: *The Emotional Lives of Animals: A Leading Scientist Explores Animal Joy, Sorrow, and Empathy - and Why They Matter*. Novato: New World Library, 2007.

[6] MEAD, G. H.: *Mind, Self, and Society*. Chicago: University of Chicago Press, 2015.
[7] ARONSON, E.: *A társas lény*. Budapest: Akadémiai Kiadó, 2008.
[8] WILSON, E. O.: *The Social Conquest of Earth*. New York: Liveright, 2013.
[9] WAAL, F. d.: *The Age of Empathy: Nature's Lessons for a Kinder Society*. New York: Crown, 2010
[10] WAAL, F. d.: *Our Inner Ape: A Leading Primatologist Explains Why We Are Who We Are*. Stanford: Granta Books, 2006.
[11] CSÁNYI V.: *Az emberi viselkedés*. Budapest: Sanoma Kiadó, 2007.
[12] BALCOMBE, J.: *Pleasurable Kingdom: Animals and the Nature of Feeling Good*. London: St. Martin's Griffin, 2007.
[13] BEKOFF, M.: *The Emotional Lives of Animals: A Leading Scientist Explores Animal Joy, Sorrow, and Empathy – and Why They Matter*. Novato: New World Library, 2008.
[14] CHENEY, D. L. – SEYFARTH, R. M.: *How Monkeys See the World: Inside the Mind of Another Species*. Chicago: University of Chicago Press, 1992.
[15] ABBAS, M. B.: *Fear, Panic, and Anxiety: A Comparative Review of the Behavioural Responses of Animals and Humans to Threats*. Newcastle upon Tyne: Cambridge Scholars Publishing, 2015.
[16] MEALEY, L.: *The Biology of Peace and War: Men, Women, and the Genesis of Conflict.* Mahwah: Lawrence Erlbaum Associates, Inc, 1997.
[17] FOUCAULT, M.: *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books, 2012.
[18] CZENCZER O. – RUZSONYI P (szerk.), *Büntetés-végrehajtási reintegrációs ismeretek*. Budapest: Dialog Campus, 2019.
[19] BECK, U.: Risk Society: *Towards a New Modernity*. London: SAGE Publications, 1992.
[20] BAUMAN, Z.: *Modernity and the Holocaust*. New York: Cornell Uniersity Press, 2002.
[21] HORKHEIMER, M. – ADORNO, T. W.: *Dialektik der Aufklärung*. Amsterdam: Querido Verlag, 1947.
[22] TILLY, C.: *Social Movements 1768-2018*. New York: Routledge, 2020.
[23] DURKHEIM, E.: *The Division of Labor in Society*. London: Free Press, 2014.
[24] GLASSNER, B.: *The Culture of Fear*. New York: Basic Books, 2018.
[25] MOFFETT, M. W.: *The Human Swarm: How Our Societies Rise, Thrive and Fall*. New York: Basic Books, 2019.
[26] HINTON, S.E.: *The Outsiders*. New York: Penguin Group, 2006.
[27] MCINERNEY, J.: *Bright Lights, Big City*. New York: Vintage Books, 1984.
[28] ORWELL, G.: *1984*. London: Secker and Warburg, 1949
[29] KOLLÁR Cs.: Kína és a társadalmi kredit rendszere. *HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA* 30: 2, 2020. pp. 79-97.
[30] KOLLÁR Cs.: Kína és a társadalmi kredit rendszerének információbiztonsági kérdései. *BIZTONSÁGTUDOMÁNYI SZEMLE 2: 2*, 2020. pp. 93-109.
[31] KOLLÁR Cs.: A mesterséges intelligencia társadalmi léptékű működése, a társadalmi kredit rendszere (nem csak) Kínában. In: HORVÁTH R. – BEKE É. – STADLER R. G. (szerk.) *Mérnöki Szimpózium a Bánkin előadásai: Proceedings of the Engineering Symposium at Bánki (ESB 2019)* Budapest: Óbudai Egyetem, 2019. 94 p. pp. 67-72.

[32] KOTLER, P.: *Marketing menedzsment*. Budapest: Műszaki Könyvkiadó, 1999.
[33] GIDDENS, A.: *Szociológia*. Budapest: Osiris Kiadó, 1997.
[34] SZABÓ I.: *Bevezetés a szociálpszichológiába*. Budapest: Nemzeti Tankönyvkiadó, 1998.
[35] GOFFMAN, E.: *Asylums: Essays on the Social Situtation of Mental Patients and Other Inmates*. Harmondsworth: Penguin, 1961.
[36] Csányi V.: *Van ott valaki? Válogatott írások*. Budapest: Typotex Kiadó, 2000.

DESIGNING SMART HOMES FOR ASSISTED LIVING: UNDERSTANDING ELDERLY CUSTOMER NEEDS

GONDOSKODÓ OKOSOTTHONOK TERVEZÉSE: AZ IDŐSEK FOGYASZTÓI IGÉNYEINEK MEGÉRTÉSE

ZS. SZABÓ Kitti[1] – ZSÁK Péter[2]

Abstract

As the population ages, there is a growing interest in leveraging smart home technology to provide care and support for elderly individuals. However, the effectiveness of these solutions hinges on a thorough understanding of customer needs. This article explores the importance of analyzing customer needs before establishing a smart home for assisted living for the elderly. It delves into the unique challenges faced by seniors, including physical limitations, cognitive decline, and emotional well-being, and outlines methods for gathering insights, such as surveys and interviews. Key considerations in analyzing customer needs, including safety, comfort, and independence, are discussed, along with the role of technology in addressing these needs. By prioritizing the understanding of customer ne eds, smart home designers and installers can create compassionate and effective smart home environments that enhance the quality of life for elderly.

Keywords

Assisted living, smart home, domotics, elderly, designing

Absztrakt

A népesség öregedésével egyre nagyobb az érdeklődés az okosotthon technológia kihasználása iránt, hogy az idősek számára gondozást és támogatást nyújtson. E megoldások hatékonysága azonban az ügyfelek igényeinek alapos ismeretén múlik. Ebben a cikkben azt vizsgáljuk, hogy mennyire fontos az ügyfelek igényeinek elemzése, mielőtt az idősek számára gondoskodó okosotthont hoznánk létre. Bemutatjuk az időskor egyedi kihívásait, beleértve a fizikai korlátozottságot, a kognitív problémákat és az érzelmi jóllétet, és felvázoljuk azokat a módszereket, amelyekkel a szükséges információk összegyűjthetőek (például felmérések, interjúk). Az ügyfelek igényeinek - többek között a biztonság, a kényelem és a függetlenség - elemzése során felmerülő legfontosabb szempontokat, valamint a technológia szerepét tárgyaljuk az igények kielégítésében. A vásárlói igények megértésének előtérbe helyezésével az okosotthonok tervezői és telepítői együttérző és hatékony okosotthoni környezetet hozhatnak létre, amelyek javítják az idősek életminőségét.

Kulcsszavak

Gondoskodó okosotthon, domotika, idősek, tervezés

[1]Kitti.szabo@smartopert.com | ORCID: 0009-0002-8348-4217 | COO/CEO, Smartopert Kft. | operatív/ügyvezető, Smartopert Kft.

[2] Peter.zsak@smartopert.com | ORCID: 0009-0000-4256-4910 | CTO/CEO, Smartopert Kft. | technológiai/ügyvezető, Smartopert Kft.

INTRODUCTION

With advancements in technology, the concept of smart homes has transformed from a luxury to a necessity, particularly in the context of caring for the elderly. By the aging of populations there is a pressing need for innovative solutions that enable seniors to maintain independence and quality of life in their own homes. Smart home technology offers promising opportunities to address these needs, providing assistance, security, and convenience tailored to the unique challenges faced by elderly individuals.

However, the success of these smart home solutions hinges not only on the sophistication of the technology but also on a deep understanding of the customers they serve. Before establishing a smart home for assisted living for the elderly, it is imperative to analyze and comprehend their specific needs, preferences, and limitations. This foundational step is crucial for designing solutions that are not only technologically advanced but also empathetic and human-centered.

In this article, we delve into the importance of analyzing customer needs in the context of establishing smart homes for the elderly. We explore the multifaceted challenges faced by seniors, ranging from physical impairments to cognitive decline and emotional well-being. Additionally, we discuss various methods for gathering insights into customer needs, including surveys, interviews, and collaboration with healthcare professionals.

By prioritizing a customer-centric approach, designers, caregivers, and technologists can ensure that smart home solutions for the elderly are not just functional but also compassionate and empowering. Understanding customer needs lays the groundwork for creating transformative and inclusive smart home environments for the aging population.

UNDERSTANDING THE UNIQUE NEEDS OF ELDERLY CUSTOMERS

Understanding the unique needs of elderly customers is essential for designing smart home solutions that cater to their specific challenges and enhance their quality of life. By addressing physical limitations, cognitive challenges, and emotional well-being, smart homes can empower elderly individuals to age in place safely, comfortably, and with dignity. The population of both the European Union and Hungary is rapidly aging. In Hungary, in 2022, 20.3% of the population was 65 years or older, and according to projections, this proportion may reach 30% by 2050. [1]

Physical Limitations

Mobility issues: Mobility limitations are common among elderly individuals, affecting their ability to move around freely and perform daily activities. Conditions such as arthritis, Parkinson's disease, and stroke can significantly impair mobility, making tasks like walking, standing, and reaching challenging. Nearly a quarter of the elderly population is affected by some form of joint-related musculoskeletal disorder, which is one of the leading causes of disability in this age group. Osteoporosis affects one-fifth of those aged 65 or older. 20-30% of the elderly suffer injuries that reduce mobility and independence as a result of falls. Understanding the extent of mobility issues is crucial for designing smart home solutions that enhance accessibility and promote independence. [1]

Vision and Hearing Impairments: Age-related changes in vision and hearing can pose significant obstacles for seniors. Alterations in our visual abilities during later stages of adulthood may affect our capacity to execute routine visual tasks like object recognition,

reading, participating in mobility-related activities, and driving, consequently influencing our life quality and well-being. Reduced visual acuity and hearing loss can affect communication, navigation, and safety within the home environment. Smart home technologies must accommodate these impairments by offering features such as voice-activated controls, adjustable font sizes, and visual alerts to ensure that elderly individuals can interact with their surroundings effectively.[2]

Chronic Health Conditions: Many elderly people have chronic health conditions such as diabetes, hypertension, and heart disease. In Hungary, 72% of the population aged 65 or older is overweight or obese, while 76% suffer from some form of chronic illness. These conditions may require regular monitoring, medication management, and lifestyle modifications. Smart home solutions can play a vital role in supporting seniors' health by integrating medical devices, reminders for medication adherence, and remote monitoring capabilities to keep caregivers and healthcare providers informed about any changes in health status. [1]

Cognitive Challenges

Memory Loss: Cognitive decline, including memory loss and confusion, is a common aspect of aging, particularly among individuals with conditions like Alzheimer's disease and dementia. Memory loss can impact daily routines, medication adherence, and safety within the home. Smart home technologies can assist elderly individuals by providing reminders for important tasks, organizing schedules, and implementing location-tracking features to prevent wandering and ensure their safety.[3]

Decision-making Abilities: Declines in cognitive function can also affect elderly individuals' decision-making abilities, leading to difficulties in problem-solving and planning. Smart home solutions should be designed with simplicity and ease of use in mind, minimizing cognitive load and reducing the need for complex decision-making. Clear interfaces, intuitive controls, and automation features can help seniors navigate their environment more effectively and maintain a sense of autonomy.

Emotional Well-being

Loneliness and Social Isolation: The elderly population of Hungary is exposed to an increasing risk of psychological, social, economic, and biomedical problems related to aging due to 'unsuccessful' aging. Many elderly individuals experience feelings of loneliness and social isolation, especially if they live alone or have limited social interactions. Smart home technologies can bridge the gap by facilitating communication with family members, friends, and caregivers through video calls, messaging platforms, and social networking features. Virtual companionship and social engagement can mitigate feelings of loneliness and improve overall emotional well-being.[1]

Mental Health Concerns: Mental health issues such as depression and anxiety are prevalent among elderly individuals but often go unnoticed or untreated. Smart home solutions can incorporate mood-tracking tools, relaxation techniques, and access to mental health resources to support seniors' emotional health. Additionally, sensors and monitoring devices can detect changes in behavior or activity patterns that may indicate underlying mental health issues, enabling timely intervention and support.[3]

INCORPORATING TECHNOLOGY TO ADDRESS CUSTOMER NEEDS

Smart Home Devices and Systems

Smart home technology offers a wide range of assistive devices and systems designed to address the specific needs of elderly individuals. Examples include:

- Smart sensors: These devices can monitor movement, detect falls, and track activity levels to provide real-time insights into the well-being of elderly residents.
- Voice-activated assistants: Virtual assistants like Amazon Alexa and Google Assistant enable hands-free control of smart home devices, making it easier for elderly individuals to interact with their environment.
- Remote monitoring systems: These systems allow caregivers and healthcare providers to remotely monitor vital signs, medication adherence, and overall health status, providing peace of mind and timely intervention when needed.
- Smart home security cameras: These cameras offer enhanced security and monitoring capabilities, allowing elderly individuals and their caregivers to keep an eye on their home environment and detect any unusual activity or potential risks. [4, 5]

When incorporating technology into smart home solutions for elderly customers, it's essential to consider integration with existing infrastructure. This includes compatibility with existing devices, systems, and protocols to ensure seamless operation and minimal disruption to the home environment. By leveraging interoperability standards such as Zigbee, Z-Wave, or Wi-Fi, smart home installers can integrate new devices and systems with ease, enabling comprehensive monitoring, control, and automation capabilities throughout the home. [4]

Customization and Personalization

Customization is the key element of smart home planning. It is even more critical in case of elderly due to the potential special needs.

Tailoring Solutions to Individual Preferences: Every elderly individual has unique needs, preferences, and lifestyle habits that must be taken into account when designing smart home solutions. Installers should prioritize customization and personalization to tailor solutions to the specific requirements of each customer. This may involve conducting thorough assessments, gathering input from elderly individuals and their caregivers, and configuring smart home devices and systems to meet their individual preferences and routines. By tailoring solutions to individual needs, installers can ensure that smart home technology enhances comfort, convenience, and overall quality of life for elderly customers.

Flexibility to Adapt to Changing Needs: As the needs of elderly individuals evolve over time, smart home solutions must be flexible and adaptable to accommodate changing circumstances. Installers should design solutions with scalability and future-proofing in mind, allowing for easy expansion, upgrades, and modifications as needed. This may involve selecting modular devices and systems that can be easily reconfigured or integrated with new technologies in the future. By providing flexibility and scalability, smart home solutions can continue to meet the evolving needs of elderly individuals, supporting aging in place with confidence and peace of mind.

Incorporating technology into smart home solutions for elderly customers offers immense potential to address their specific needs and enhance their quality of life. By leveraging assistive technologies, integrating with existing infrastructure, and prioritizing customization and personalization, smart home installers can create tailored solutions that empower elderly individuals to age in place comfortably, safely, and independently. [6,7]

METHODS FOR ANALYZING CUSTOMER NEEDS FOR SMART HOME DESIGNERS AND INSTALLERS

Surveys and Interviews

Designing Questions to Gather Insights: Surveys are valuable tools for collecting data about the needs, preferences, and challenges of elderly individuals and their caregivers. When designing survey questions, it's essential to craft inquiries that elicit specific and actionable responses. Questions should cover a range of topics, including daily activities, quality life, health concerns, technology usage, and desired features for a smart home environment. By structuring surveys effectively, smart home installers can gain a comprehensive understanding of customer needs and preferences, guiding the development of tailored solutions.

Conducting Interviews with Seniors and Caregivers: In addition to surveys, interviews provide an opportunity for in-depth exploration of customer needs and insights. Conducting one-on-one or group interviews with seniors and their caregivers allows installers to delve deeper into individual experiences, challenges, and preferences. Open-ended questions can uncover valuable insights that may not emerge through structured surveys alone. By actively listening to customers' perspectives and concerns, smart home installers can refine their understanding of customer needs and ensure that solutions are aligned with their expectations.

Observation

Observing Daily Routines and Challenges: Observation is a powerful method for gaining firsthand insight into the daily lives of elderly individuals within their home environments. By spending time observing seniors as they go about their routines, smart home installers can identify pain points, inefficiencies, and areas for improvement. This approach allows installers to understand how elderly individuals interact with their surroundings, where they encounter difficulties, and how technology can be integrated to enhance their quality of life.

Identifying Pain Points and Areas for Improvement: Through observation, installers can pinpoint specific pain points and challenges that elderly individuals face in their homes. This may include difficulties with mobility, communication, medication management, or home safety. By identifying these areas for improvement, installers can tailor smart home solutions to address the unique needs of each customer. Whether it's installing grab bars in the bathroom, implementing voice-activated controls for lighting and appliances, or integrating fall detection sensors, observation enables installers to design solutions that effectively support elderly individuals in their daily lives.

Collaboration with Healthcare Professionals

Consulting Geriatricians, Occupational Therapists, etc.: Collaboration with healthcare professionals, such as geriatricians, occupational therapists, and home healthcare providers, provides valuable expertise and insights into the specific needs of elderly individuals. These professionals can offer clinical perspectives on mobility limitations, cognitive impairments, and chronic health conditions that may impact daily functioning and safety within the home. By consulting with healthcare experts, smart home installers can gain a deeper understanding of the medical and functional needs of their customers, informing the design and implementation of customized solutions.

Integrating Medical Insights into Smart Home Solutions: By integrating medical insights into smart home solutions, installers can create holistic and personalized environments that support the health and well-being of elderly individuals. This may involve incorporating medical devices for monitoring vital signs, medication adherence reminders, or remote monitoring capabilities for early detection of health issues. By leveraging healthcare expertise, smart home installers can ensure that their solutions not only enhance convenience and comfort but also contribute to improved health outcomes and peace of mind for both seniors and their caregivers.

While smart home installers may have limited resources and capabilities compared to healthcare professionals, leveraging methods such as surveys and interviews can still yield valuable insights into customer needs and preferences. By focusing on customer-centric approaches and actively engaging with elderly individuals and their caregivers, installers can develop smart home for assisted living solutions that enhance independence, safety, and quality of life for seniors aging in place. In this article we are focusing on the surveys and interview questions that can be easily used by smart home installers.

KEY CONSIDERATIONS IN ANALYZING CUSTOMER NEEDS

In analyzing customer needs for smart home solutions, installers must consider key factors such as safety, comfort, convenience, independence, and autonomy. By prioritizing these considerations and designing solutions that address the specific needs and preferences of elderly individuals, installers can create caring and compassionate environments that support aging in place with dignity and peace of mind.

Safety and Security

Assessing Risks and Vulnerabilities: Safety is paramount when designing smart home solutions for elderly individuals. Installers must conduct thorough assessments to identify potential risks and vulnerabilities within the home environment. This includes evaluating factors such as fall hazards, fire risks, and security vulnerabilities. By identifying areas of concern, installers can prioritize safety features and implement measures to mitigate risks, ensuring a secure living environment for elderly customers.

Implementing Measures for Emergency Situations: In addition to proactive safety measures, smart home solutions should include provisions for responding to emergency situations effectively. This may involve integrating features such as emergency call systems, smoke and carbon monoxide detectors, and automated alerts for caregivers or emergency services. By implementing measures for emergency situations, installers can provide peace

of mind to elderly individuals and their caregivers, knowing that help is readily available when needed.

Comfort and Convenience

Enhancing Accessibility and Usability: Smart home solutions should be designed with accessibility and usability in mind to accommodate the diverse needs of elderly individuals. This includes features such as voice-activated controls, adjustable lighting and thermostat settings, and intuitive interfaces that are easy to navigate. By enhancing accessibility and usability, installers can ensure that smart home technology is inclusive and user-friendly for elderly customers, regardless of their level of technological proficiency.

Minimizing Physical Exertion and Stress: Aging can take a toll on physical health and energy levels, making tasks that were once simple more challenging. Smart home solutions should aim to minimize physical exertion and stress by automating routine tasks and reducing the need for manual intervention. This may include features such as automated lighting and climate control, smart appliances with remote operation capabilities, and robotic assistance for tasks like cleaning and maintenance. By reducing the physical demands on elderly individuals, smart home technology can enhance comfort and quality of life.

Independence and Autonomy

Empowering Seniors to Maintain Control: Maintaining independence and autonomy is essential for preserving the dignity and well-being of elderly individuals. Smart home solutions should empower seniors to maintain control over their living environment and daily routines. This may involve features such as customizable settings, personalization options, and decision-making autonomy. By giving elderly individuals agency and control, installers can foster a sense of empowerment and self-sufficiency, promoting independence and confidence in their ability to age in place.

Balancing Assistance with Preserving Dignity: While assistance is necessary for supporting elderly individuals in their daily activities, it's essential to strike a balance that preserves their dignity and autonomy. Smart home solutions should offer assistance discreetly and respectfully, without undermining the individual's sense of independence. This may involve integrating assistive technologies that blend seamlessly into the home environment, as well as providing options for privacy and personal space. By respecting the dignity of elderly customers, installers can ensure that smart home solutions enhance their quality of life while preserving their sense of identity and self-worth.

Table 1 contains a list of questions we would suggest to guide conversations with customers. It is an additional list that can be used by the smart home experts, it cannot replace the general analysis of smart home needs of the customer. By asking these questions and actively listening to the client's responses, smart home designers and installers can gain valuable insight into their unique needs and preferences, allowing to tailor the smart home solution to meet the specific requirements for safety, comfort, and care.

Health and Mobility:	**Communication and Social Connectivity:**
Do you or your loved one have any medical conditions or mobility challenges that need to be addressed in the design of the smart home?	How do you prefer to communicate with family members, friends, or caregivers?
Are there any specific health monitoring needs, such as medication reminders, vital sign tracking, or fall detection?	Are there any concerns about social isolation or loneliness that you would like to address through the smart home technology?
Do you require assistance with activities of daily living, such as bathing, dressing, or meal preparation?	Would you be interested in features like video calling or social media integration to stay connected with loved ones?
Safety and Security:	**Comfort and Convenience:**
What safety concerns do you have regarding your current living environment?	What comfort features would enhance your daily life and overall well-being?
Are there any particular security features you would like to incorporate into the smart home system, such as surveillance cameras, smart locks, or alarm systems?	Are there any preferences regarding lighting, temperature, or environmental controls within the home?
Do you have any pets or concerns about their safety within the home?	Do you have any specific preferences for entertainment options, such as music or television?
Daily Routine and Lifestyle:	**Future Planning:**
Can you describe your typical daily routine and any challenges you encounter?	Are there any anticipated changes in your living situation or care needs that should be considered in the design of the smart home?
Are there any specific tasks or activities that you find difficult to perform independently?	How do you envision your needs evolving over time, and how can the smart home system adapt to accommodate these changes?
What leisure activities or hobbies do you enjoy, and how can the smart home system support these interests?	Are there any long-term goals or aspirations for aging in place that you would like to incorporate into the smart home design?

Table 1: Proposed questions specific to guide conversations with customers to design smart home for the eldery

CONCLUSION

Throughout this study, we have delved into the intricate landscape of smart home solutions for the elderly, emphasizing the paramount importance of understanding and analyzing customer needs. We have seen how these needs encompass not only the functional

aspects of technology but also the emotional and psychological requirements of the elderly population. By comprehensively examining their needs, preferences, and challenges, we lay the foundation for developing truly impactful and user-centric solutions.

When gathering information from a client to understand their needs for a smart home for assisted living, it's essential to ask questions that delve into various aspects of their lifestyle, health status, preferences, and concerns. As a result of our work we created a questionnaire dedicated to smart home for assisted living for elderly that smart home designers and installers can use to truly understand the need of their customers.

In conclusion, by prioritizing the analysis of customer needs and embracing a compassionate approach to design, we can pave the way for a future where smart home solutions truly enrich the lives of the elderly, fostering independence, dignity, and meaningful connections.

LITERATURE

[1] Szarvas Zs., Ungvári Z.: Életmód és életmód-intervenció az orvosi gyakorlatban. In: Megelőző orvostan és népegészségtan. (Szerk.: Ádány et. al.,) Budapest: Medicina Könyvkiadó Zrt, 2023 page: 616-622

[2] Owsley, C. (2016). Vision and Aging. Annual Review of Vision Science, 2, 255-271.

[3] Kiss I.: A nem fertőző betegségek epidemiológiája. Megelőző orvostan és népegészségtan. (Szerk.: Ádány et al.) Budapest: Medicina Könyvkiadó Zrt, 2023 page:227-246

[4] Zsák P.: Otthonautomatizálás kézikönyve. Szeged: Smartopert Kft, 2021

[5] Zs. Szabó K., Zsák P.: Útikalauz okosotthon felhasználóknak. Szeged: Smartopert Kft, 2024

[6] Zsák P. – Zs. Szabó K.: Okosotthon Guru® Okosotthon telepítő képzés. Szeged: Smartopert Kft, 2024

[7] Zsák P. – Zs. Szabó K.: Domotika rendszer tervezése. In: Domotika 2 (Szerk.: Kollár Cs. Et al.) Kolozsvár: Koinónia 2024 page: 209-240

RISK ASSESSMENT, EVALUATION AND MANAGEMENT IN LOW LEVEL LASER THERAPY (LLLT)

KOCKÁZATOK FELMÉRÉSE, ÉRTÉKELÉSE ÉS KEZELÉSE A LÁGYLÉZER TERÁPIÁBAN

MORVAY László[1] – SZŰCS Endre[2]

Abstract

In the case of any activity using an ionizing radiation source, the protection and safety of workers must be optimized in order to keep the magnitude of individual doses, the number of persons exposed to radiation, and the probability of radiation exposure at the lowest reasonably achievable level. In addition to scientific and technical features, economic and social factors must also be taken into account during optimization. Occupational radiation exposure shall be considered any radiation exposure that the employee may receive during his or her work. Our study explores the risks of the therapy through a specific laser class 4 low-level laser therapy (LLLT) device, and deals in detail with the dangers that arise during the treatments and the risks arising from them. After explaining the basic parameters of low-level laser therapy, it presents the process of risk assessment and risk management step by step, which provides guidelines for institutions dealing with low level laser therapy to compile their own risk management documentation.

Keywords:

soft laser therapy, LLLT, dangers, risks, risk assessment, risk management

Absztrakt

Bármely ionizáló sugárforrást alkalmazó tevékenység esetében a munkavállalók védelmét és biztonságát optimalizálni kell annak érdekében, hogy az egyéni dózisok nagysága, a sugárzásnak kitett személyek száma és a sugárterhelés valószínűsége az észszerűen elérhető legalacsonyabb szinten maradjon. Az optimalizáláskor tekintettel kell lenni a tudományos és technikai adottságok mellett a gazdasági és társadalmi tényezőkre is. Foglalkozási sugárterhelésnek kell tekinteni bármilyen olyan sugárterhelést, amelyet a munkavállaló a munkavégzése során kaphat. Tanulmányunk egy konkrét 4. lézerosztályú lágylézer terápiás készüléken keresztül tárja fel a lágylézer terápia kockázatait, részletesen foglalkozik a kezelések során felmerülő veszélyekkel és az azokból fakadó kockázatokkal. A lágylézer terápia alapvető paramétereinek ismertetése után lépésről-lépésre mutatja be a kockázatértékelés és kockázatkezelés folyamatát, amely útmutatást ad a lágylézer terápiával foglalkozó intézményeknek a saját kockázatkezelési dokumentációjuk összeállításához.

Kulcsszavak:

lágylézer terápia, LLLT, veszélyek, kockázatok, kockázatértékelés, kockázatkezelés

[1] morvay.laszlo@phd.uni-obuda.hu | ORCID: 0009-0004-2064-8856 | doctoral student, Óbudai University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] szucs.endre@bgk.uni-obuda.hu | ORCID: 0000-0003-2818-262X |senior lecturer, Óbudai University Doctoral School on Safety and Security Sciences |egyetemi oktató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A lézersugár és annak felhasználásával működő lézerberendezések széles köre a 20. század egyik legjelentősebb felfedezése. A lézersugár megvalósításának alapjait az elektromágneses indukció leírása (Michael Faraday 1831), a kvantumelmélet (Max Planck 1900) és a fénykvantumelmélet (Albert Einstein 1905) kidolgozása teremtette meg. Az áttörést Ernest Rutherford atomelmélete (1911), majd Albert Einstein indukált emisszióra vonatkozó felfedezése (1917) hozta meg. A kísérleti feltételek és a még hiányzó technológiák miatt az első működő lézersugarat 1960-ban készítette el Theodore Maiman. Magyarországon a Központi Fizikai Kutató Intézetben Jánossy Lajos vezetésével, Bakos József, Csillag László, Kántor Károly és Varga Péter közreműködésével 1963-ban született meg az első hazai lézerberendezés, amely egy He-Ne gáz-lézerforrás volt. [1]

LÉZEREK ALKALMAZÁSI TERÜLETEI

A lézersugár is fény. Fotonok alkotják, ezért anyag, ennél fogva egy másik anyaggal találkozva egyidejűleg három esemény lép fel: visszaverődés (reflexió), áthaladás (transzmisszió) és elnyelődés (abszorpció). Teljes értékű, 100%-os fényteljesítmény nem létezik, ami a gyakorlatban azt jelenti, hogy a kölcsönhatás során mindhárom jelenség egyszerre valósul meg. Az, hogy melyikről beszélünk, az egyes jelenségek teljesítményarányai alapján dől el. A lézersugár alkalmazási lehetőségeit is ez a három jelenség határozza meg. [2]

Három fő alkalmazási területe az ipar, a haditechnika és a gyógyászat. Az ipar területén a visszaverődés jelenségét használjuk ki a lézermutatók, lézeres szintezők, a lézermutatós daraboló gépek, a lézeres térképészeti távolságmérők, a rendőrségi traffipaxok, valamint a CD-, DVD-olvasók esetében. Az áthaladást elsősorban a telekommunikáció területén hasznosítjuk, ahol a lézersugár segítségével üvegszálban, megfelelő erősítőeszközök közbeiktatásával az információ gyakorlatilag tetszőleges távolságra juttatható el. Az elnyelődés jelenségével pedig a lézernyomtatók, a fénymásolók, a CD-, DVD-írók, a félvezetőgyártás, a forgácsolás, a hegesztés, a gravírozás és a nanotechnológia terén találkozunk. [2]

A haditechnikai alkalmazását tekintve a lézersugár, illetve a lézerberendezések az alábbi célokat szolgálják:

- felderítés, távolságmérés, célmegjelölés;
- lézeres önirányítás (aktív és félaktív);
- vakítás, rongálás, megsemmisítés [3]

A lézersugár 1960-as években történő megjelenése egybeesett a 20. század második felére jellemző egészségügyi, szociális, tudományos és technikai fejlődéssel. A lézersugárra jellemző kis divergencia (kollimáció), a kis spektrális sávszélesség (monokromaticitás), a nagy spektrális energiasűrűség, a nagy teljesítmény, az extrém rövid impulzusok lehetősége (ps, fs), a polarizáció, a térbeli és időbeli koherencia kiválóan alkalmassá teszi a diagnosztikában és a terápiában történő alkalmazására. A legfontosabb alkalmazási területei a medicinában a klinikai és laboratóriumi diagnosztika, a rákos szövetek célzott, szelektív elpusztítása (photodynamiás terápia), a lézersebészet és a lágylézer terápia. [4]

A fizioterápia alapvetése, hogy célzott kezelésekkel az emberi szervezet saját védekezőképességét erősítse, amivel csökkenti a fájdalomcsillapítást szolgáló gyógyszerkészítmények beviteli mennyiségét és fokozza a szervezet belső gyógyító erejét, ami betegség

esetén a harmonikus egyensúly helyrehozására és a természetes állapot mielőbbi visszaállítására törekszik. A fizioterápia a természetben előforduló energiákat (mechanikai, hő, fény, elektromágneses stb.) alkalmazza. A fizioterápián belül a lágylézer terápia a fototerápiák közé tartozik. [6]

Az elmúlt évtizedek gyors műszaki fejlődése a házilag is alkalmazható terápiás készülékeket sem kerülte el, amelyek az egyre csökkenő méretük és árszintjük miatt egyre többek számára elérhető. Öt hazai, egészségügyi terápiás készülékeket forgalmazó vállalatot vizsgálva látható, hogy az árbevételük 2018-tól az 1. ábrán látható dinamikus növekedést vagy a korábbi években elért nettó árbevétel-szint megtartását mutatja. [5]

1. ábra Terápiás készülékek hazai forgalmazóinak nettó árbevétel alakulása 2001-2022 között (szerzők saját szerkesztése [5] alapján)

A közeli infravörös tartományban működő, diagnosztikai vagy terápiás céllal alkalmazott lézersugár esetében az elnyelődés jelenségét használjuk ki. Az optikai sugárzás a vizsgált vagy kezelt testfelülettel találkozik, melynek külső rétegei elnyelik azt, ezért a lézersugár biológiai hatásai a bőr és a szem esetében jelentkeznek. Az infravörös tartományt elsősorban a hőhatás jellemzi, de a szemet érő, rövid ideig tartó, nagy intenzitású vagy kis intenzitású, de 10 másodpernél hosszabb ideig tartó lézersugár – a szemlencse fókuszáló hatása miatt - súlyos látáskárosodást okoz. [3] A háztartásokban egyre nagyobb számban jelenlévő terápiás készülékek és azok helytelen használatából fakadó egészségkárosodások miatt kiemelten fontos a lágylézer terápia kockázatainak felmérése és kezelése.

A LÁGYLÉZER KEZELÉSEK ALAPVETŐ PARAMÉTEREI

Energia és teljesítmény

Az optikai sugárzás egyfajta anyagáramlás, ezért a lágylézer kezelés során kölcsönhatásba lép az emberi bőrszövettel, amelynek állapota a kölcsönhatás következtében megváltozik (felmelegszik). A fizikai tudományok területén az állapotváltozást előidéző folyamatokat munkavégzésnek nevezzük, melynek mértékét az SI mértékegységrendszerben az

energia jellemez, mértékegysége a Joule (J). A teljesítmény pedig a munkavégzés sebessége, azaz az egységnyi idő alatt elvégzett munka, melynek mértékegysége a watt (W). A két származtatott fizikai mennyiség közötti összefüggés az alábbi képlettel írható le: [3]

$$P(t) = \frac{dE(t)}{dt}$$

A képlet minden időpillanatra megadja az energiaáramlás intenzitásának a mértékét (pillanatnyi teljesítmény függvény), azonban, ha az energia-idő függvény lineáris, akkor a teljesítmény az adott időegységhez tartozó munkavégzésre utal (lineáris időfüggvény deriváltja minden időpillanatban konstans), ezért a fenti képlet leegyszerűsödik: [3]

$$P = \frac{E}{t}$$

Mindezt a lágylézer terápia területére vetítve, ahol a munkát a fotonok végzik, a foton energiáját a foton frekvenciájának és a Planck-állandó szorzatával számítjuk ki: [7]

$$E_{foton} = h \cdot \nu$$

ahol a Planck-állandó $h = 6{,}626196 \cdot 10^{-34}$ Js, ν pedig a frekvencia.

Teljesítményűrűség és energiasűrűség

Lágylézer terápia esetén a lézerfénnyel megvilágított felület adott pontjaira időegység alatt eltérő mennyiségű foton érkezik, ami azt jelenti, hogy az egyes pontokban a teljesítmény nem lesz állandó. E jelenség leírására vezették be a teljesítménysűrűség fogalmát, ami az adott felületen eloszló teljesítmény mértékét adja meg. [3]

$$Sp = \frac{P}{A} = \frac{Lézersugár\ kimenő\ teljesítménye\ [W]}{Lézersugár\ keresztmetszete\ [cm^2]}$$

A tetszőleges időtartam alatt az egységnyi felületen áthaladó fotonok összenergiáját pedig az energiasűrűség fejezi ki [3]:

$$Se = \frac{E}{A} = \frac{Lézerenergia\ [J]}{Lézersugár\ keresztmetszete\ [cm^2]}$$

Behatolási mélység

A lágylézer terápia elsődleges célja, hogy az emberi szervezet jól meghatározott részébe lézersugár formájában fotonokat juttasson a különböző okokból sérült és/vagy rendellenesen működő sejtekbe és molekulákba, hogy azokban a koherens elektromágneses tér hatására elinduló fotokémiai és fototermális hatások felgyorsítsák a rendellenes állapot megszűnését, azaz elősegítsék a mielőbbi gyógyulást. Ez a folyamat kizárólag abszorpcióval (elnyelődéssel) érhető el. [3]

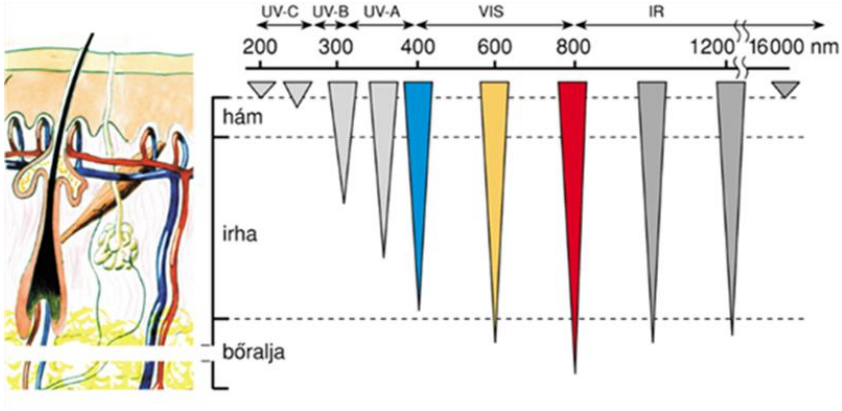
Nem feledkezhetünk el azonban a szóródás jelenségéről, amely abból fakad, hogy a testszövetbe belépő fotonok elektronokat gerjesztenek, amelyek a gerjesztett állapotból alapállapotba jutáskor újabb fotonokat bocsájtanak ki. Ezek mozgási iránya azonban a belépési felülethez viszonyítva már nem merőleges lesz, hanem véletlenszerű (spontán emisszió). A szóródás a besugárzott lézernyaláb intenzitását fokozatosan, exponenciális függvény mentén csökkenti, azaz csillapítja. Biztonságtechnikai szempontból kiemelendő, hogy míg általánosságban igaz az, hogy biológiai szövetek esetében a fény terjedését az elnyelő-

dés és a szóródás együttesen határozza meg, ez alól kivételt jelent a szem, melynek optikailag átlátszó részei (szaruhártya, szemlencse) a fényt szinte veszteség nélkül átengedik. [8]

A fényelnyelő anyagon áthaladó fény elnyelődésének mértéke a Lambert-Beer törvény szerinti abszorpciós egyenlettel írható le: [9]

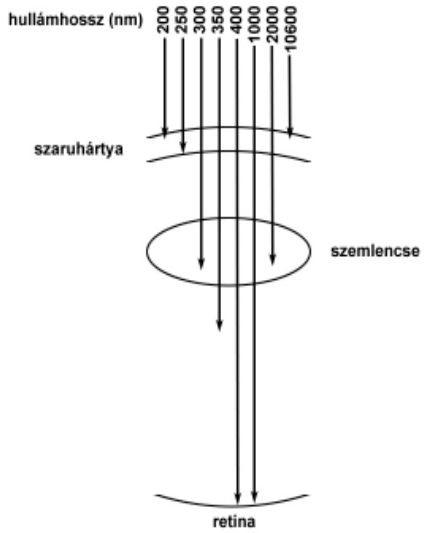
$$I = I_0 \cdot e^{-\alpha x}$$

ahol I_0 a beérkező fény intenzitása, x az anyag vastagsága, α az abszorpciós együttható.
A behatolási mélység függ a beérkező fény hullámhosszától is, melynek arányait az emberi bőr esetében a 2. ábra mutatja. [3] Látható, hogy a szövetekben a legmélyebbre a vörös és a közeli infravörös fény hatol. Fontos megjegyezni, hogy a szóródás miatt a szövetekben a fény terjedése nem nyílhegy, hanem egy felfordított tölcsér alakra hasonlít. [3]



2. ábra Fény elnyelődése a bőr rétegeiben a hullámhossz függvényében [4]

A szem esetében szintén a látható vörös és a közeli infravörös fény jut a legmélyebbre, egészen a retináig, bizonyos esetekben még azon túl is. Ezt szemlélteti a 3. ábra. [7]



3. ábra Különböző hullámhosszúságú fények behatolási mélysége a szemben [7]

Dózis

A lágylézer terápiában az emberi szövetek változatossága miatt jelenleg nincsenek egzakt értékek arra vonatkozóan, hogy mekkora energiát kell közölni az adott felületre az optimális gyógyulás eléréséhez. A dózis általános mennyiségegyenlete:

$$D = \frac{E}{A}$$

ahol E az energia, A a felület, mértékegysége a J/cm^2.

Lágylézer kezelések esetében a megfelelő dózis adagolása kiemelten fontos, ugyanis a szükségesnél kisebb dózis esetén a gyógyulás nem, vagy csak nagyon lassan indul el (alulkezelés), míg túlzott dózis esetén a páciens a kezelés okozta fájdalomtól is szenvedni fog (túlkezelés). Megállapítható, hogy a lágylézerkezelések esetében a legnagyobb kockázatot a legnagyobb behatolási mélységű (nagy teljesítményű), közeli infravörös tartományban működő berendezések jelentik.

LÁGYLÉZER TERÁPIÁS KÉSZÜLÉKEK BIZTONSÁGI OSZTÁLYOZÁSA

Az MSZ EN 60825-1:2015 szabvány a lézereket a hozzáférhető kibocsátás határértéke alapján hét osztályba sorolja. A magasabb számú osztály nagyobb kockázatot jelent a felhasználók számára. Minél magasabb osztályba tartozik egy lézer, annál magasabb szintű biztonsági óvintézkedéseket kell foganatosítani, pl. vészkapcsoló, kettős indítású készülékek, védőszemüveg, jelzőfény, a lézer felhasználási területének elkerítése, lezárása a lézer működési időtartamára stb. A szabvány 6. fejezete részletesen tárgyalja az egyes lézerosztályok leírását és a hozzájuk tartozó biztonsági intézkedéseket, amelyeket az 1. táblázat foglal össze.

		LÉZEROSZTÁLYOK						
		1	1M	2	2M	3R	3B	4
Veszélyek		ésszerű körülmények mellett biztonságos	szabad szemre biztonságos, optikai (nagyító) eszközök használata növeli a veszélyt	rövid expozíció esetén biztonságos, a szem védelméről az elkerülő reflex (pislogás) gondoskodik	szabad szemre rövid expozíció esetén biztonságos, optikai (nagyító) eszközök használata növeli a veszélyt	a sérülés kockázata alacsony, képzetlen személyre helytelen használat esetén veszélyes lehet	a lézer közvetlen szembe jutása veszélyes	a szemre és a bőrre is veszélyes + tűzveszély
Biztonsági intézkedések	Területvédelem	nem kell	lokalizált vagy zárt	nem kell	lokalizált vagy zárt	zárt	zárt + reteszelő berendezés	zárt + reteszelő berendezés
	Biztonsági kulcs	nem kell	nem kell	nem kell	nem kell	nem kell	kell	kell
	Egyéni védőeszköz	nem kell	nem kell	nem kell	nem kell	kockázatértékeléstől függően szükséges lehet	kell	kell

		LÉZEROSZTÁLYOK						
		1	1M	2	2M	3R	3B	4
Biztonsági intézkedések	Oktatás	gyártói utasítás szerint	javasolt	gyártói utasítás szerint	javasolt	kell	kell	kell
	Kockázatértékelés	nem kötelező, de lehet	nem kötelező, de lehet	nem kötelező, de lehet	nem kötelező, de lehet	kötelező	kötelező	kötelező
	Óvintézkedések	normál körülmények esetén nem kell	kerülni kell az optikai eszközök használatát	ne nézzen a lézersugárba	ne nézzen a lézersugárba, kerülni kell az optikai eszközök használatát	a szemet érő közvetlen expozíció kerülése	a szemet és a bőrt érő közvetlen expozíció kerülése, visszaverődés kivédése	a szemet és a bőrt érő közvetlen és szórt expozíció kerülése, visszaverődés kivédése
Alkalmazási területek		lézernyomtató CD- és DVD író	száloptika	vonalkód leolvasó	szintező lézerek lézeres távolságmérő	nagy teljesítményű lézermutatók	fizioterápiás lézerek kutató-laborok lézerei	lézer-sebészet fizioterápiás lézerek lézerkivetítés

1. táblázat Lézerosztályok, veszélyek és óvintézkedések (szerzők saját szerkesztése [3] és [11] alapján)

A kötelezően elvégzendő kockázatelemzés, a kiemelt veszélyesség és az átfogó biztonsági intézkedések miatt a továbbiakban a 4. lézerosztályba sorolt orvostechnikai eszközt, nevezetesen a Zimmer Medizintechnik GmbH. OptonPro típusú lágylézer készülékét vizsgáltuk, amely 2 db 810 nm-es és 2 db 980 nm-es diódalézer párhuzamos működtetésével dolgozik. [13]

SUGÁRBIZTONSÁGI KÖVETELMÉNYEK

A lágylézer alkalmazásával kapcsolatos munkahelyi sugárvédelmet a sugárzás természetének és a sugárterhelés mértékének ismeretére, a sugárvédelem optimálásának végrehajtására kell alapozni. A sugárveszélyes munkavégzés feltételeit úgy kell megállapítani, hogy a munkavállalók és a környezetében tartózkodók sugárterhelése a vonatkozó dóziskorlátokat ne haladja meg, és a sugárvédelem optimalizált legyen. A munkáltatónak minden lehetséges intézkedést meg kell tennie annak érdekében, hogy a munkavállalók szabályos sugárterhelése, valamint az esetleges sugárterhelés kockázata – a gazdasági tényezők figyelembevételével – az észszerűen elérhető legkisebb legyen. A munkáltató köteles gondoskodni a biztonságos munkavégzés tárgyi feltételeinek teljesítéséről, a szükséges biztonsági berendezésekről, az ionizáló sugárzás elleni védőeszközökről, a berendezések és eszközök hatékonyságának ellenőrzéséről, valamint a sugárvédelmi műszerek működőképességéről, kalibrációjáról és hitelesítéséről. Minderről az Európai Unióban forgalmazott orvostechnikai eszközökre vonatkozó 93/42/EGK irányelveket honosító 4/2009. (III. 17.) EüM rendelet az orvostechnikai eszközökről részletesen rendelkezik. [3]

A lézersugárral közvetlen kapcsolatba kerülő munkavállalók esetében az expozíciós

határértékekről a 22/2010. (V. 7.) EüM rendelet a munkavállalókat érő mesterséges optikai sugárzás expozícióra vonatkozó minimális egészségi és biztonsági követelményekről 2. melléklete ad iránymutatást. A szem és a bőrfelszín esetében a 810 nm és 980 nm hullámhosszok esetében 100 másodperc feltételezett időtartammal kell számolni. [3]

KOCKÁZATOK FELMÉRÉSE, ÉRTÉKELÉSE ÉS KEZELÉSE A LÁGYLÉZER TERÁPIÁBAN

A kockázatkezelés folyamatának első lépése a veszélyek azonosítása. A lágylézer kezelés lépéseit sorra véve meghatározzuk a kockázatokat, amelyek a páciens és a munkavállaló egészségét, a munkakörnyezet, valamint a terápiás készülék állapotát negatívan befolyásolhatják. [14]

A feladat elemzése (a lágylézer kezelés menete)

- Betegtájékoztatás, adminisztráció
    - Páciens tájékoztatása a kezelés menetéről, a lézerterápia lényegéről, előnyeiről, a kontraindikációk ismertetése.
    - Beleegyező nyilatkozat kitöltése és aláírása a páciens és a kezelést végző személy részéről.
    - A páciens kikérdezése, a rendelkezésre álló leletek ellenőrzése, szükség esetén konzultáció a kezelő orvossal.
    - A megállapított problémára vonatkozó kezelési terv kidolgozása, a kezelési lap kitöltése.
- Kezelési környezet kialakítása
    - A figyelmeztető lámpa bekapcsolása és elhelyezése a kezelő helyiség ajtajának külső részén.
    - A kezelő helyiség ajtajának becsukása, reteszelése.
    - A tükröződő felületek (tükrök, ablaktáblák) eltakarásának ellenőrzése.
    - Kezelő fej és a kezelő betétek fertőtlenítése.
    - Védőszemüvegek felvétele.
- A kezelés műszaki feltételeinek biztosítása
    - A biztonsági kulcs csatlakoztatása a készülékhez.
    - A vészleállító gomb ellenőrzése.
    - Készülék bekapcsolása.
    - A biztonsági kód megadása.
    - A kezelési tervben szereplő értékek beprogramozása.
- Kezelés
    - A kezelőfej elhelyezése a kezelendő területen.
    - Az érintőképernyőn lévő engedélyező START gomb megnyomása.
    - A lábkapcsoló működtetése.
    - Kezelés az érintett területeken a beállított üzemmód (folyamatos vagy impulzus-mód), az intenzitás (W) és a dózis (J/cm^2) alapján.
    - A beállított dózis elérésekor az OptonPro készülék automatikusan lekapcsolja a lézersugarat.
- Kezelést követő műveletek

- A készülék kikapcsolása, a biztonsági kulcs eltávolítása, elzárása, a figyelmeztető lámpa kikapcsolása és elhelyezése a tároló állványban.
- A kezelő fej és a kezelő betétek fertőtlenítése.

Veszélyek jegyzékének összeállítása

Ebben a lépésben előzetes veszély-analízissel az előző pontban felsorolt mozzanatokhoz hozzárendeltük a lehetséges veszélyeket. [14]

Feladat	Veszélyek
Betegtájékoztatás, adminisztráció	Kezelés meghiúsulása. Hibás kezelési terv kialakítása.
Kezelési környezet kialakítása	Expozíciós határérték túllépése. Szemek károsodása. Fertőzésveszély.
A kezelés műszaki feltételeinek biztosítása	Kezelés meghiúsulása.
Kezelés	Expozíciós határérték túllépése. Szemek károsodása. Bőrfelszín károsodása. Tűzveszély. Terápiás készülék károsodása.
Kezelést követő műveletek	Illetéktelen használat. Tűzveszély. Fertőzésveszély.

2. táblázat Kockázatkezelés: veszélyek jegyzéke (szerzők saját szerkesztése)

Okok hozzárendelése a veszélyekhez

A kockázatkezelési folyamat következő lépésében összeállítottuk a feladatokhoz rendelt veszélyek kialakulásának lehetséges okait. Ahol egy veszély kialakulásához több ok is vezet, ott kiemelt figyelmet fordítottunk az alapvető ok pontos felderítésére. [14]

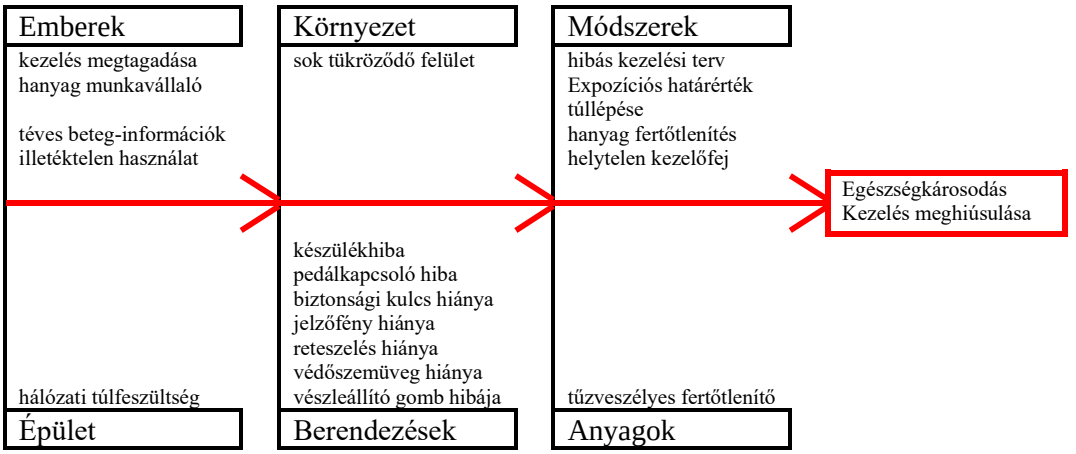
Veszélyek	Lehetséges okok
Kezelés meghiúsulása.	Páciens a kezelést megtagadja. Terápiás készülék meghibásodása. Szem- vagy bőrsérülés a nem megfelelő kezelés következtében. Biztonsági kulcs hiánya.
Hibás kezelési terv kialakítása.	Páciens hiányos és/vagy megtévesztő információkat ad.
Expozíciós határérték túllépése.	A terápiás készülék gyártója által megadott nominális veszélyességi távolságon belül (esetünkben 3 méter) a munkavállalót napi 8 órában a 22/2010. (V. 7.) EüM rendelet 2. mellékletében megadott expozíciós határértéknél több sugárzás éri.
Fertőzésveszély.	Kezelőágy, kezelőfej, védőszemüveg nem megfelelő fertőtlenítése.
Szemek károsodása.	Tükröződő felületek (pl. tükrök, ablakok, vitrinek) nem megfelelő eltakarása. Védőszemüveg hiánya. Az aktív lézersugárra figyelmeztető vörös

Veszélyek	Lehetséges okok
	jelzőfény meghibásodása vagy hiánya. Kezelőhelyiség ajtó reteszelésének meghibásodása vagy hiánya. Fáradt, hanyag munkavállaló.
Bőrfelszín károsodása.	Páciens a valós állapotát elhallgatja. Hibás kezelési terv miatt túl magas intenzitású, helytelen jelformájú vagy túl hosszú ideig tartó aktív lézersugárral történő kezelés. Vészleállító gomb meghibásodása vagy hiánya. Nem megfelelő kezelőfej használata. Terápiás készülék meghibásodása.
Tűzveszély.	A 4. lézerosztályú készülék lézersugara keltette magas hőmérséklet miatt a fertőtlenítéshez használt vegyszerek lángra lobbannak.
Terápiás készülék károsodása.	A fertőtlenítéshez használt vegyszer a készülékbe ömlik. Helytelen használat miatt a készülék és a kezelőfej közötti összeköttetés megszakad. Helytelen használat miatt a készülék és a pedálos kapcsoló közötti összeköttetés megszakad. Hálózati túlfeszültség.
Illetéktelen használat.	Biztonsági kulcs nem megfelelő tárolása.

3. táblázat Kockázatkezelés: a veszélyeket kiváltó okok (szerzők saját szerkesztése)

Stratégiai veszély-meghatározás

Az előzőekben felsorolt veszélyek és az azok kialakulásához vezető okokat Ishikawa-diagramban ábrázolva a veszélyforrások, így a kockázatok közép- és hosszútávon történő minimalizálása valósítható meg. Az ok-okozati diagram a kockázatkezelés következő lépéséhez, a kockázatbecsléshez is megfelelő alapot nyújtott. [14]



4. ábra Kockázatkezelés: veszélyek ok-okozat (Ishikawa) diagramja (szerzők saját szerkesztése)

Kockázatbecslés

A kockázatbecslés szemléltetéséhez kockázatbecslési mátrixot készítettünk a feltárt veszélyek súlyossága és az azok kialakulásához vezető okok valószínűsége alapján. A veszélyek súlyosságát négy kategóriába soroltuk, nevezetesen: katasztrofális, kritikus, csekély, elhanyagolható. A bekövetkezésük valószínűségének becsléséhez pedig öt kategóriát állítottunk fel: gyakori, valószínű, eseti, ritka, valószínűtlen. Az elvégzett kezelések tapasztalati adatai alapján kialakult kockázati szintekhez a magas, közepes, alacsony és csekély kategóriákat alkalmaztuk. [14]

KOCKÁZATBECSLÉSI MÁTRIX			VALÓSZÍNŰSÉG				
			Gyakori (5)	Valószínű (4)	Eseti (3)	Ritka (2)	Valószínűtlen (1)
SÚLYOSSÁG	Katasztrofális (4)		20	16	12	8	4
	Kritikus (3)		15	12	9	6	3
	Csekély (2)		10	8	6	4	2
	Elhanyagolható (1)		5	4	3	2	1
Értékelés	1-3	csekély	Elfogadható (intézkedés nem szükséges)				
	4-6	alacsony	Vizsgálat szükséges (eredménytől függő intézkedés)				
	8-10	közepes	Vizsgálat után kockázatcsökkentés szükséges!				
	12-20	magas	Kerülendő, haladéktalan kockázatcsökkentés kell!				

4. táblázat Kockázatkezelés: kockázatbecslési mátrix (a szerzők saját szerkesztése [14] alapján)

Veszélyek kockázati besorolása

Annak érdekében, hogy megfelelő intézkedési terv jöjjön létre a kockázatok csökkentésére, a korábban meghatározott veszélyeket kockázati szempontból rangsorolnunk kellett. Az 5. táblázatban látható kockázati besorolás a szerzőnek(1) az elmúlt tíz év lágylézer terápiás gyakorlata alapján készült.

Veszélyek	Súlyosság	Valószínűség	Kockázati besorolás
Kezelés meghiúsulása.	katasztrofális	eseti	magas
Szemek károsodása.	katasztrofális	valószínűtlen	alacsony
Bőrfelszín károsodása.	katasztrofális	ritka	közepes
Hibás kezelési terv kialakítása.	kritikus	ritka	alacsony
Expozíciós határérték túllépése.	kritikus	valószínűtlen	csekély
Fertőzésveszély.	kritikus	valószínűtlen	csekély
Tűzveszély.	csekély	valószínűtlen	csekély
Terápiás készülék károsodása.	csekély	valószínűtlen	csekély
Illetéktelen használat.	csekély	valószínűtlen	csekély

5. táblázat Kockázatkezelés: a veszélyek kockázati besorolása (Szerzők saját szerkesztése)

Az 5. táblázat alapján a kezelés meghiúsulását kiváltó okok esetében haladéktalan, ezt követően a szemek és a bőrfelszín károsodása tekintetében kell kockázatcsökkentő lépéseket tenni. A hibás kezelési terv tekintetében az okok vizsgálatát követőn, annak eredményétől függően szükséges a kockázatok csökkentése.

Kockázatcsökkentési lehetőségek és azok várható hatásai

A kezelés meghiúsulása megtörténhet akkor, ha a páciens a kezelést megtagadja. Ennek oka lehet a nem megfelelő betegtájékoztatás. Amennyiben ez előfordul, akkor felül kell vizsgálni a tájékoztatás tartalmát, valamint a munkavállalók hozzáállását. Intézkedésként a kezelést végző munkavállalók oktatása, motiválása jöhet szóba. A terápiás készülék meghibásodása esetén haladéktalanul gondoskodni kell a hibás készülék szakszervízbe történő elszállításáról és a mielőbbi javításáról. A kezelés meghiúsulása kivédhető egy alacsonyabb intenzitású, ezért alacsonyabb rendelkezésre állási költséggel bíró cserekészülékkel. A biztonsági kulcs hiánya úgy védhető ki, ha a lágylézer terápiás készülék használatára jogosultak a biztonsági kulcsot minden esetben a kijelölt, idegenek által nem hozzáférhető tárolóhelyen tartják. Amennyiben a helytelenül használt kezelőfej vagy a tükröződő felületek nem megfelelő eltakarása miatt szemsérülés, vagy a helytelenül megválasztott intenzitás/kezelési idő miatt bőrsérülés (égés) következik be, annak orvosi ellátásáról haladéktalanul gondoskodni kell. A páciens esetleges kártérítési igényének anyagi kihatásának kockázatát pedig szakmai felelősségbiztosítás megkötésével lehet csökkenteni.

A hibás kezelési terv kockázatának csökkentése úgy lehetséges, ha a beteg az első alkalommal bemutatja a kórelőzményeit tartalmazó vizsgálati leleteket, hogy a kezelő személy objektív adatok alapján döntsön a kezelési paraméterekről. Lényeges, hogy a páciens rendelkezzen orvosi ajánlással. A lehetséges kontraindikációk miatt orvosi javallat hiányában meg kell kérni a beteget, hogy a kezelések megkezdése előtt kérjen szakorvosi véleményt. Az intézkedések megtételét követően az új protokoll betartását rendszeresen ellenőrizni kell, és az 1993. évi XCIII. törvény a munkavédelemről 54. § (3) alapján „a munkáltató a kockázatértékelést, a kockázatkezelést és a megelőző intézkedések meghatározását – eltérő jogszabályi rendelkezés hiányában – a tevékenység megkezdése előtt, azt követően indokolt esetben, de legalább 3 évente köteles elvégezni.” [15] A kockázatértékelés alapján foganatosított intézkedések megtétele és azok maradéktalan betartása esetén a veszélyek kockázati besorolása a 6. táblázatban foglaltak szerint alakul.

Veszélyek	Súlyosság	Valószínűség	Kockázati besorolás
Kezelés meghiúsulása.	katasztrofális	valószínűtlen	alacsony
Szemek károsodása.	katasztrofális	valószínűtlen	alacsony
Bőrfelszín károsodása.	katasztrofális	valószínűtlen	alacsony
Hibás kezelési terv kialakítása.	kritikus	valószínűtlen	csekély
Expozíciós határérték túllépése.	kritikus	valószínűtlen	csekély
Fertőzésveszély.	kritikus	valószínűtlen	csekély

Veszélyek	Súlyosság	Valószínűség	Kockázati besorolás
Tűzveszély.	csekély	valószínűtlen	csekély
Terápiás készülék károsodása.	csekély	valószínűtlen	csekély
Illetéktelen használat.	csekély	valószínűtlen	csekély

6. táblázat Kockázatkezelés: a kockázatcsökkentő intézkedések várható hatásai (szerzők saját szerkesztése)

KÖVETKEZTETÉSEK, JAVASLATOK

A lágylézer kezelések esetében feltárt kockázatok többsége esetén intézkedésekre van szükség. A sugárbiztonsági szabályok betartásával az optikai sugárzást kibocsátó készülékkel történő munkavégzés úgy a munkavállalók, mint az azzal kapcsolatba kerülő környezet számára biztonságos kell, hogy legyen. A munkavállalók védelmét és biztonságát optimalizálni kell annak érdekében, hogy az egyéni dózisok nagysága, a sugárzásnak kitett személyek száma és a sugárterhelés valószínűsége az észszerűen elérhető legalacsonyabb szinten maradjon Az optimalizáláskor tekintettel kell lenni a tudományos és technikai adottságok mellett a gazdasági és társadalmi tényezőkre is. Az intézkedések hatékonyságának ellenőrzésére a munkaadó részéről célszerű balesetelhárítási és cselekvési tervet lefektetni, amely tartalmazza azokat az általános és helyi műszaki, valamint adminisztratív intézkedéseket, amelyek a kockázatok csökkentését, minimalizálását szolgálják.

FELHASZNÁLT IRODALOM

[1] Varga B.: Lézerberendezések. lasertanacsado.hu. https://lasertanacsado.hu/berendezes.html (letöltve 2024. március 27.)
[2] J.E. Harry és I. Dr. Kertész I.: Ipari lézerek és alkalmazásuk. Műszaki Könyvkiadó, Budapest, 1979, ISBN 963-10-2594-2
[3] Sandra S.: Lágylézer terápia I. San-Ergonómia Kft, Budapest, 2016, ISBN 978-963-12-5067-1
[4] Damjanovich S. – Fidy J. – Szöllősi J.: Orvosi biofizika. Medicina Könyvkiadó, Budapest, 2006, ISBN: 9632260244
[5] Online Beszámoló és űrlapkitöltő Rendszer, Igazságügyi Minisztérium Céginformációs és az Elektronikus Cégeljárásban Közreműködő Szolgálat, https://e-beszamolo.im.gov.hu/oldal/kezdolap# (letöltve: 2024. március 28.)
[6] Csermely M.: A fizioterápia kézikönyve. White Golden Book, 2011, ISBN: 9799639476331
[7] Dr. Hopp B. et al.: Lézerek az Orvostudományban. Szegedi Tudományegyetem, 2012, TÁMOP-4.1.1.C-12/1/KONV-2012-0005 projekt „Ágazati felkészítés a hazai ELI projekttel összefüggő képzési és K+F feladatokra", https://titan.physx.u-szeged.hu/tamop411c/public_html/Lézerek%20az%20orvostudományban/21_az_elektromgneses_spektrum.html (letöltve: 2024.03.28.)
[8] Hamblin M.R.-de Sousa M.V.P.-Agrawal T.: Handbook of Low-Level Laser Therapy. Pan Stanford Publishing Pte. Ltd., USA, 2017, ISBN 978-981-4669-60-3 (Hardcover), ISBN 978-981-4669-61-0 (eBook), (letöltve: 2024.03.28.)
[9] R.I. Barbosa, E.C. de Jesus Guirro, L. Bachmann, et al., Analysis of low-level laser

transmission at wavelengths 660, 830 and 904nm in biological tissue samples, Journal of Photochemistry & Photobiology, B: Biology (2020), https://doi.org/10.1016/j.jphotobiol.2020.111914
[10] Dr. Horváth J.: Lágylézer terápia. Lézer-Praxis, Budapest, 2003, ISBN 9632063015
[11] MSZ EN 60825-1:2015 Lézergyártmányok sugárbiztonsági előírásai. 1. rész: Készülékosztályozás és követelmények (IEC 60825-1:2014) ICS: 31.260 Optoelektronika. Lézerberendezések; 13.110 Gépek biztonsága, Megjelenés dátuma: 2015.04.01, https://szabvanykonyvtar.hu/web/viewer.php?file=Standard/045XU3Y6OL33ORG4.pdf&name=RC5TLkMuIEh1bmdhcmlhIEtmdC4= (letöltve: 2024.03.28.)
[12] 22/2010. (V. 7.) EüM rendelet a munkavállalókat érő mesterséges optikai sugárzás expozícióra vonatkozó minimális egészségi és biztonsági követelményekről, Net Jogtár, https://net.jogtar.hu/jogszabaly?docid=A1000022.EUM (letöltve: 2024.03.28)
[13] Zimmer OptonPro Gebrauchsanweisung, Manualslib, https://www.manualslib.de/manual/661641/Zimmer-Optonpro.html (letöltve:2024.03.28.)
[14] Dr. Pokorádi L.: Karbantartás elmélet, Elektronikus tansegédlet, Debrecen, 2002 https://dea.lib.unideb.hu/server/api/core/bitstreams/e00d0e40-8031-41de-b1af-61a869eeec99/content (letöltve: 2024.02.16.)
[15] 1993. évi XCIII. törvény a munkavédelemről. https://net.jogtar.hu/jogszabaly?docid=99300093.TV (letöltve: 2024. 04. 12.)

CURRENT CYBER SECURITY OF THE ELECTRICITY SYSTEMS

VILLAMOSENERGIA-RENDSZEREK AKTUÁLIS KIBERBIZTONSÁGA

DÉR Attila[1]

Abstract

We have built ourselves an infrastructure system that supports our daily lives and makes them more comfortable, but these systems rely almost entirely on IT systems. But everything requires electricity. The electricity system has changed significantly over the last decade, becoming more complex, more sophisticated and increasingly indispensable. This highlights the crucial role of security of supply. The need for research is also underlined by the fact that cyber-attacks on critical infrastructure are increasing year on year. The research objective of this paper is to explore the current state of security of electricity supply systems and to define the security of the domestic energy supply systems in the light of this. In terms of research methods, I compare several critical infrastructures at international and national level. Current cyber security risks will be assessed, analysed and evaluated through expert interviews. Furthermore, I will evaluate existing data on the protection of energy supply systems and make recommendations based on this data.

Keywords

cyber security, cyber defence, electricity system, critical infrastructure, electricity supply

Absztrakt

Kiépítettünk magunknak egy olyan infrastruktúra rendszert, amely a mindennapi életünket támogatja, komfortosabbá teszi, azonban ezek a rendszerek szinte teljes mértékben az informatikai rendszerekre támaszkodnak. Mindenhez azonban villamos energiára van szükség. A villamosenergia-rendszer az elmúlt évtized óta jelentős változásokon ment keresztül összetettebb, bonyolultabb és egyre nélkülözhetetlenebb lett. Mindez abszolút rávilágít az ellátásbiztonság kulcsfontosságú szerepére. A kutatás szükségességét az a tény is alátámasztja, hogy kibertámadások a kritikus infrastruktúrák tekintetében évről évre növekszik. Jelen cikk kutatási célja feltárni a villamosenergia-rendszerek jelen helyzetű védelmi helyzetét, és ennek tükrében meghatározni a hazai energiaellátó rendszerek védelmét. A kutatási módszerek tekintetében összehasonlítok több kritikus infrastruktúrát nemzetközi és hazai szinten. Az aktuális kiberbiztonsági kockázatokat felmérem, elemzem és szakértői interjúk segítségével kiértékelem. Továbbá az energiaellátó rendszerek védelméről meglévő adatokat kiértékelem és ennek alapján ajánlásokat teszek.

Kulcsszavak

kiberbiztonság, kibervédelem, villamosenergia-rendszer, kritikus infrastruktúra, villamosenergia-ellátás

[1] der.attila@uni-obuda.hu | ORCID: 0009-0008-9547-102X | PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A villamosenergia-rendszerek kialakulása a múlt század legelejére tehető, amikor még a fogyasztó csak egyetlen villamos hálózattal volt összekötve az erőművel. Ez azt jelentette, hogy hibák és karbantartások esetén kiesések lehettek a fogyasztói hálózaton a termelő egység teljes tartalék tartását követelte meg. Ennek következtében a fogyasztók ellátásának biztonsága érdekében meghatározott körzetekben lévő villamos termelő létesítményeket összekapcsoltak, hogy a tartalékok és terheléseloszlásokat kiegyenlítsék a különböző erőművek között. Végül ezekből a kisebb kooperációkból napjainkra már kontinens méretű együttműködés alakult ki. Magyarországon, mint villamosenergia-rendszer hivatalosan 1949-ben lett kialakítva VER néven, amely később 2011-től lett tagja ENTSO-E RG CE (Europian Network of Transmission system Operators for Electricity, Regional Gro up Continental Europe)

Amikor már nem közvetlen kapcsolat van a fogyasztó és az energiaellátást biztosító intézmény között és egyre nagyobbak a távolságok, akkor már komoly szállításról, illetve átvitelről beszélünk, amelyek már külön kategóriát képviselnek a villamosenergia-rendszeren belül. Az átviteli és az elosztó hálózati rendszerek feszültségszinteknek megfelelően lettek besorolva. Közvetlenül az erőműből természetesen a legnagyobb feszültségű vezetékek szállítják az elektromos áramot. A nagyfeszültségű vezetékek 750kV-, 400kV és 220kV értékek között mozoghatnak, attól függően, hogy milyen teljesítményű erőművekre csatlakoznak. Fontos viszont megemlíteni, hogy a nagyfeszültségű hurkolt vagy alap átviteli hálózat és az elosztó hálózat közötti feszültségszint határa a 120kV, ahol a 400/120kV és 220/120kV-ra transzformált feszültséget transzformátorokkal csökkenti tovább középfeszültségűszintre, azaz 35kV-, 20kV és 10kV elosztó hálózati szintre. Itt már megjelenek már a különféle ipari fogyasztók is, mint például gyárak, üzemek vasúti szállítás stb. Végül a legkisebb feszültségű hálózatok 0,4kV-val üzemelő a kisfeszültségű hálózatok, amelyek már a főként lakossági fogyasztókkal vannak összefüggésben. [1]

VILLAMOSENERGIA-RENDSZER RÖVID ÁTTEKINTÉSE

A cikk megírásával kapcsolatban releváns bemutatni ennek a három hálózati szintnek a topológiáját is, mivel kibertámadások alkalmával egyáltalán nem mindegy, hogy milyen elrendezésűek ezek a rendszerek. Az alap nagyfeszültségű hálózat hurkolt, nem véletlenül nevezik a teljes rendszer gerincének. Míg a középfeszültségen sugaras kialakítású a táppont és a fogadó pont között egy átviteli út van. A középfeszültségű elosztó hálózat fogadó pontjai a középfeszültségű elosztó hálózati gyűjtősínek, transzformátorállomások. Az azonos feszültségszinten sugarasan üzemelő vezetékeken az energiaellátás folyamatosságának és így a fogyasztók ellátása biztonságának növelésére bontási helyeket (összekapcsolási lehetőségeket) alakítanak ki, ezáltal a sugarasan ellátott körzetek nagysága változtatható. A vidéki szabadvezetékes elosztóhálózat jellemző feszültségszintje 20 kV, a városi kábelhálózatok zöme 10 kV névleges feszültségű. A kisfeszültségű hálózatokra általában a sugaras topológia a legjellemzőbb, de meg lehet találni speciális hurkolt kialakítást is, ahol a sugaras vezeték összeillesztését biztosító eszköz segítségével oldják meg. [1]

Mint már említettem a bevezetőben a villamosenergia-rendszer fő célja a villamosenergia-termelése, -átvitele és –szállítása az erőművektől a végfelhasználókig, amelyek

közé tartoznak a háztartások, a kereskedelmi épületek és az ipar. A hagyományos energetikai hálózataink az elmúlt évek során átalakult egy speciális intelligens hálózattá, amely a kiber-fizikai rendszert is magában foglalja, mint ahogy egyes kutatásokban Smart Grid (SG) és Cyber-Physical System (CPS), mint angol kifejezéseket már együtt használják. A hagyományos elvek szerint a villamosenergia-rendszernek két tartópillére van az egyik a fizikailag kiépített rendszer, mint például erőművek, alállomások, átviteli vezetékek, okos mérőberendezések stb. és a másik az információs és kommunikációs technológiákon alapuló irányítási rendszer. Természetesen a hagyományos felépítés nem változott meg alapjaiban, hanem csak a vezérlés és az irányítás technológiája fejlődött napjainkra óriási léptéket. Így a már említett kiber-fizikai rendszer összekapcsolása intelligens hálózatokkal felvetett egy újfajta csoportosítást, amelyben négy kulcsfontosságú elem található. Az első elem a villamosenergia-rendszer a második elembe tartoznak a méréseket, érzékelőket és az aktuátorokat irányító rendszer, a harmadik a vezérlő egységeket magába foglaló rendszer és negyedik a kommunikációs rendszer. Ennek megfelelően az intelligens hálózati rendszerek alrendszereiben is megtalálhatók a védelem és az áramellátás kapcsolatában az intelligens elektronikával felszerelt eszközök, távoli elérésű terminálegységek (RTU), relék, áram- és feszültségszabályozók, feszültségszint átalakítására szolgáló transzformátorok, valamint különféle méretű és fajtájú megszakítók. A villamosenergia-rendszer felügyeletéhez és működtetéséhez szükséges elektromos jelek mérését is az intelligens elektronikával felszerelt eszközök, távoli elérésű terminálegységek (RTU) és a fázismérő egységek szolgáltatják. Ezeket a mérési adatokat az alállomások adatgyűjtő egységei összegyűjtik és továbbítják a villamosellátást irányító központokba.[2]

Az irányítóközpont felelős az energiarendszer felügyeletéért, biztonságáért és stabilitásáért. Az állapotbecslő alkalmazások tervezéséhez a SCADA-rendszerből kapott mérési adatokat használja fel a villamosenergia-rendszer működésének becsléséhez. Az állapotbecslő alkalmazások ezután elemzik a villamosenergia-rendszer biztonságát és stabilitását.[3]

NEMZETKÖZI KITEKINTÉS

Egyesült Államok

Ebben a fejezetben egy rövid kitekintést tennék más országok villamosellátásával kapcsolatosan, hogy összehasonlítás nyújtson hazánk helyzetével. Az egyik ilyen kiemelkedő fontosságú ország az Amerikai Egyesült Államokban, ahol hatalmas kiterjedésű és rendkívül összetett rendszer van. A nagyságrendek érzékeltetéséhez két adatot említenék: körülbelül 3300 szolgáltató van az Amerikai Egyesült Államokban, amely 200000 mérföldnyi átviteli hálózattal rendelkezik. Mivel az Egyesült Államok rengeteg államból áll, így az egész országra kiterjedő egységes szabályozás igencsak nehéz. Van egy úgynevezett Észak-Amerikai Villamos Megbízhatósági Tanács a NERC(North America Electric Reliability Council)[4], amely a kritikus infrastruktúra előírásaival egyetemben kidolgozott megbízhatósági szabványokat a villamosenergia rendszerek védelmére. Ezek az egyes államokra kötelező jellegű szabályozások különböző szempontokra terjednek ki, mint például a rendszer és a vezérlés biztonságának kezelésére, a személyzet képzésére, a kritikus kibereszközök azonosítására, fizikai biztonságra és helyreállítási tervek elkészítésére stb. A 45 követelményt és kilenc szabványt tartalmazó előírás jelentősen befolyásolja és biztosítja a nagy

teljesítményű villamosenergia-rendszerek nagyfokú megbízhatóságát. Ennek ellenére az észak-amerikai közművek felére vonatkoznak kötelező jelleggel. Felmérések szerint az amerikai villamoshálózat ellen intézett támadások jellentő kárt tudnának okozni az energiaellátásban, akár több tíz millió fogyasztónál lehetne elérni időlegesen áramszünetet. Az amerikai Nemzeti Szabványügyi és Technológiai Intézet a NIST (National Institute of Standards and Technology) létrehozta a NISTIR 7628 Rev. az intelligens hálózatok kiberbiztonságára vonatkozó iránymutatások (Guidelines for Smart Grid Cybersecurity) jelentését, amelyben egy speciális keretrendszert dolgozott ki a hatékony kiberbiztonsági stratégiák kidolgozásához. Az Intelligens Hálózatokban részvevők kockázatértékeléshez, valamint a kockázatok azonosításához és a megfelelő biztonsági követelmények alkalmazáshoz használhatják. A NISTIR 7628 Rev.1. 2014-ben vezették be, hogy felváltja a NISTIR 7628 iránymutatást, amely a 2010. évben jelent meg. Ez a szabvány már megemlíti, hogy az elektromos hálózatok átalakulóban vannak viszonylag zárt rendszerből egy összetett, nagymértékben összekapcsolt környezetté. Továbbá fontos szempontként kiemeli, hogy az egyes kritikus infrastruktúráknak együtt kell fejlődniük karöltve a technikai fejlődéssel, hogy elkerüljék az elmúlt években megsokszorozódott hálózat biztonságát fenyegető veszélyek elkerülését.[3][5]

Európai Unió

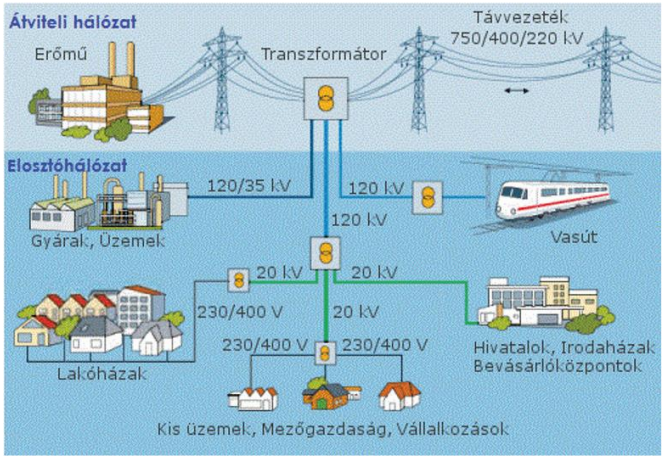
A Európai Unióban három főbb szabályozás vonatkozik a villamosenergia rendszerekre az EU Tanács által kiadott 2008/114/EK irányelve, amely az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szól. A második Az Európai Uniós Kiberbiztonsági Ügynökség(ENISA) vonatkozásában az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály). Végül a harmadik komponens a Hálózati és információs rendszerek biztonságáról (NIS2) szóló irányelv.[6]

Az Európai Bizottság 2017/1485 számú rendelete a villamosenergia-átviteli hálózat üzemeltetésére vonatkozóan módszertani javaslatokat fogalmaz meg az egyes hálózati elemek kiesésének relevanciája kapcsán (Európai Unió 2017). Fontos mérföldkő ennél a rendeletnél, hogy a rendszerirányítóknak modellezések és szimulációk segítségével egy olyan módszertant kell kialakítani, amelyben képesek az átviteli és elosztórendszerek létfontosságát megvizsgálni és kiértékelni. Utána kettő év múlva lett kihirdetve az Európai Parlament és a Tanács 2019/941 rendelete a villamosenergia-ágazati kockázatokra való felkészülés vonatkozásában, amelyben minden tagállamnak nemzeti kockázati tervet kell kidolgoznia a regionális és tagállami villamosenergia-ellátási válságforgatókönyvek alapján (Európai Parlament és Tanács 2019).[7] Minden megújuló technológia ott hasznosulna a rendszerben, ahol a legjobbak a földrajzi adottságok: a nagy szélerőműparkok a tengerpartokra, a naperőművek az intenzív besugárzású területekre, a vízerőművek a hegyvidéki övezetekbe stb. települnének.[8]

HAZAI VILLAMOSENERGIA-RENDSZER HELYZETE

Magyarországnak 23 nagyerőműve van, amelyek bruttó beépített teljesítménye 6.756,9 MW, de ez a teljesítmény nem használható ki teljes mértékben az erőművek önfogyasztása, valamint az állandó hiány miatt. A rendszerszintű koordinációban mind a 23 villamos termelő egység jelentős kapacitással vesz részt. Ebből a legjelentősebb a Paksi Atomerőmű, amely nagyjából az összes hazai beépített teljesítmény egyharmadát adja nagyjából 2000MW-ot.[9]

A hazai villamosenergia-rendszer működéséért, az ellátásbiztonságért és a fogyasztás pillanatnyi egyensúlyának fenntartásáért a Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zártkörűen Működő Részvénytársaság (MAVIR Zrt) gondoskodik nap, mint nap. Legnagyobb mértékben természetesen működése a magyar átviteli hálózatra tevődik, ezért különös figyelmet fordít a feszültség értékekre, meddő teljesítményre és terhelési szögekre. Továbbá folyamatosan monitorozza a hálózat túlterheltségét, illetve megfelelő feszültségszintjét. Gyakran tartanak kiesés vizsgálatokat és szimulációs gyakorlatokat, amelyben a beállított hálózati részeket kikapcsolják, hogy a megterhelt vezetékeken átfolyó áram nem okoz-e túlterhelődést más közelben lévő részekre. A MAVIR ezeket a számításokat periodikusan egész nap az év 365 napjában teszteli.



1. ábra átviteli és elosztóhálózat, forrása:[9]

Az európai országokban is megvannak a MAVIR-hoz hasonló rendszerirányító központok, amelyek egyébként napjainkban már teljes belépő és kilépő villamos hálózata össze van kötve egymással. Így a magyar villamosenergia-rendszer szimbiózisban van a többi tagország rendszereivel, ami azt jelenti, hogy bármely nagyobb nemzeti üzemzavar vagy szabályozás az egész európai rendszert érinti. Ennek következtében nagyon fontos, hogy ezen kritikus infrastruktúra irányítói szoros kooperációban együttműködjenek egymással és egy teljes részt alkossanak az Európai Unió zökkenőmentes energiaellátásának biztosítása érdekében.[9]

Kockázatok és sérülékenységek a villamosenergia ellátásban

Természetesen már a legelején le szeretném szögezni, hogy kutatásomban előforduló kockázatokat és sérülékenységeket csak specifikusan a témával szorosan összefüggő adatok és elemzések alapján vizsgáltam a teljesség igénye nélkül. A megújuló alapú villamosenergia-termelés aránya az elmúlt években exponenciálisan nőt és az elkövetkezendő évekre is ez a tendencia lesz majd érvényes. Ezeket a zöld energiával rendelkező egységeket is el kell látni megfelelő kommunikációs hálózati csatornával illetve hozzá kapcsolódó protokollokkal, hogy egységesen lehessen őket kezelni egy nagy kiterjedésű térség (EU, USA) vagy ország energetikai ellátás láncában. Ennek következtében egyre növekvő Kiberbiztonsági kockázatot is jelentenek évről évre a villamosenergetikai rendszerekben. További kockázatok lehetnek még az ipari felügyeleti rendszerek nyílt forráskódú elérhetőségei vagy a SCADA rendszerek gyártói támogatásának, frissítésének megszűnése. Egyébként az ipari rendszerek legtöbb gyártója sincs felkészülve a különböző kiberfenyegetésekkel szemben, mivel nincs meg a kellő tapasztalatuk és gazdasági érdekük ezzel kapcsolatosan. Így az energetikai rendszerek irányító testületeinek kell olyan beszállítókat találni vagy szerződéseket kötni, ahol markánsan jelen vannak az erre szakosodott védelmi mechanizmusok. Vannak próbálkozások, de sajnos nem kielégítőek egy meghatározó követelményrendszer megalkotásához, amelyek az információs technológia és ICS/SCADA rendszerek legalapvetőbb logikai követelményszintjének megfelelően megalapoznának egy erős védelemhez szükséges feltételrendszert.[6] Ugyan így vannak forgatókönyvek, amelyekben már bekövetkezett eseményeket dolgoznak fel vagy lehetséges fenyegetésekre való felkészülést is tartalmazhatnak. A cél mindig a fenyegetések elleni hatékony megelőzés illetve a már bekövetkezett támadás elhárításának leggyorsabb és leghatásosabb eredeti állapotok visszaállítása. Egy megvalósítható fenyegetéseseménynek négy elemet kell tartalmaznia: az eseményt kezdeményező fenyegetés forrását, a fenyegetésesemény célobjektumát, a célobjektum sebezhetőségét és a sebezhetőséget kihasználó fenyegetés forrását. Ha a potenciális fenyegetés forrása, a sebezhetőség és a sebezhetőséget okozó fenyegetés vektorát azonosítottuk és megértettük, akkor megkaphatjuk a megvalósítható fenyegetésesemény teljes tartalmát**.**[10]

Az elektromos hálózat intelligens hálózatokra történő átalakítása további biztonsági problémákat vett fel a hagyományos elektromos hálózattal ellentétben, amely a Felügyeleti irányítás és adatgyűjtő SCADA-rendszerre támaszkodik a felügyelet és az irányítás tekintetében. Míg az Intelligens hálózatok a hatékonyabb ellenőrzésre és felügyleti pontosság növelésére az információ- és kommunikációstechnológiát (IKT) és Fázismérő egységeket használják. Viszont ennek a technológiának az a hátrány például, hogy a fázismérő egységek feszültség- és áramfázis méréseket továbbítanak meghatározott központi egységek felé kommunikációs csatornákon keresztül, és erre ugyanaz a központi egység vezérlőjeleket ad vissza a fázismérőnek cserébe. Így a felügyeleti és szabályozási folyamatot sérülékenyebbé teszi kibertámadásokkal szemben, ami csökkenti a teljes energiaellátás biztonságát.[2]

Az intelligens hálózatok ellen intézett kibertámadások a rosszindulatú támadások széles skáláját jelentik, amelyek célja a villamos hálózatok adatainak, kommunikációs rendszereinek sebezhetőségének kihasználása. Az ilyen támadások veszélyeztethetik az adatok titkosságát, sértetlenségét és rendelkezésre állását, megzavarhatják a hálózati működést, áramkimaradásokat és egyéb súlyos következményeket eredményezhetnek. Néhány gyakori kibertámadás a villamosenergia rendszer ellen, mint például szolgáltatásmegtagadással járó

támadás (DoS), hamis adatinjekció (FDI), közbeékelődéses támadás man-in-the-middle, malware, adathalászat, terhelésmódosítás, visszajátszás és spoofing támadások.[10]

Intelligens hálózatok valós idejű nyomon követésére és ellenőrzésére SCADA-rendszereket alkalmaznak. Rendszeres időközönként adatokat szereznek az intelligens mérőórák leolvasásából, állapotérzékelőkből és egyéb forrásokból, lehetővé téve a hatékony folyamatirányítást. Ezek a rendszerek távoli elérésű telemechanikai terminál egységekből és programozható logikai egységekből állnak, amelyek távoli érzékelőkkel és működtetőkkel kommunikálnak egymással. Az összegyűjtött adatokat ezt követően egy központi fő terminálegységhez küldik el elemzésre. A SCADA-rendszerek tartalmaznak egy HMI-egységet is, amely lehetővé teszi a kezelők számára a rendszer működésének valós idejű nyomon követését és módosítását. Ezen felügyeleti és adatgyűjtő konstrukciók fő célja az elosztott rendszerek megfelelő felügyelete és kezelése, ami költségmegtakarítást, jobb karbantartást és az energiaellátás megbízhatóságának növelésélést eredményezi. Funkciójának ellátásához azonban a SCADA-nak a kibertámadásokkal szembeni valamennyi biztonsági célkitűzésnek meg kell felelnie. Különböző biztonsági technológiák, mint például a behatolásérzékelő rendszerek (IDS), virtuális magánhálózatok (VPN), internetprotokoll-biztonság, stb. (IPsec) és tűzfalak, amelyeket a SCADA-hálózatokban alkalmaznak a következők védelmére biztonságukat és megbízhatóságukat.[3]

A bevezetésben már említettem a villamosenergia-ellátás topológiáját, amely nagyban függ a hálózat feszültségszítjétől, átviteli vagy elosztó hálózat és az adott térség földrajzi adottságaitól. Ezeket a topológiákat jól lehet vizsgálni és kiértékelni különböző aspektusokban. Ennek hatására kutatásokban gráfelmélet alapján próbálják meg lemodellezni egy lehetséges kibertámadást főként átviteli villamos rendszer hálózatait és csomópontjait figyelembe véve. Meglepetésre a 132kV vezetékek eltávolítása jelentette a legnagyobb sérülékenységet. Ennek oka, hogy ezen élek eltávolítása a gráf több részre eséséhez vezet, szigetüzemű ellátási területeket létrehozva. Ezeknél a tanulmányoknál jól látható, hogy a csomópontok jelentősebbek, mint az élek. A hazai villamosenergia átviteli hálózat két központi alállomását 80%-ban biztosan érinti egy nagyobb kibertámadás. Kombinált támadásoknál általában a keleti országrészben lesznek érzékelhetők a támadások hatásai. Magyarország gerincvezetékét alkotó hurkolt 400kV-os vezetékrendszer szerencsére egyszeres vezetékkiesésre ellenálló.[7][11]

Fontos észrevételem, hogy villamosenergia rendszerben és a leggyakrabban előforduló irányítási és ellenőrző egységek ICS/SCADA-nál kiberbiztonsági kockázatértékelés ne csak papíron legyen, hanem gyakorlatban is ki legyen építve, illetve tesztelve erre tervezett szimulációval vagy akár valós helyzetű gyakorlatokkal. A határvédelemnél nagyobb figyelmet kellene fordítani a hozzáférési lista létrehozására, a port szintű biztonsági alkalmazások megfelelő ellenőrzésére. A tűzfal szabályokat rétegelt stratégiával kell kiépíteni behatolás észlelő és megelőző rendszer kompatibilitásának megőrzése mellett. A hálózati behatolás megelőző rendszer mellett érdemes minden egyes hálózati szegmensbe is hálózati észlelő eszközt telepíteni. Az operatív vagy más néven üzemeltetési technológia hálózataiba behatolás megelőző rendszer helyett inkább a behatolás észlelő rendszert érdemes betervezni. Sőt az érzékeny adatok védelmére ajánlott kriptográfiával titkosított protokollt alkalmazni. Mindig ellenőrzött beszállítótól szerezük be a szükséges rendszerelemeket.

ÖSSZEFOGLALÁS

Villamosenergia rendszer egy dinamikusan felépülő valós idejű folyamat, amelyben olyan visszacsatolásos szabályozás vagy direkt irányítás történik, ahol kiesésnek nincs helye. A Gyors és precíz reagálás ennél a kritikus infrastruktúránál elengedhetetlen feltétele, hogy üzembiztosan működjön. Így a kibervédelmeket is, mint más egyéb védelmeket úgy kell megtervezni, illetve a már meglévőt átalakítani, hogy semmilyen körülmények között se lassítsa az elvárt reakcióidőt. Fontos elvárás az üzemeltetőktől, hogy kialakítsanak egy erre az ágazatra kiélezett eljárásrendet, amely a támadás elhárítása után az eseményeket megfelelően kiértékeli. Továbbá rendelkezik egy saját eseménykezelő csapattal, Biztonsági eseménykezelési szabályzattal és tervezettel. Nemzetközi összehasonlításban kimondható, hogy a magyar villamosenergia-rendszer kibertámadás szempontjából megbízhatóbb, mint az amerikai vagy globálisan nézve az egész Európai Uniós rendszer. Nyílván gazdasági okokra is visszavezethetően nem rendelkezik a legújabb intelligens hálózatok üzemeltetéséhez szükséges információs technológiával – amely nem biztos, hogy mindig hátrány -, de a hálózati topológia kialakítása és a manuális rendszerelemek megléte nagyban hozzájárul ezen tény megállapításához. Az Európai Unió kiberbiztonsági stratégiája és villamosenergia specifikus szabályzatai nagymértékben hozzájárulnak a tagállamok és így hazánk villamosenergia-ellátásának biztonságához és megbízható működéséhez. A jövőre váró ajánlás egy olyan kibervédelmi ellenálló képességére vonatkozó keretrendszer megtervezése, amelyben mesterséges intelligencia által támogatott automatizált helyreállítás, incidensekre való reagálás szervezését biztosítja majd az uniós tagállamok nemzeti szintű igényeihez. [12]

FELHASZNÁLT IRODALOM

[1] Faludi , Andor és Szabó, László, *Villamosenergia-rendszer üzeme és irányítása*, 2012. kiad. Budapest, Hungary: BME.

[2] K. Bitirgen és Ü. B. Filik, „A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid”, *International Journal of Critical Infrastructure Protection*, köt. 40, o. 100582, márc. 2023, doi: 10.1016/j.ijcip.2022.100582.

[3] M. K. Hasan, R. A. Abdulkadir, S. Islam, T. R. Gadekallu, és N. Safie, „A review on machine learning techniques for secured cyber-physical systems in smart grid networks”, *Energy Reports*, köt. 11, o. 1268–1290, jún. 2024, doi: 10.1016/j.egyr.2023.12.040.

[4] „NERC”. Elérés: 2024. május 12. [Online]. Elérhető: https://www.nerc.com/AboutNERC/Pages/default.aspx

[5] The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee, „Guidelines for smart grid cybersecurity”, National Institute of Standards and Technology, NIST IR 7628r1, szept. 2014. doi: 10.6028/NIST.IR.7628r1.

[6] Bonnyai, Tünde, Görgey, Péter, és Krasznay, Csaba, *Villamosenergetikai ipari felügyeleti rendszerek kiberbiztonsági kézikönyve*. Budapest, Hungary: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, 2023. [Online]. Elérhető: https://seconsys.eu/wp-content/uploads/2023/02/SeConSys_kezikonyv_aktual_2023_jan.pdf

[7] B. Hartmann, „Hogyan befolyásolja a villamosenergia-hálózatról rendelkezésre álló információ a fizikai támadások által okozott sérülékenységről alkotott képet?: A hazai energiaszolgáltatás túlélőképessége”, *ScientSec*, köt. 2, sz. 2, o. 155–163, okt. 2021, doi: 10.1556/112.2021.00030.

[8] P. J. Horváth, É. S. Somossy, és T. Tóth, „A decentralizált villamosenergia-rendszerek fejlődésének nemzetközi és hazai szempontjai”, *Közgazdasági Szemle*, köt. 69, sz. 6, o. 697–720, jún. 2022, doi: 10.18414/KSZ.2022.6.697.

[9] G. Kovács, „Az országos villamosenergia-rendszer irányítása”, *Légkör*, köt. 67, sz. 3, o. 157–162, 2022, doi: 10.56474/legkor.2022.3.5.

[10] X. Song, J. Zhao, H. Yuan, Z. Li, Y. Zhi, és X. Zhang, „Network Attack Scenario Analysis and Threat Identification”, in *2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, Chongqing, China: IEEE, okt. 2019, o. 1055–1059. doi: 10.1109/IMCEC46724.2019.8984024.

[11] N. D. Fîţă, M. D. Marcu, D. Păsculescu, F. G. Popescu, és T. Lazăr, „Security Risks Assessment on the 400/275/25 kV Elvanfoot Power Substation from Scotland in Order to Ensure Resilience and Energy Security”, in *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Cape Town, South Africa: IEEE, nov. 2023, o. 1–6. doi: 10.1109/ICECET58911.2023.10389271.

[12] K. Fysarakis *és mtsai.*, „PHOENI2X – A European Cyber Resilience Framework With Artificial-Intelligence-Assisted Orchestration, Automation & Response Capabilities for Business Continuity and Recovery, Incident Response, and Information Exchange”, in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, Venice, Italy: IEEE, júl. 2023, o. 538–545. doi: 10.1109/CSR57506.2023.10224995.

PASSWORD USAGE IN HUNGARY AND SLOVAKIA AMONG USERS OF SMART DEVICES

JELSZÓHASZNÁLAT MAGYARORSZÁGON ÉS SZLOVÁKIÁBAN AZ OKOSESZKÖZ HASZNÁLÓK KÖRÉBEN

MANDIĆ Dorottya[1] – KISS Gábor[2]

Abstract

The number of IoT devices is increasing and more and more people are buying different smart devices, but they do not know how to use them safely. That is why we thought it important to conduct a survey among smart device users, which examines what smart device users use in relation to password use. For example, do they use the same password in several places, how long are the symbols used, how often do they change their password, whether the password they use contains meaningful words or personal information and whether the password contains uppercase and lowercase letters, numbers and special characters. In addition, the survey also deals with showing how popular smart devices are among the participants in the survey in Hungary and Slovakia. The purpose of this study is to present the results of the survey conducted in Hungary and Slovakia among smart device users regarding the use of passwords.

Keywords

password, smart devices, security, IoT, password usage

Absztrakt

Egyre jobban nő az IoT eszközök száma, és egyre többen vásárolnak úgy okoseszközöket, hogy nem tudják hogyan kellene az okoseszközöket biztonságos használni. Ezért fontosnak gondoltunk elvégezni egy felmérést az okoseszköz használók körében, mely azt vizsgálja, hogy az okoseszköz használók a jelszóhasználatra vonatkozóan milyen jelszavakat használnak, például ugyan azt a jelszót használják-e több helyen, milyen hosszú a jelszavakat használnak, milyen gyakran változtatják meg a jelszót, a jelszó amit használnak tartalmaz-e értelmes szót vagy személyes információt, valamint, hogy a jelszó tartalmaz-e kis és nagybetűket számokat, speciális karaktereket. Ezen kívül a felmérés azzal is foglalkozik, hogy bemutatja, hogy Magyarországon és Szlovákiában a felmérésben résztvevők válaszai alapján mennyire népszerűek az okoseszközök. Jelen tanulmány Magyarországon és Szlovákiában végzett felmérés eredményeit szeretné bemutatni a jelszóhasználatra vonatkozóan az okoseszköz használók körében.

Kulcsszavak

jelszó, okoseszközök, biztonság, IoT, jelszóhasználat

[1] mandic.dorottya@uni-obuda.hu | ORCID: 0000-0002-3384-5590 | PhD Student, Óbuda University Doctoral School on Safety and Security Science| PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola
[2] kiss.gabor@bgk.uni-obuda.hu | ORCID: 0000-0002-0447-937 | associated professor, Óbudai University|egyetemi docens, Óbudai Egyetem

INTRODUCTION

The use of smart devices has already become a part of our daily life and more and more people are using various smart devices in their everyday life [1]. Due to the rapid spread of IoT devices it is important to deal with the security of the devices [2], [3], [4]. Among the users there are smart device users who do not take measures to use smart devices more safely. For example ,,many people use a password that is weak and easy to guess." Since more complicated passwords would be much more difficult to remember so they often prefer a password that is easy to guess and that they do not forget [5], [6]. IoT devices often do not have strong passwords so they are vulnerable to attacks and even if users change the password, they often choose a password that is easy to guess [7].

According to Statista's report the five most used passwords for IoT devices in 2021 were ,,admin", ,,root", ,,nc11", ,,user" and ,,enable"[8]. Unfortunately, users often use their smart devices in their everyday life without having sufficient knowledge to be able to use their smart devices safely [9], [10], [11]. There are also smart device users who don't even change the default password, such as ,,123456" or use a password that contains meaningful words or personal information as their date of birth or the name of their favorite pet [12]. According to the NordPass report the most common password in 2019 was ,,12345", followed by ,,123456" in 2020-2021 and ,,password" in 2022 [13]. However, it may also happen that the same password is used in several places. Since this way they do not have to remember several passwords and it is enough to remember the given password. The use of simple passwords is not safe as they can be easily guessed, which attackers can easily take advantage of [14].

On the Security.org page we can see how long it takes to crack a password when passwords of different lengths and content are used [15]. According to Security.org, it takes 2 seconds to crack a 7-character password if it only contains ,,uppercase and lowercase letters" and numbers and if the password does not contain numbers, it takes even less time as 1 second is enough to crack the password. If the password contains both ,,uppercase and lowercase letters", numbers and symbols, 4 seconds are enough to crack the password. If the password contains 8 characters, as well as lower and uppercase letters, in this case 28 seconds are enough to crack the password. If the password contains ,,uppercase and lowercase letters" and numbers, 2 minutes are required. If the password also contains symbols, it takes 5 minutes to crack the password. However, according to Security.org's report, if the password we use contains at least 12 characters and the password contains upper and lower case letters, in this case, according to the report, 6 years may be necessary [16].

According to the Cybernews 2024 report passwords such as ,,123456", ,,123456789", ,,qwerty", ,,password" and ,,12345" were among the top five most used passwords worldwide. Despite the fact that we can find different suggestions on how and why it is important to use strong and unique passwords, as well as why it is recommended to use a password manager. Many people still use weak and easy-to-guess passwords, which even a novice cybercriminal can easily hack [17].

In this survey, we investigated the lengths of passwords that users use among smart device users in Hungary and Slovakia for example whether the password they use contains meaningful words and personal information and whether the password contains small and capital letters, numbers, and special characters and whether the same password is used in

several places. In the research, we looked for the answer to whether there is a difference between the two countries regarding the use of passwords among smart device users, especially when a meaningful word is used as a password.

RESEARH METHODOLOGY

In the research, we looked for the answer to whether there is a difference in the use of passwords between the two countries among smart device users especially if a meaningful word is used as a password. The study examines the password usage habits of smart device users in Hungary and Slovakia, whether smart device users use lower- and upper-case letters, numbers, special characters, personal data, meaningful words and whether they use the same password in several places, the length of the passwords and how often they change the password they use. This survey examines the password usage of smart device users. A total of 194 people in Hungary and Slovakia took part in the survey. The survey was conducted online in both countries and the data was analyzed using the SPSS statistical program. We used the Mann-Whitney U test, and we compared the differences in password usage according to gender in Hungarian and Slovakia.

THE RESULT OF THE SURVEY

A total of 194 people in Hungary and Slovakia took part in the survey. The survey was conducted online in Hungary and Slovakia. A total of 135 people participated in Hungary of which 107 were men (79.3%) and 28 were women (20.7%). A total of 59 people took part in the survey in Slovakia of which 25 were men (42.4%) and 34 were women (57.6%).

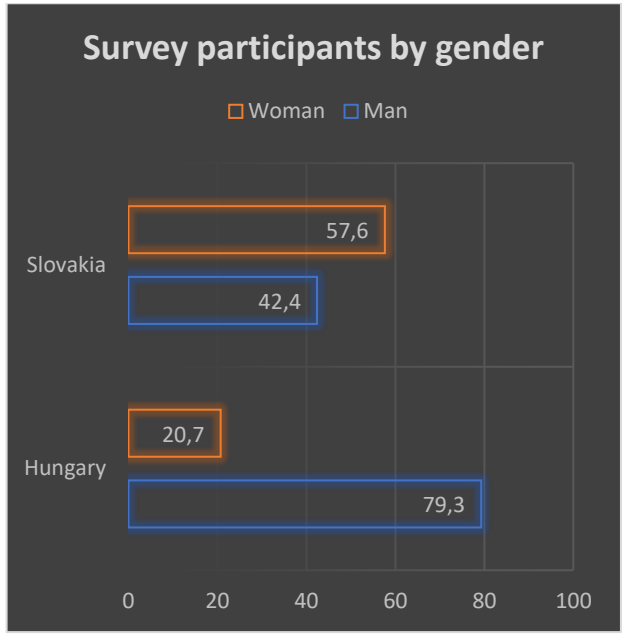


Figure 1: Shows the survey participants in Hungary and Slovakia by gender represented in a diagram. (Source:Created by the author)

On the (Fig.1) diagram, we can see that in Hungary more men took part in the survey than women and in Slovakia more women took part in the survey than men.

Age	Hungary		Slovakia	
	Freq.	**Perc.**	***Freq.***	**Perc.**
18-24 years old	100	74.1%	43	72.9%
25-34 years old	24	17.8%	9	15.3%
35-50 years old	11	8.1%	7	11.9%

Table 1: Age of survey participants in Hungary and Slovakia. (Source:Created by the author)

In (Table 1), we can see that among the participants in the survey in Hungary (74.1%) of the 18-24 year olds took part in the survey, (17.8%) of the 25-34 year olds and (8.1%) of the 35-50 year olds. In Slovakia (72.9%) of 18–24-year-olds participated in the survey (15.3%) of 25–34-year-olds and (11.9%) of 35–50-year-olds. We can see that the 18–24-year-old age group took part in the survey in both Hungary and Slovakia.

Education attainment	Hungary		Slovakia	
	Freq.	**Perc.**	***Freq.***	**Perc.**
Elementary school	10	7.4%	0	0%
High School	82	60.7%	42	71.2%
College	28	20.7%	16	21.7%
University	10	7.4%	1	1.7%
Others	5	3.7%	0	0%

Table 2: Educational level of the participants in the survey in Hungary and Slovakia. (Source:Created by the author)

In Table 2, we can see that 10 (7.4%) of the participants in the survey answered that they had a primary school education 82 (60.7%) had a secondary school education and 28 (20.7%) answered that they had a college degree and 10 (3.7%) answered that they had a university degree and 5 (3.7%) answered that they had other degrees. In Slovakia 42 (71.2%) of the survey participants answered that they had high school education and 16 (21.7%) answered that they had college education and only 1 of the respondents (1.7%) answered that they have a university degree. In the survey, we also examined how many of the respondents who use smart devices have an IT degree in Hungary and Slovakia. Based

on the survey in Hungary (33.4%) answered that they had an IT degree and (66%) answered that they did not. In Slovakia (41.4%) of survey participants answered that they had an IT degree and (58.6%) answered that they did not. When asked whether the participants in the survey use smart devices, we can see in (Figure 2) that in Hungary (98.5%) answered that they use smart devices and only (1.5%) answered that they do not. In Slovakia (98.3%) of the participants in the survey answered that they use a smart device and (1.7%) answered no. We can see that based on the responses of the participants in the survey in Hungary and Slovakia more than 98% of the respondents answered that they use at least one smart device. Figure 2. shows how many of the survey participants answered that they use smart devices.

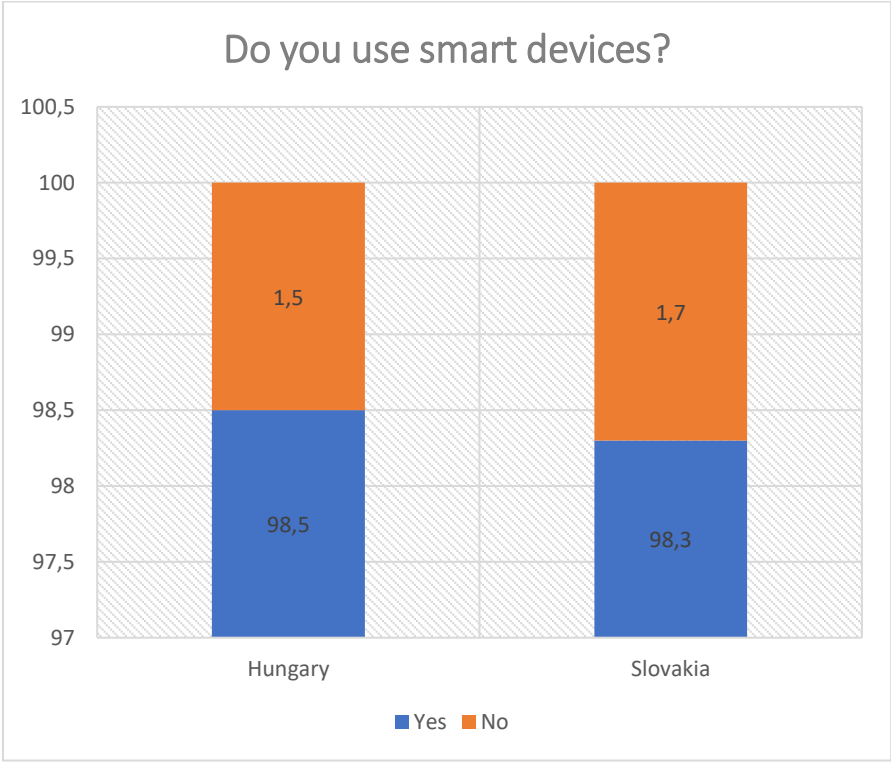


Figure 2: Based on the answers of the participants in the survey, whether they use smart devices in Hungary and Slovakia. (Source:Created by the author)

Smart devices use by gender	**Hungary**		**Slovakia**	
	Freq.	**Perc.**	***Freq.***	**Perc.**
Man	106	79.7%	24	42.1%
Women	27	20.3%	33	57.9%

Table 3: Smart device users by gender in Hungary and Slovakia. (Source:Created by the author)

If we look at the number of people who answered that they use smart devices by gender, then based on the survey in (Table 3), we can see that in Hungary 106 of the men (79.7%) answered that they use smart devices and 27 of the women (20.3%) answered that they use reasoning tools based on the survey. In Slovakia based on the survey 24 (42.1%) of the men and women 33 (57.9%) answered that they use smart devices.

How long is the password that you use?	**Hungary**		**Slovakia**	
	Freq.	**Perc.**	***Freq.***	**Perc.**
Less than 8 characters.	4	3%	27	45.8%
8-10 characters.	71	53.4%	0	0%
12 or more characters.	58	43.6%	31	52.5%

Table 4: The answers of the participants in the survey about what long passwords are used in Hungary and Slovakia. (Source:Created by the author)

In (Table 4.), we can see that in Hungary 4 (3%) of the participants in the survey answered that they use less than 8 characters as a password, 71 respondents (53.4%) answered that the password they use uses 8-10 characters and 58 (43.6%) answered that they use 12 or more characters as a password. Median=2 U=1452 z= -0.114 p=0.910 r=0.010 In Slovakia 27 (45.8%) respondents answered that they use a password that contains less than 8 characters and 31 (52.5%) answered that the password they use contains 12 or more characters. Based on the survey, we can see that more people in Slovakia answered that they use 12 or more characters as passwords than in Hungary. Most of the participants in the survey in Hungary answered that they use 8-10 characters as passwords. Median= 3 U=336 z=-1.390 p=0.165 r= 0.198

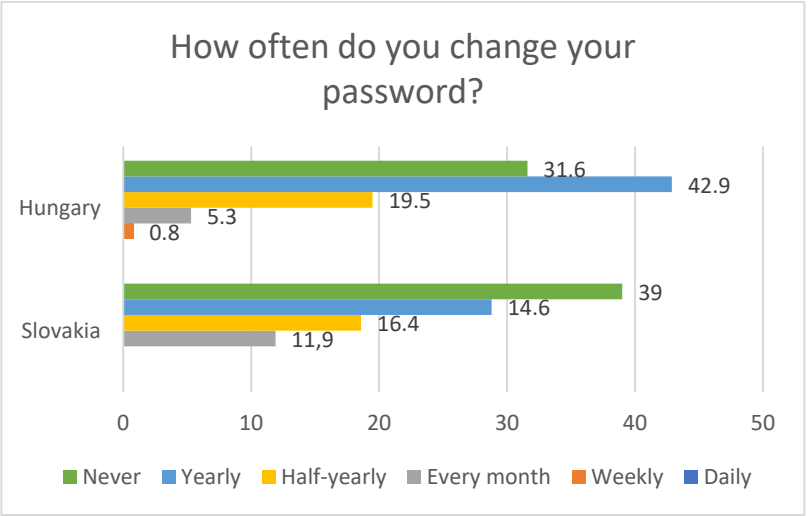


Figure 3: Frequency of password changes by participants in the survey in Hungary and Slovakia. (Source:Created by the author)

Figure 3. shows that (0.8%) of the participants in the survey in Hungary answered that they change their password on a weekly basis, (5.3%) change it every month, (19.5%) every semester and (42.9%) every year, (31.6%) answered that they never change their password. Median=5 U=1435 z= -0.206 p=0.837 r=0.018 In Slovakia, (11.9%) of survey participants answered that they change their password every month, and (16.4%) answered that they change their password every six months, (14.6%) answered that they change the password they use every year and (39%) answered that they never change the password they use. Median= U=331 z=-1.346 p=0.178 r=0.192

Password usage habits	**Hungary**		**Slovakia**	
	Freq.	**Perc.**	***Freq.***	**Perc.**
Password contains upper- and lower-case letters, numbers, and special characters.				
Yes	125	94%	35	59.3%
No	8	6%	23	39%
The password contains personal data.				
Yes	30	22.9%	20	33.9%
No	101	74.8%	38	64.4%
The password contains a meaningful word.				
Yes	69	51.9%	38	64.4%
No	64	48.1%	20	33.9%
Use the same password in several places.				
Yes	86	64.7%	40	67.8%
No	47	35.3%	18	30.5%

Table 5: *Password usage habits based on the responses of survey participants in Hungary and Slovakia. (Source:Created by the author)*

We can see that 125 (94%) of the participants in the survey in Hungary answered that they use a password that contains upper- and lower-case letters, numbers and special characters. Only 8 answered (6%) that the password they use does not contain ,,uppercase and lowercase letters", numbers and special characters. Median=1 U= 1249 z= -2.955 p=0.003 r= 0.268 30 (22.9%) of the survey participants answered that the password they use contains personal information and 101 (74.8%) answered that the password they use does not contain personal information. Median=2 U=1326 z= - 0.606 p=0.545 r=0.055 When asked if the password contains meaningful words 69 (51.9%) answered that the pass-

word they use contains meaningful words and 64 answered (48.1%) that it does not. Median= 2 U= 973 z= -3.169 p=0.002 r=0.288 When asked whether they use the same password in several places 86 (64.7%) answered that they use the same password in several places and (35.3%)of 47 answered no. Median=1 U=1463 z= -0.047 p=0.963 r=0.004 In Slovakia 35 respondents (59.3%) answered that they use a password that contains ,,uppercase and lowercase letters", numbers and special characters and 23 respondents (39%) answered no. Median=1 U=270 z= -2.640 p=0.008 r=0.377 When asked whether the password they use contains personal information 20 (33.9%) answered yes and 38 (64.4 %) answered that the password they use does not contain personal information. Median=2 U=249.5 Z=-3.108 p=0.002 r=0.444 When asked whether the password contains a meaningful word 40 (67.8%) answered that the password also contains a meaningful word (33.9%) answered no. Median=1 U=343.5 z=-1.316 p= 0.188 r= 0.188 In the survey 86 people (64.7%) answered yes to the question of whether they use the same password in several places and 47 (35.3%) answered that they do not use the same password in several places. Median=1 U=405.5 z=-0.137 p=0.891 r=0.019

Mann-Whitney U test

,,The Mann-Whitney U Test is a statistical test used to determine if 2 groups are significantly different from each other on your variable of interest." [18] ,, A significant level of 0.05 indicates a 5% risk of concluding that a difference exists when there is no actual difference."[19]

MANN-Whitney U test	**Hungary**	**Slovakia**
	P	**p**
The password contains upper- and lower-case letters, numbers and special characters.	0.003	0.008
The password contains personal data.	0.545	0.002
The password contains a meaningful word.	0.002	0.188
The same password used in several places.	0.963	0.891
The password changes.	0.834	0.178
The password length.	0.837	0.165

Table 6: A Mann Whitney U test result for password usage in Hungary and Slovakia. (Source:Created by the author)

We can see in (Table 6.) the Mann-Whitney U test in the case of password use when a meaningful word is used as a password, the p value in Slovakia is much higher than in Hungary.

CONCLUSIONS

We can say that based on the survey, the use of smart devices is popular in both Hungary and Slovakia as more than 98% of the participants answered that they use at least one smart device in both countries. As for password length, according to the survey, more people in Slovakia use passwords with 12 or more characters than in Hungary. When asked whether they use ,,upper and lower-case letters", numbers and special characters in the password, according to the survey in Hungary, more people use upper- and lower-case letters, numbers and special characters than in Slovakia. In the case of passwords fewer people use personal information in Hungary than in Slovakia. The Mann-Whitney U test shows that the p value in Slovakia is higher than in Hungary in the case of password use when a meaningful word is used as a password. On the basis of this we can say that people living in Slovakia are exposed to a greater risk of attacks than people living in Hungary. According to Kaspersky's report as to, how to create a strong password, it is important to pay attention to the following. For example the password should be at least 10-12 characters long, but the longer the password the better. It is important to avoid easily guessed passwords such as,,12345" password, since the password can be cracked in seconds by a ,,brute force" attack. It is important that the password contains lowercase and uppercase letters, numbers, special characters, as this makes it more difficult to crack the password[20]. According to Keeper's 2023 report a strong password consists of 16 characters and contains uppercase letters, numbers and special characters and does not contain personal information and the same password should not be used in multiple places [21]. The Americas Cyber Defense Agency (CISA) reports that using simple passwords is not secure, so you should never choose a password that can be easily guessed along with your date of birth as easy-to-guess passwords can be easily cracked [22]. One way for IoT devices to be protected is to use these hard-to-guess passwords [23]. In addition, it is very important to always change the default passwords on our IoT devices [24].

REFERENCE

[1] Dorottya Mandić, „Az okoseszközök veszélyei", Biztonságtudományi Szemle *5*:3, pp. 37–45, p. 9, 2023.

[2] Blessing, Elisha & Potter, Kaledio & Klaus, Hubert., „Security and Privacy in IoT: Considerations for securing IoT devices.", 2024, [Online]. Available: https://www.researchgate.net/publication/377853082_Security_and_Privacy_in_IoT_Considertions_for _securing_IoT_devices

[3] Kollár Csaba, „Társadalom és információbiztonság. A humán információbiztonság a digitális korban", International Research Institute, (2016) 488p.pp.189-194.,6p.. doi: 10.18427/IRI-2016-0023.

[4] Kollár Csaba „IoT a gyakorlatban, az információbiztonság fókuszában I.: Az IoT működése, fejlődési tendenciái", Bolyai Szemle 2017:1pp.41-54.,14p. (2017)

[5] X. Su, B. Wang, C. Choi, and D. Choi, „Case study on password complexity enhancement for smart devices", in 2017 *14*th IEEE Annual Consumer Communications &

Networking Conference (CCNC), Las Vegas, NV: IEEE, jan. 2017, p. 1–5. doi: 10.1109/CCNC.2017.8013419.

[6] S. A. Baho and J. Abawajy, „Analysis of Consumer IoT Device Vulnerability Quantification Frameworks", Electronics, 12(5), p. 1176, feb. 2023, doi: 10.3390/electronics12051176.

[7] R. J. and V. S. M., „Security Challenges Prospective Measures In The Current Status of Internet of Things (IoT)", in 2022 International Conference on Connected Systems & Intelligence (CSI), Trivandrum, India: IEEE, aug. 2022, p. 1–8. doi: 10.1109/CSI54720.2022.9923984.

[8] „Most common passwords used in Internet of Things (IoT) devices over a 45 day period worldwide in 2021". [Online]. Available: https://www.statista.com/statistics/1298495/frequently-seen-passwords-in-iot-devices/

[9] S. Sanaullah and B. Liu, „Information Security Challenges in the Internet of Things (IoT) Ecosystem", in 2022 International Symposium on Electrical, Electronics and Information Engineering (ISEEIE), Chiang Mai, Thailand: IEEE, feb. 2022, p. 124–129. doi: 10.1109/ISEEIE55684.2022.00029.

[10] D. Mandić and G. Kiss „Az okoseszközök és vírusvédelem használata Magyarországon és Szerbiában", 30th Anniversary conference of the safety and security enineering education: A biztonságtechnikai mérnök képzés 30évi jubileumi konferenciája, Budapest, Magyarország (2023) 127p. pp. 64-75.,12p., ISBN:9789634493297

[11] D. Mandić and J. Simon, „Biztonságosak-e az okosotthonokban használt okoseszközök",Biztonságtudományi Szemle 4:4pp.59-67.,9p(2022)

[12] K. Andras, „Life is Short. Have another Affair - Password Security", p. 121–130, 2015.

[13] „Top 200 most common passwords of the year 2019-2022". [Online]. Available: https://s1.nordcdn.com/nord/misc/0.78.0/nordpass/top-200-2023/200-most-common-passwords-en.pdf

[14] D. K. Davis, M. M. Chowdhury, and N. Rifat, „Password Security: What Are We Doing Wrong?", in 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA: IEEE, Maj 2022, p. 562–567. doi: 10.1109/eIT53891.2022.9814059.

[15] „How Secure Is My Password?" [Online]. Available: https://www.security.org/how-secure-is-my-password/

[16] „How Long Does It Take for a Hacker to Crack a Password?" [Online]. Available: https://tech.co/password-managers/how-long-hacker-crack-password

[17] „Most common passwords: latest 2024 statistics". [Online]. Available: https://cybernews.com/best-password-managers/most-common-passwords/

[18] „Mann-Whitney U Test". [Online]. Available: https://www.statstest.com/mann-whitney-u-test/#Assumptions_for_a_Mann-Whitney_U_Test

[19] „Interpret the key results for Mann-Whitney Test". [Online]. Available: https://support.minitab.com/en-us/minitab/help-and-how-to/statistics/nonparametrics/how-to/mann-whitney-test/interpret-the-results/key-results/

[20] „Internet of Things security challenges and best practices". [Online]. Available: https://usa.kaspersky.com/resource-center/preemptive-safety/best-practices-for-iot-security

[21] „What Makes a Strong Password?" [Online]. Available: https://www.keepersecurity.com/blog/2023/08/31/what-makes-a-strong-password/

[22]„Use Strong Passwords”. [Online]. Available: https://www.cisa.gov/secure-our-world/use-strong-passwords
[23]„Best Practices for IoT device security”. [Online]. Available: https://bytebeam.io/blog/iot-security-how-to-protect-your-connected-devices/
[24]„Best Practices in Securing Passwords for IoT Devices”. [Online]. Available: https://iotmktg.com/best-practices-in-securing-passwords-for-iot-devices/

BLOCKCHAIN-BASED IMPLEMENTATION FOR AUTOMOTIVE ENVIROMENT

BLOKKLÁNC ALAPÚ ALKALMAZÁS AUTÓMOBIL KÖRNYEZETRE[1]

NAGY Csaba Norbert[2] – OLÁH Norbert[3]

Abstract

Nowadays, the rapid development of the automotive industry poses new challenges for IT security and data management in vehicles. Numerous incidents (e.g. Kia and Tesla incidents) show the vulnerability of the vehicles. In our proposed solution, we have studied the automotive environment's characteristics, security features and requirements. We have designed a solution to enhance cyber resilience by using blockchain for secure identity and access management (permissioned blockchain, two-factor authentication) and distributed storage to store and manage data. Updating the software in cars is a critical point from the information security perspective. Our proposed implementation will alert the user of the release of new software updates (Over-the-Air), and the system components allow continuous updating of vehicle data, moreover, storage and validation of the user account password using smart contracts.

Keywords

IT security, Blockchain, Password management, Automative industry, Smart contracts

Absztrakt

Az autóipar gyors fejlődése új kihívásokat vet fel a járművek informatikai biztonságával és adatkezelésével kapcsolatban. Számos incidens mutatja az alkalmazott rendszerek sérülékenységét. Az általunk javasolt megoldásban az autómobil környezet jellemzőit, biztonsági sajátosságait és követelményeit tanulmányoztunk. Megoldást dolgoztunk ki a kiber-ellenálló képesség növelésére, amelyben blokklánc alkalmazásával biztonságos identitás- és hozzáférés-kezelést (engedélyköteles blokklánc, kétfaktoros hitelesítés) és elosztott tárolást dolgoztunk ki az adatok tárolása, kezelése érdekében. Az autók szoftvereinek frissítése kritikus pont információbiztonsági szempontból. Az általunk javasolt alkalmazás figyelmezteti a felhasználót az új szoftver frissítések megjelenéséről (Over-the-Air), a rendszer komponensei lehetővé teszik a gépjárművek adatainak folyamatos frissítését, továbbá a felhasználói fiók jelszavának tárolását és ellenőrzését okosszerződések alkalmazásával.

Kulcsszavak

IT Biztonság, Blokklánc, Jelszó menedzsment, Járműipar, Okosszerződések

[1] Jelen tanulmány az I. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencián, 2023.10.25-én elhangzott előadás szerkesztett változata.

[2] nagy.csaba@inf.unideb.hu | ORCID: 0009-0009-0678-281X | technician, University of Debrecen, Faculty of Informatics, Department of Data Science and Visualization| technikus, Debreceni Egyetem, Informatikai Kar, Adattudomány és Vizualizáció Tanszék

[3] olah.norbert@inf.unideb.hu |ORCID: 0000-0002-0007-8508| Assistant Professor, University of Debrecen, Faculty of Informatics, Department of Data Science and Visualization| adjunktus, Debreceni Egyetem, Informatikai Kar, Adattudomány és Vizualizáció Tanszék

BEVEZETÉS

Az autóipar digitalizációjának eredményeként a modern járművekben megjelenő különböző hardverekből és szoftverekből álló rendszerek számos egyezést mutatnak a dolgok internetének (IoT) rendszereivel mind felépítésben, mind működésben és az ezeket a rendszereket érő kihívásokban egyaránt. A járműipari digitalizáció így nem csak új lehetőségeket hozott magával, hanem új problémákat és felelősségeket is a gyártók és felhasználók számára. A járművek egyre komplexebbé válnak, amelyek a hétköznapi életünk központi részévé váltak a közlekedésben és a szállításban. Ahogy a hagyományos informatikai rendszerek és szoftverek is rendszeres frissítéseket igényelnek, úgy a modern járművek esetében is elengedhetetlen, hogy időben hozzáférjenek a szükséges szoftverfrissítésekhez a gyártóktól. Ezeket a frissítéseket gyakran hagyományos módon, szervizekben végzik el, de egyre népszerűbb az úgynevezett Over-the-Air (OTA) megoldás, melynek keretében az interneten keresztül továbbítják és telepítik a járművekbe a frissítéseket. Ugyanakkor ezt a technológiát a támadók is kihasználhatják, kártékony programok bejuttatásával, amelyek révén hozzáférhetnek a jármű rendszeréhez, személyes adatokat lophatnak, vagy akár az autó fizikai irányítását is átvehetik.

IT BIZTONSÁGI SÉRÜLÉKENYSÉGEK ÉS MEGOLDÁSOK A JÁRMŰIPARBAN

Az informatikai forradalom térhódításával a járműipar is átalakult, amely számos új kihívást és biztonsági problémát hozott magával. Ezen problémák közül jól mutatja a szoftverfrissítés hiányát a Kia incidense, ahol egy hiányzó szoftver modul miatt kialakult a közösségi médiaplatformon zajló úgynevezett "Kia Challenge". Ennek során a "Kia Boyz" néven ismert tolvajok oktatóvideókat tettek közzé arról, hogyan lehet kijátszani a járművek biztonsági rendszerét olyan egyszerű eszközökkel, mint egy USB-kábel. Az incidens számos autólopáshoz, 14 bejelentett súlyos balesethez és nyolc halálesethez vezetett. Ezen kívül biztonsági szakértők 16 autógyártó járműveiben (többek között Ferrari, BMW, Rolls Royce, Porsche) fedeztek fel sérülékenységeket, amelyek lehetővé tették az autó funkcióinak távoli vezérlését ([1]). A sérülékenységek között szerepelt továbbá, hogy a támadók kizárhatják a felhasználókat a távoli járműkezelésből vagy akár megváltoztathatják az autóhoz tartozó felhasználói fiókot, amely mutatja az autókhoz kapcsolódó hitelesítési mechanizmusok fontosságát. Emellett kiemelt a jelentősége annak, hogy az autók műszaki, technológiai paraméterei ma már a korábbinál jóval magasabb szinten állnak, ezáltal a tulajdonsoknak könnyebb elérni az aktuális információkat az autók állapotáról. Azonban számtalan esetben kerülnek ezen adatok meghamisításra, ami komoly bizalmatlanságot teremt például a használt autópiacon. A jelenlegi autóimporthoz használt szabályozások és keretek nem megfelelőek, sokszor hiányosak, amely indokolja erre a problémára egy transzparens és nem hamisítható rendszer kialakítását. A blokklánc tulajdonságai, mint a nyilvános főkönyv, a blokklánc elemeinek módosíthatatlansága vagy az adatok nagyobb rendelkezésre állásának biztosítása jól alkalmazható ezen problémára, amelyet demonstrál többek között az Alfa Romeo gyár, ahol már az egyes modelleknél NFT-ben rögzítik a jármű különböző adatait. A jármű adatainak tokenjéről tanúsítványt állítanak ki, melynek segítségével biztosítható, hogy az autót megfelelően karbantartották. Ez pozitív hatással lehet az autó marad-

ványértékére ([2]). A [3] cikkben egy megbízható, járművek adatait tartalmazó adatbázisrendszert javasoltak a szerzők, amely szintén blokklánc technológiát alkalmaz és az Ethereum platformra épül. A rendszer engedélyköteles láncot használ, melynek segítségével egy megbízható harmadik fél (pl. karbantartó üzem és kormányzati hivatal) rögzítheti a jármű adatokat a blokkláncra, így a járműadatok integritása megőrizhető és ellenőrizhető. A rendszer előnyei közé tartozik, hogy az ügyfelek könnyen lekérdezhetik a releváns járműinformációkat a rendszerfelületen keresztül és elkerülhetik, hogy hamis járműinformációkat kapjanak.

Mivel az autóipar komplex értéklánccal rendelkezik, ezért az információk pontossága és hitelessége alapvető fontosságú. Az autóalkatrészek gyártásától kezdve azok összeszerelésén át egészen a járművek értékesítéséig és karbantartásáig a blokklánc lehetőséget kínál a folyamatok ellenőrzésére és optimalizálására. A gyártók és a beszállítók közötti tranzakciók megkönnyítésétől kezdve a járművek történetének hiteles dokumentálásáig a blokklánc javíthatja az iparág átláthatóságát és csökkentheti a csalások kockázatát. Összegezve a blokklánc technológia alapvető tulajdonságait, mint az adatintegritás biztosítása, a transzparencia, az elosztottság, a decentralizált működés és a kriptográfiai primitívek garantálják az információk manipulálhatatlanságát növelve az ügyfelek és az iparág szereplőinek bizalmát.

BLOKKLÁNCCAL KAPCSOLATOS FOGALMAK

Az általunk javasolt autómobil környezetben alkalmazandó blokklánc alapú rendszer megértéséhez szükséges, hogy a hozzá kapcsolódó fogalmakat meghatározzuk.

Blokklánc

Egy peer-to-peer, elosztott főkönyv (distributed ledger), amelynek a biztonságát kriptográfiai primitívek garantálják, csak bővíthető művelettel rendelkezik (append-only), nem hamisítható és a résztvevők közötti konszenzus vagy megállapodás révén frissíthető. A blokklánc blokkok sorozata, melyeket kriptográfiai hash függvényekkel kötnek össze (hash-lánc), ezáltal a blokklánc teljes története megváltoztathatatlan (immutable). A hash függvény olyan algoritmus, mely egy tetszőleges hosszúságú bemeneti adatot egy fix hosszúságú karakterlánccá képez le. A hash függvény alapvető tulajdonsága az ütközésmentesség, a lavinahatás és az irreverzibilitás. A blokklánc egyes blokkjaiban lévő adatokat tranzakcióknak hívjuk, melyeket elosztottan, több csomópont tárol. A tranzakció egy a felek által digitálisan aláírt műveletek sorozata, amely a blokklánc főkönyvében kerül rögzítésre ([4]). A főkönyv egy adatbázis, amely tartalmazza az összes tranzakciót, amelyet a blokklánc hálózatában végrehajtottak. A decentralizáció az egyik legjelentősebb tulajdonsága a blokkláncnak, ahol nincs szükség megbízható harmadik félre vagy közvetítőre a tranzakciók érvényesítéséhez. A résztvevők a hálózaton keresztül időbélyegezik és ellenőrzik minden egyes tranzakciót. Résztvevőnek tekinthető minden olyan fél, aki tagja a blokkláncnak. ([5][6])

Ethereum

Az Ethereum (ETH) egy nyílt forráskódú, decentralizált blokklánc platform, amely okosszerződést (smart contract) használ. Az Ethereum hálózaton számos számítógép (node) működik és futtatja az Ethereum virtuális gépet (EVM), amely lehetővé teszi az Ethereum

állapotgépének folyamatos, megszakítás nélküli és változatlan működését, valamint az okosszerződések futtatását. A konszenzus mechanizmus biztosítja, hogy az összes csomópont ugyanazon az állapoton dolgozzon, és elfogadja az egyetlen, hiteles változatot az állapotról. Ezáltal lehetséges az egyének közötti konszenzus megvalósítása. Aki részt vesz az Ethereum hálózatban, annak egy másolattal kell rendelkeznie az EVM állapotáról, ezen felül bárki küldhet kérést az EVM részére, hogy tetszőleges számításokat végezzen rajta. Ilyen fajta kérések esetében a hálózat többi résztvevőjének ellenőrizni, validálni és végrehajtani kell a kért számításokat. A számítási kéréseket tranzakciós kéréseknek nevezzük, ahol az összes tranzakció és az EVM állapotának nyilvántartása mind a blokkláncon szerepelnek, amelyet az összes csomópont elosztva tárol és egyeztet. A platform natív kriptovalutája az Ether. A Bitcoin (BTC) után az Ethereum a második legnagyobb és legaktívabban használt kriptovaluta a piacon, egy pont-pont (peer-to-peer) hálózat, ahol a csomópontok konszenzus mechanizmus segítségével működtetik a blokkláncot. Az Ethereumra jellemző a Turing teljesség, ami Alan Turing által meghatározott fogalom. A Turing teljesség magába foglalja, hogy egy adott számítási rendszer vagy modell képes szimulálni bármely más számítási modellt vagy rendszert. Egy számítási modell csak akkor tekinthető Turing teljesnek, ha képes szimulálni minden olyan algoritmust, amely végrehajtható egy Turing-gépen. ([4][5])

Konszenzus mechanizmus

A konszenzusmechanizmus olyan lépések összessége, amelyeket a blokklánc legtöbb vagy összes csomópontja tesz annak érdekében, hogy megállapodjon egy javasolt állapotról vagy értékről. Az Ethereum konszenzus mechanizmust használ, ami 2022 előtt a PoW (Proof-of-Work) volt azonban napjainkban már a PoS (Proof-of-Stake) használatos ([4]). A mechanizmus cserére azért volt szükség, mert a PoS gazdasági szempontból biztonságosabb, hatékonyabb és kevesebb erőforrást igényel, mint a PoW mechanizmus. A konszenzus mechanizmusban azok a résztvevők játszanak kulcsszerepet a hálózat integritásának és biztonságának fenntartásában, akik jelentős mennyiségű Ethereum tokent letétbe helyeznek. Ezzel biztosítják, hogy a hálózaton belüli döntéshozatalban és tranzakciók validálásában a legtöbb tokent birtokló résztvevőknek legyen a legnagyobb befolyásuk, miközben rosszindulatú cselekvés esetén a bizalom megrendülhet és a letétbe helyezett tokenjeik elértéktelenedhetnek. Az Ethereum hálózatán belül a legtöbb tőkével rendelkező résztvevők nagyobb érdekeltséggel rendelkeznek a hálózat biztonsága és fenntarthatósága iránt. Ennek következtében kevésbé valószínű, hogy rosszindulatúan viselkednek, vagy kárt okoznak a hálózatban. Míg a PoW-alapú rendszerekben a támadások jelentős számítási erőforrásokat igényelnek, a PoS mechanizmusoknál a támadások nagyarányú token letétbe helyezését követelik meg, ami különböző kockázatokat és költségeket jelent a támadók számára. Az Ethereum platform fejlesztői eszköztárban található tesztkörnyezet alapvetően a PoW konszenzus mechanizmust alkalmazza. Ugyanakkor az Ethereum Virtual Machine (EVM) strukturális kialakítása kínál egy integrált keretet, melyben az Ethereum Client másnéven Ethereum Validator szerepel. Ez a kliens magában foglal egy Execution Engine-t, amely a tranzakciók megfelelő futtatását garantálja, illetve a Beacon Node-ot, amely a konszenzus mechanizmus koherens végrehajtásért felelős. Az Ethereum platform jellegzetes rugalmasságának köszönhetően a fejlesztők képesek testre szabni a tesztkörnyezetet úgy, hogy többféle konszenzus mechanizmus közül kiválasztják a legoptimálisabbat a projekt igényeinek megfelelően.

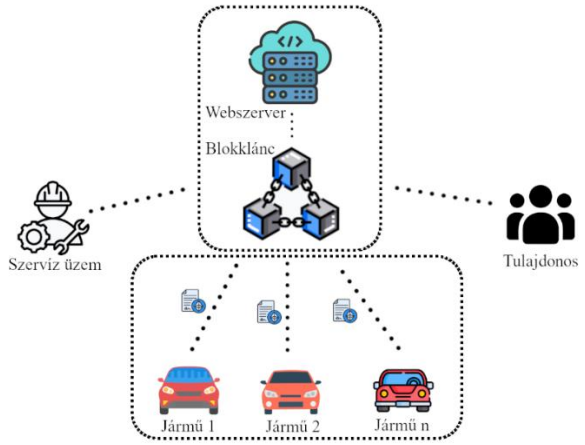
Okosszerződés

Az okosszerződés egy önmagát végrehajtó számítógépes program, amely képes vizsgálni az adott szerződés feltételeinek teljesülését a felek között. Ezek a szerződések sok esetben blokklánc technológián alapulnak, amely egy biztonságos és decentralizált környezetet biztosít a tranzakciók végrehajtásához és tárolásához. Az EVM az Ethereum blokklánc egy olyan alapvető technológiája, amelynek fontos szerepe van okosszerződéseken. Ez a virtuális környezet lehetővé teszi, hogy a blokkláncon tárolt szerződések végrehajthatók legyenek az Ethereum hálózaton. Az EVM pontosabban egy biztonságos futtató környezet, amely garantálja a kódok megbízható végrehajtását, mindeközben kihasználja a blokklánc előnyeit. Széleskörű felhasználási lehetőséget kínálnak, beleértve a pénzügyi tranzakciókat, a beszerzési láncok kezelését vagy a felhasználók profiljához tartozó adatok ellenőrzését. Az okosszerződések elosztott számítógépes programok, amelyek tartalmazzák a szabályokat és a feltételeket. Ha a feltételek teljesülnek a szerződés automatikus végrehajtja az intézkedéseket anélkül, hogy emberi beavatkozásra vagy harmadik felek bevonására lenne szükség. Mivel az okosszerződés blokkláncon működik, így megváltoztathatatlanok és manipulálhatatlanok a kriptográfiai primitíveknek köszönhetően, ezáltal a szerződés feltételei is ugyanezeket a tulajdonságokat örökli. Az EVM-en futtatott okosszerződések gyakran a Solidity programozási nyelvvel készülnek, de léteznek más nyelvek is, mint például a Vyper, Bamboo vagy Serpent, amelyeket szintén használnak Ethereum okosszerződések készítéséhez, ezáltal megvalósulhat az Ethereum blokkláncra való fejlesztés. ([4][7])

JAVASOLT KERETRENDSZER

A járműiparban újonnan megjelenő és a használt autópiacon folyamatosan növekvő számú autómobilokra kidolgoztunk egy olyan keretrendszert, amely képes az adott járműhöz tartozó összes szenzitívnek tekinthető fizikai (kilométeróra állás, alváz szám, hengerűrtartalom, teljesítmény, jelenlegi állapot, előélet) és logikai (szoftver/firmware azonosító, beépített szenzorok által mért adat, biztosítás, diagnosztika által mért adat) attribútumok kezelését, továbbítását és tárolását megvalósítani blokklánc technológia segítségével. Járművek sokasága alkotják az általunk felügyelni kívánt környezetet. Minden autómobilról külön-külön képesek vagyunk az attribútumaikat okosszerződések segítségével kezelni és továbbítani blokkláncra. Ebben az esetben minden jármű egy csomópontnak felel meg és az EVM segítségével képesek vagyunk az okosszerződések kezelésére. A blokkláncot adattárolás szempontjából tartjuk fontosnak emellett teljesíti a megkövetelt bizalmasság (engedélyköteles), integritás és rendelkezésre állás tulajdonságait. A tulajdonos, a szervizműhely, a webszerver és a blokklánc közötti kommunikációhoz TLS (Transport Layer Security) protokollt alkalmazunk. Az adatok és a rendszer integritása érdekében több kriptográfiai primitívet implementálunk, mint például a digitális aláírás és az SHA-256 hash függvény. Az elosztott alkalmazások (DApp) és tárolás nagyobb rendelkezésre állást biztosít emellett a keret kialakítása során figyeltünk a skálázhatóságra (a felhasználó tetszőleges számú autót kezelhet). A letagadhatatlanság szerepet játszik a felhasználók és a tárolt adatok transzparenciája és nyomonkövethetőség érdekében. Az engedélyköteles blokklánc alkalmazása lehetővé teszi az adatokhoz való hozzáférést a jogosult és hitelesített felhasználók számára. Az adatokat titkosítva tároljuk elosztott módon az AES-GCM szimmetrikus blokktitkosítási algoritmus segítségével. Az elosztott tárolásnak a csalások és egyéb kompromitálások

(ransomware támadás) esetében kialakult adatveszteség és az egyszerű visszaállíthatóság érdekében van meghatározó szerepe. Így a tulajdonosok közül csakis azok férhetnek hozzá a tárolt attribútumokhoz, akik rendelkeznek a visszafejtéshez szükséges kulccsal, vagyis csak a jármű tulajdonosa férhet hozzá a saját járműve adataihoz. A webszerver az általunk elkészített járműkezelő felületet valósítja meg egy felhasználóbarát platform keretein belül. A webszerver semmilyen adatot nem tárol, csakis a járműadatokhoz való egyszerű hozzáférhetőséget és módosítások menedzselését teszi lehetővé a tulajdonos és szervizműhelyek számára. Kétfaktoros hitelesítést alkalmazunk, ahol az első faktor esetében a felhasználónak blokklánc fiókkal kell rendelkezni és ez által tagjának kell lennie az adott láncnak (felhasználó név és jelszó páros), majd a második faktor a járműkezelő felülethez való csatlakozást megelőzően egy a felület által generált OTP (One Time Password) megadásával képes hozzáférni a felülethez.



1. Ábra: Blokklánc alapú alkalmazás autómobil környezetre, saját szerkesztés.

ÖSSZEHASONLÍTÁS

A tudományos irodalomban és gyakorlati megvalósításokban több blokklánc alapú megoldást is javasoltak a használtautó piacra. A [8] cikkben bemutatott megoldás az általunk javasolt rendszerhez hasonló célokat valósít meg, ahol kiemelt hangsúlyt kap a használt autók adatintegritása és átláthatósága. Figyelembe veszik az általunk is alkalmazni kívánt eladók és vevők szempontjait egy új vagy használt autó vásárlása esetén. Dél-Koreában a használt autó piac mérete és az autók tranzakciójának száma folyamatosan nő. Ezen a piacon gyakran előfordulnak mulasztások az eladó és a vevő közötti információ aszimmetria miatt. A [8] tanulmányban egy használt autó tranzakciókezelő rendszert javasolnak, amely a nyilvános blokklánc Ethereumon alapuló okosszerződések segítségével garantálja a megbízhatóságot harmadik felek beavatkozása nélkül. A nyilvános blokkláncot a használt autó tranzakciókezelő rendszerben alkalmazták az autók információjának megbízhatósága alapján egy biztonságos és megbízható tranzakciókezelő rendszer tervezésére. Az okosszerződéseket a használt autó kereskedési szerződések tervezésére (adásvételi szerződés) és adat továbbításra használták. A rendszer csökkenti az információ aszimmetriát a vevők és az eladók között a blokklánc integritása és átláthatósága révén. Az adattároláshoz az IPFS-t

(InterPlanetary File System) használták, ahol hash értékeket adtak vissza az okosszerződésekben, amelyeket egy Mongo adatbázison alapuló Node.js szerverben tároltak. Amikor egy új autó eladására kerül sor, a tulajdonos egy böngészőn keresztül fér hozzá a platformhoz, ahova képes manuálisan feltölteni a járműhöz tartozó adatokat. Ezek az adatok átmenetileg a Mongo adatbázisban kerülnek tárolásra, majd okosszerződések segítségével lesznek véglegesítve a blokkláncon. A Korea Fogyasztói Ügynökség szerint a használt autók károk miatti kárelhárítási kérelmek száma csökken, de a használt autók teljesítményének és állapotának ellenőrzési aránya növekszik. A használt autó tranzakciók okozta károk 80%-a hamis információk miatt keletkezik. A használt autó kereskedelmi rendszer átfogó sémája hét entitásból áll: vásárló, bankokkal társított partnercég, használt autó, javítással kapcsolatos partnercég, használt autóértékesítési cégek, munkaadók és munkaadókat kezelő entitás.

A [9] cikkben az általunk alkalmazni kívánt technológiákat és védekezési mechanizmusokat gyűjtötték össze. A járműpiac az emberi civilizáció egyik legnagyobb gazdasági ágazata. Ez egy létfontosságú és folyamatosan változó piac, amelynek közvetlen hatása van az emberi életre, a biztosítási társaságokra, a kormány költségvetésére, a nyereségre és a költségekre. Problémát jelentenek a kilométer óraállás manipulációja a javítóműhelyek és az autókereskedések által, mivel a járműtörténeti nyilvántartások papíralapúak így elveszhetnek vagy károsodhatnak. Továbbá ezek a nyilvántartások megváltoztathatóak és manipulálhatóak, amely komoly aggodalomra ad okot és évente körülbelül 5,6 és 9,6 milliárd eurós kárt okoz az európai fogyasztóknak. A használt járműpiac csalásmegelőzésére számos javaslatot tettek, mint például a használt járművek valóságos árainak automatizálása statisztikai adatok alapján és gépi tanulási technikák alkalmazásával (k-legközelebbi szomszéd algoritmus, naiv Bayes osztályozó), illetve sokan az óraállás csalások megelőzésére összpontosítottak statisztikai adatokat figyelembe véve. Az eddigiekben tárgyalt megoldások többsége statikus jármű adatok kezelést elemeztek, azonban nem vették figyelembe a dinamikus jármű adatok kezelését, továbbítását és tárolását, illetve hogyan lehet ellenőrizni az adatok érvényességét és hitelességét. 2017-ben a Renault csoport és a Microsoft csapat közreműködésük során megalkották az első digitális autókarbantartási könyv prototípusát ([10]). 2019-ben VINChain projekt ([11]) egy blokklánc alapú megoldást javasolt a járművekre vonatkozó adatok elosztott tárolására. 2019-ben a Car-Vertical projekt esetében az autóhoz tartozó állapot adatokat tárolták, mint például kilométer óraállás, márka, totálkár azonban az autó szervízelésével kapcsolatban nem tároltak adatokat. 2017-ben Chanson egy rendszert javasolt a kilométer óraállás manipuláció megelőzésére, ahol a blokkláncot, mint adatvédelmi eszközt használja ([12]). A rendszer rögzíti az autó kilométeróráját és GPS adatait egy dongle (hardverkulcs) segítségével és rögzíti azokat az Ethereum blokkláncra. Egy alkalmazás az eszközön belül fogadja az adatokat Bluetooth segítségével, majd elküldi az adatok hash értékét. Az adatokat a felhasználó privát kulcsával írják alá az Ethereum blokkláncon. Az alkalmazás titkosítja az adatkészletet és elküldi egy privát, biztonságos felhő adatbázisba.

Míg az [8] és [9] tanulmányok különböző technológiákat és megközelítéseket alkalmaznak, és néhány adatot vagy nem tárolnak, vagy csak bizonyos esetekben, saját rendszerünk egy átfogó, integrált megoldást kínál a járművek összes releváns adatának tárolására, az elosztott tárolási és alkalmazási lehetőségekkel kombinálva. Ezzel nem csak a járműpiac adatintegritásának és átláthatóságának növelését célozzuk meg, hanem a rendszer teljes körű biztonságát és megbízhatóságát is. A [8] megoldásban előnyként emelhető ki a

tárgyalt keretrendszer tesztkörnyezetben alkalmazott megvalósítása, hiszen valós környezetben láthatóak a rendszer erősségei és esetleges hiányosságai, így növelhető a felhasználói élmény a visszajelzések alapján. Ezentúl a rendszer csökkenti a vevők és az eladók közötti információ aszimmetriát. Azonban a publikus blokklánc alkalmazása jogosulatlan felek közbeavatkozását teszi lehetővé, ami befolyásoló tényező lehet az adatok integritásának megőrzése érdekében. Emellett az okosszerződések sokkal több funkciót látnak el, ami a fejlesztők számára nehézségeket jelenthet esetleges problémák megelőzése vagy helyreállítása esetén. A [9] cikkben több alkalmazott technológiáról olvashatunk, amelyek mindegyike külön-külön egy jól működő, adott területet lefedő alkalmazás. Hátrányként emelhető ki, hogy a technológiákról együttesen nem készült egy összefogó implementáció, ami egy jól kidolgozott keretrendszerhez vezet. Az általunk javasolt keretrendszer előnyei közé tartozik a kidolgozott és már alkalmazható implementáció, ami blokklánc alkalmazásával a biztonságos identitás- és hozzáférés- kezelést, illetve az elosztott tárolást, alkalmazást és az adatok tárolását, kezelését valósítja meg. Azonban további kutatási célként megfogalmazva, a hátrányok közé soroltuk a saját rendszerünkben a kulcsmegosztással kapcsolatos felmerülő hatékonyabb protokoll létezését a szervizműhelyek és az autótulajdonosok között. Az 1-es táblázatban az általunk javasolt rendszer előnyeit és hátrányait vetettük össze a [8] és [9] tanulmányban felsorolt megoldásokkal.

A feldolgozott megoldások mindegyikénél fontos szempont volt az információ aszimmetria csökkentése és a transzparencia növelése és a felhasználó barát alkalmazás megvalósítása. Azonban eltérések mutatkoznak a rendszerek között, mint például a járművekhez tartozó adatok feldolgozási módja, a blokklánc technológia és alkotó elemeinek alkalmazási módja és a biztonsági követelmények teljesülése.

Tanulmányok	Előnyök	Hátrányok
Seung Gyun Yoo, Byeongtae Ahn [8]	• Tesztkörnyezetben alkalmazott rendszer Dél-Korea térségében • Információ aszimmetria csökkentése • Transzparencia.	• Publikus blokklánc • Okosszerződések nem megfelelő alkalmazása
Sara El-Swtiti, Mohammad Qatawneh [9]	• Alkalmazott technológiák részletes elemzése	• Nincs összefogó kidolgozott implementáció
Általunk javasolt megoldás	• Kidolgozott és alkalmazható rendszer • Engedélyköteles blokklánc • Elosztott adattárolás és alkalmazás	• Nincs hatékony kulcsmegosztás a szervizműhelyek és a felhasználó között • Még nem alkalmazott tesztkörnyezeten kívül

1. Táblázat: Alkalmazott rendszer összehasonlítása, saját szerkesztés.

ÖSSZEFOGLALÁS

A cikkben feltérképezésre kerültek az autóipar digitalizációjának nehézségei és egy transzparens engedélyköteles blokklánc alapú rendszert javasoltunk ezen problémák kezelésére. Figyelembe vettük a tudományos és gyakorlati blokklánc alapú megoldásokat a használt autó piacon. Emellett kifejtésre kerültek a szükséges fogalmak és kapcsolódó technológiák, amely egy általunk javasolt keretrendszer alkalmazásához szükségesek. Végezetül összehasonlítást végeztünk a rendszerünk és a több tudományos irodalomban javasolt megoldás között, ahol kiemeltük a kapcsolódó előnyöket és a hátrányokat egyaránt. Célunk a kiber-ellenálló képesség növelése, a transzparencia és a csalások csökkentése a használtautó-piacon. A későbbi kutatási cél, hogy továbbfejlesszük a javasolt rendszert és kibővítsük egy hatékonyabb kulcsmegosztással a szervizműhely és az autótulajdonos között.

FELHASZNÁLT IRODALOM

[1] Curry S., “Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More” in *Samcurry.net*, 2023. [Online] Elérhető: https://samcurry.net/web-hackers-vs-the-auto-industry/

[2] Vitelaru E., & Persia L., *Fractional Vehicle Ownership and Revenue Generation Through Blockchain Asset Tokenization.* Transport and Telecommunication Journal, 24(2), 120-127, 2023.

[3] Jiang, Y. T., & Sun, H. M., *A blockchain-based vehicle condition recording system for second-hand vehicle market.* Wireless Communications and Mobile Computing, 1-10, 2021. [Online] Elérhető: https://doi.org/10.1155/2021/6623251

[4] Ethereum, 2023. [Online] Elérhető: https://ethereum.org/en/developers/docs/intro-to-ethereum/

[5] Bashir I., *Mastering Blockchain*. Packt Publishing Ltd. Birmingham, 2020.

[6] Md Ashraf Uddin, *Introduction to Blockchain Technology*. Federation University Australia, Jagannath University, pp. 1-2, 4, 14-20, 2021. [Online] Elérhető: https://www.researchgate.net/publication/356784725

[7] Zheng G., Gao L., Huang L. & Guan J., *Ethereum Smart Contract Development in Solidity*, 2021. [Online] Elérhető: https://books.google.hu/books?id=OGn6DwAAQBAJ&lpg=PR7&ots=_g2xRs3S7I&dq=smartcontract%20and%20solidity&lr&hl=hu&pg=PA3#v=onepage&q&f=false

[8] Yoo G. S.& Ahn B., *A study for efficiency improvement of used car trading based on a public blockchain.* The Journal of Supercomputing, 2021. [Online] Elérhető: https://doi.org/10.1007/s11227-021-03681-z

[9] El-Switi S. & Qatawneh M., *Application of Blockchain Technology in Used Vehicle Market: A Review*. International Conference on Information Technology (ICIT), 2021. [Online] Elérhető: https://www.researchgate.net/publication/353488375

[10] Automotive World, *Groupe renault teams with Microsoft and Viseo to create the first-ever digital car maintenance book prototype*. 2017. [Online] Elérhető: https://www.automotiveworld.com/news-releases/groupe-renault-teams-microsoft-viseo-create-first-ever-digital-car-maintenance-book-prototype/

[11] Vinchain, *Decentralized Vehicle History — Car Accident History Check by VIN*. 2019. [Online] Elérhető: https://vinchain.io

[12] Chanson M., Fleisch E., Bogner A. & Wortmann F., *Blockchain as a privacy enabler: an odometer fraud prevention system*. ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers. 2017. [Online] Elérhető: https://www.researchgate.net/publication/319602303

PÁLYÁZATRA UTALÓ MEGJEGYZÉS

A KULTURÁLIS ÉS INNOVÁCIÓS MINISZTÉRIUM ÚNKP-23-1 KÓDSZÁMÚ ÚJ NEMZETI KIVÁLÓSÁG PROGRAMJÁNAK A NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS ALAPBÓL FINANSZÍROZOTT SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.

CRITICAL INFRASTRUCTURE FOR FUTURE-PROOFNESS

A JÖVŐBIZTOS KRITIKUS INFRASTRUKTÚRA

PÁL Anita[1]

Abstract

In recent years, critical infrastructures such as energy supply, water supply and transport networks have increasingly become dependent on IT systems and digital communication, which has significantly increased their vulnerability to cyber threats and technological errors. The application of AI in critical infrastructure cancer opens up new opportunities for increasing operational efficiency, early detection of threats and rapid response, but at the same time it also raises ethical dilemmas, such as autonomous decision-making and the lack of human supervision. The article highlights that the protection of critical infrastructure requires not only national, but also international cooperation in the fight against cyber threats, and that the stability and security of modern societies is closely related to the effective protection of critical infrastructures, which is essential for future challenges in treatment..

Keywords

Artificial Intelligence (AI), Critical Infrastructure Protection, Cyber Security, Industry 5.0, Digital Dependence, Security-Political Instability

Absztrakt

Az elmúlt években a kritikus infrastruktúrák, mint az energiaellátás, a vízellátás és a közlekedési hálózatok, növekvő mértékben váltak függővé az informatikai rendszerektől és a digitális kommunikációtól, ami jelentősen növelte ezek sérülékenységét a kiberfenyegetésekkel és technológiai hibákkal szemben. Az MI alkalmazása a kritikus infrastruktúrákban új lehetőségeket nyit meg az operatív hatékonyság növelésére, a fenyegetések korai felismerésére és a gyors válaszadásra, ugyanakkor etikai dilemmákat is felvet, mint az autonóm döntéshozatal és az emberi felügyelet hiánya. A cikk kiemeli, hogy a kritikus infrastruktúra védelme nem csupán a nemzeti, hanem a nemzetközi összefogást is igényli a kiberfenyegetések elleni küzdelemben, valamint hogy a modern társadalmak stabilitása és biztonsága szorosan összefügg a kritikus infrastruktúrák hatékony védelmével, ami elengedhetetlen a jövő kihívásainak kezelésében.

Kulcsszavak

Mesterséges intelligencia (MI), Kritikus infrastruktúra védelme, Kiberbiztonság, Ipar 5.0, Digitális függőség, Biztonságpolitikai instabilitás

[1] pal.anita@phd.uni-obuda.hu | ORCID: 0000-0003-4750-193X | PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

A JÖVŐBIZTOS KRITIKUS INFRASTRUKTÚRA: AZ MI SZEREPE A VÉDELEMBEN ÉS STABILITÁSBAN

A 21. század küszöbén az infrastruktúrák biztonsága és sebezhetősége kiemelkedő fontossággal bír a modern társadalmakban. Az egyre összetettebbé váló infrastruktúrák digitális függősége növeli a kibertámadások és technológiai hibák kockázatát, amelyek visszafordíthatatlan gazdasági, társadalmi és biztonságpolitikai instabilitást okozhatnak. A kritikus infrastruktúra védelme kulcsfontosságú a biztonsági percepció működésének szempontjából. A mesterséges intelligencia és az új kibertéri fegyverek megjelenése új dimenziókat nyitottak a kiberbiztonságban és a védelemben. A digitális támadások aszimmetrikus jellege és pusztító ereje arra sarkall, hogy prioritásként kezeljük a kritikus infrastruktúra elleni védelmet és a megelőzést.

Az informatikai forradalom hatása a kritikus infrastruktúrára

Az informatikai forradalom, különösen az elmúlt évtizedekben, forradalmi változásokat hozott a társadalmainkban és gazdaságainkban. Az információs technológia térnyerése és az internet elterjedése gyökeresen átalakította a világ működését. Az információs forradalom ugyanakkor létrehozta az infrastruktúra sebezhetőségeinek új dimenzióját is. Az egyre összekapcsoltabbá váló és kölcsönös függőségen alapuló világban a kritikus infrastruktúra elemei fokozottan függenek az informatikai rendszerektől és az adatoktól. Ezáltal a digitális fenyegetések és a kiberbiztonság kérdései létfontosságúvá váltak. Így ebben a kontextusban, a mesterséges intelligencia megjelenése új lehetőségeket kínál a kritikus infrastruktúra működésének javítására, valamint a veszélyek korai felismerésére. Ugyanakkor alkalmazása új kihívásokat vet fel az adatvédelem, az etika és az emberi beavatkozás kérdéseiben.

A globalizáció és a technológiai fejlődés erőteljesen összefonódott, és ezek közös hatásaiban létrejöttek a hálózat és az Ipar 5.0 koncepciói. Az 5G (ötödik generációs) hálózat a legújabb és leggyorsabb mobilkommunikációs technológia, amely kiemelkedő sebességet, alacsony késleltetést és nagy adatkapacitást kínál. A globális összekapcsoltság és az adatok gyors és nagy mennyiségű átvitele révén az 5G lehetővé teszi az új technológiák, mint például a dolgok internete (IoT) széleskörű alkalmazását. Az Iparban megjelent 5.0 egy paradigmaváltást jelent, amely elmossa a határokat a digitális és a fizikai világok között. Az 5G és az Ipar 5.0 egymást erősítik, mivel az 5G kiterjedt hálózati kapacitása és az alacsony késleltetés lehetővé teszi a gyors és pontos adatátvitelt, amely elengedhetetlen az Ipar 5.0 alkalmazásaihoz. Komplexitása miatt ezen hálózatok kezelése nem képzelhető el kognitív funkciók és a mesterséges intelligencia használata nélkül.[1]

Az Internet of Things (IoT) egy dinamikus globális információs hálózat, amely olyan eszközökből áll, amelyek mind rendelkeznek internetkapcsolattal. Ezek az eszközök olyan rádiófrekvenciás azonosítókból, érzékelőkből és hajtóerőkből állnak, amelyek az internet elválaszthatatlan részét képezik. Így az elmúlt évek során egyre több olyan megoldás jelent meg az iparági piacokon amelyek között széles körben alkalmazták a kontextus-érzékeny technológiai szempontokat. A kontextus-érzékeny technológiai szempontok olyan faktorok és elemek, amelyek figyelembe veszik és reagálnak a környező kontextus vagy környezet változásaira, hogy javítsák a rendszer teljesítményét, alkalmazkodhassanak a körülményekhez és növeljék a felhasználói élményt.[2]

Az ipari szolgáltatások prioritásának megváltozásával felgyorsult az IoT (Internet of Things) bevezetése a COVID-19 járvány idején. A kedvezőtlen körülmények hatására bekövetkezett digitalizáció rugalmasabbá és változatosabbá tette az életfontosságú infrastruktúrák fontosságát.[3]

Azonban ezek a technológiai fejlesztések, különösen az 5G, egyben sérülékenyebbé is tehetik a kritikus infrastruktúrát. A nagyobb függőség az 5G és az Ipar 5.0 terjedésével, növeli a digitális támadások iránti kockázatok lehetőségét. A kritikus infrastruktúrák, mint például az energiaellátás, a víz- és élelmiszer-ellátás, az egészségügyi rendszerek, az adatközpontok stb., szorosan kapcsolódnak az informatikai rendszerekhez és az 5G-hez. A támadók kihasználhatják a sebezhetőségeket azáltal, hogy az 5G és az Ipar 5.0 rendszereket célzottan támadják, ami komoly következményekkel járhat a társadalom és a gazdaság számára, mint ahogy azt a Stuxnet esetében is láthattuk, ahol egy célzott ipari támadásról volt szó, amely főként a nukleáris erőművek vezérlőrendszereit célozta meg. A megfelelő védelem és kiberbiztonsági intézkedések elengedhetetlenek az ilyen típusú fenyegetések leküzdéséhez és a kritikus infrastruktúra biztonságának megőrzéséhez.

Mi számít kritikus infrastruktúrának?

Az infrastruktúrák, különösen a kritikus infrastruktúrák, a társadalmunk meghatározó pillérjeit képezik. A szóban forgó rendszerek és létesítmények, mint például az energiaellátás, vízellátás, közlekedési hálózatok és kommunikáció, nem csupán a mindennapi életünk zavartalan működéséhez szükségesek, hanem az országok gazdasági stabilitását és nemzetbiztonságát is alapvetően meghatározzák. Ha ezek a rendszerek meghibásodnak vagy támadás éri őket, akár az élet és halál kérdése is felmerülhet.

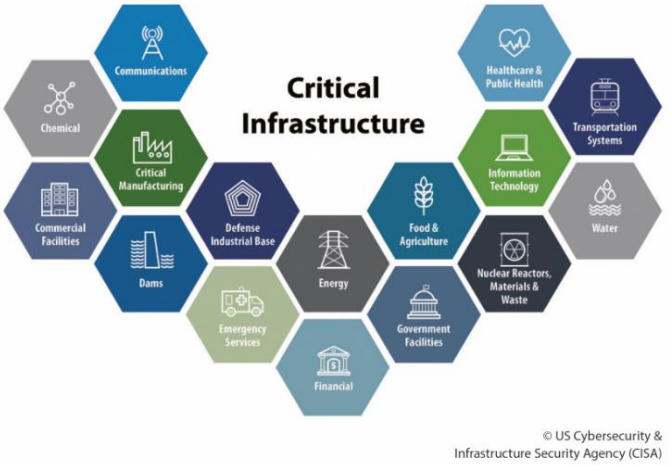
A kritikus infrastruktúra különböző ágazatokat ölel fel, például az energiaellátást (villamosenergia-termelés, gáz- és olajellátás), a víz- és hulladékgazdálkodást, a közlekedést (vasút, közút, légi közlekedés), az információs és kommunikációs rendszereket, valamint a pénzügyi és egészségügyi szektorokat. Nem csak a mindennapi élet alapvető pillérei, hanem az országok gazdasági stabilitásának és nemzetbiztonságának is kulcsfontosságú elemei. Ezeknek a rendszereknek a meghibásodása vagy támadás alá kerülése komoly veszélyeket jelent a társadalom számára.

A kritikus infrastruktúrák meghatározása és védelme bonyolult feladat, különösen a technológiai fejlődés és a digitális világ folyamatos változása miatt. Kihívást jelent meghatározni, hogy mely rendszerek és létesítmények számítanak létfontosságúnak, és hogyan kezeljük az új típusú kihívásokat, mint az aszimmetrikus hadviselés és a kibertér adta fenyegetések.

Az elengedhetetlen rendszerek határainak meghatározása a társadalom zavartalan működésének védelmét célozza meg, és folyamatosan változik a technológia fejlődésével.

Az alapvető szükségleteinket kielégítő infrastruktúrák védelme számos tényezőtől függ. Ide tartoznak azok a létesítmények, amelyek biztosítják a hozzáférést az ivóvíz-szolgáltatáshoz, a villamosenergia-ellátáshoz, a digitális szolgáltatásokhoz, a közösségi közlekedéshez, vagy az egészségügyi ellátáshoz. A negyedik ipari forradalom küszöbén az egyik legösszetettebb kérdéskört talán az lengi körbe, hogy a digitalizáció gyors fejlődési üteme által generált új típusú kihívások, az aszimmetrikus hadviselés és a kibertér adta "lehetőségek" közötti határvonal elmosódása miatt hol húzódik meg az a határ, ami garantálni tudja

a mindennapok zavartalanságát biztosító rendszerek védelmét. Felmerül a kérdés, hogy ezeket a határvonalakat milyen szempontok alapján strukturáljuk, vagy hogy szükség van-e szigorúbb előírásokra? A válasz mindig attól függ, hogy mi teszi a társadalom működéséhez nélkülözhetetlen rendszereket valóban elengedhetetlenné, létfontosságúvá vagy kritikussá.[4]



1. Ábra: Critical Infrastructure Security Guide: Understanding and Securing our Nation's Critical Infrastructure
Understanding and Securing our Nation's Critical Infrastructure (valentisinc.com)

A terminológia kérdése is felmerül, amikor a kritikus infrastruktúráról illetve annak megkülönbözőségéről beszélünk. Az általánosabban elfogadott "kritikus infrastruktúra" mellett vannak olyan fogalmak, mint a "létfenntartó rendszerek elemei," amelyek gyakran országspecifikusak. Amíg a "kritikus infrastruktúra" általánosabban elfogadott, és szélesebb körben használt a nemzetközi tudományos irodalomban, addig a "létfenntartó rendszerek elemei" fogalma inkább az adott ország jogszabályaiban definiált területspecifikus fogalom.[5]

A jelenlegi szakirodalom alapján kiemelkedő figyelmet fordítanak a nemzeti kritikus infrastruktúrák védelmére, ugyanakkor nem szabad elhanyagolni az európai és védelmi kritikus infrastruktúrák szerepét sem. Az infrastruktúra kritikusságát több szempontból is vizsgálhatjuk, például az ország területi szintjén beszélhetünk regionális, területi és lokális (például települési) kritikus infrastruktúrákról. A "kritikusság" dinamikusan változó tulajdonság lehet az adott felhasználói kör számára, és fontos az általános és helyzetfüggő kritikus infrastruktúrák megkülönböztetése.[6]

A mesterséges intelligencia (MI) térnyerése és szerepe a kritikus infrastruktúra biztonságában

A mesterséges intelligencia (MI) rohamos fejlődése és alkalmazása a kritikus infrastruktúrákban, mint az energiaelosztás, közlekedés és katasztrófaelhárítás, forradalmasítja ezeknek a rendszereknek a működését, növelve hatékonyságukat és rendelkezésre állásukat. Bár az MI kínálta lehetőségek izgalmasak és sokrétűek a kritikus infrastruktúrák működtetésében és védelmében, az új technológiáknak a bevezetése komoly kihívásokat is felvet az

adatvédelem, az etika és a biztonság területén, különösen a kiberfenyegetések és az emberi hibákból eredő problémák tekintetében.

A mesterséges intelligencia olyan tudományág az informatika területén, amelynek célja olyan gépek és rendszerek kifejlesztése, amelyek képesek emberi intelligenciához hasonlóan gondolkodni és döntéseket hozni. Az MI technológiák és alkalmazások robbanásszerű fejlődése az elmúlt években forradalmasította a modern társadalmat és gazdaságot. Fejlődésük olyan területekre is kiterjed, amelyek már hosszú ideje a kritikus infrastruktúra részét képezik. Például, az MI rendszerek részt vesznek az energiaelosztás és hálózatok optimalizálásában, a közlekedési irányításban, valamint a katasztrófák előrejelzésében és reagálásában. Az MI által vezérelt eszközök és algoritmusok hatékonyabbá tehetik ezeknek az infrastruktúráknak a működését és növelhetik a rendelkezésre állásukat.

A mesterséges intelligencia alkalmazása kritikus rendszerekben számos izgalmas lehetőséget rejt magában. Az infrastruktúra, ideértve a villamosenergia-ellátást, adatkommunikációt, víz- és üzemanyagellátást, valamint a légi, szárazföldi és vízi közlekedést, az egy modern társadalom alapvető pillére. Az MI lehetővé teszi ezeknek az átviteli rendszereknek a hatékonyabb működését, csökkentve ezzel az idő-, energia- és anyagpazarlást. Emellett növeli a zavarok elkerülésének és minimalizálásának képességét, például hurrikánok vagy jégviharok esetén.[7]

Az MI sokféle alkalmazási területet kínál a kritikus infrastruktúrában. Ezen területek egyike az előrejelző elemzések és diagnosztika, ahol az MI segíthet a rendszerhibák, energia- vagy vízszivárgások, vagy akár a fogyasztási minták előrejelzésében. Az intelligens rendszerek képesek gyorsan észlelni a rendellenességeket, elősegítve a gyors reakciót és a megelőzést.[8]

A mesterséges intelligencia fontos szerepet játszik az emberiség néhány legösszetettebb rendszerében, különösen a biztonságkritikus rendszerekben. Ezekben a kulcsfontosságú rendszerekben a szoftver általában felelős az elektromechanikai komponensek viselkedésének irányításáért és azok kölcsönhatásainak felügyeletéért.[9]

Segíthet a kritikus rendszerek működésében olyan területeken, ahol emberi beavatkozásra van szükség, például hibák észlelésére és döntések meghozatalára. Az MI hatékonyabb lehet az embereknél, és csökkentheti az emberi hibákból eredő problémákat.[10]

Alkalmazható továbbá az infrastruktúra optimalizálásában, például az energia- és vízellátás hatékonyabb kezelésében. Az algoritmusok segíthetnek az energiafogyasztás optimalizálásában, a hálózati terhelés szabályozásában, vagy akár az okos közlekedési rendszerekben is, ahol a forgalomirányítás vagy a parkolási rendszerek hatékonyabb működtetése lehetséges az MI által.

A mesterséges intelligencia is szorosan kapcsolódik a kritikus infrastruktúrák védelméhez. Használata lehetővé teszi az infrastruktúrák hatékonyabb és intelligensebb védelmét. Például képes folyamatosan monitorozni az infrastruktúrák működését, azonosítani a rendszert érő fenyegetéseket, és gyorsabban reagálni a biztonsági incidensekre. Emellett az MI alkalmazása a kiberbiztonság terén is segít az azonosítás és az adathalászattal vagy kártékony szoftverekkel szembeni védelemben. Lehetőséget nyújt a prediktív elemzésekre is, amelyek segítenek az infrastruktúraüzemeltetőknek megelőzni a hibákat és a rendszeresedő problémákat. Az adatok elemzésével képes az infrastruktúra karbantartásának optimalizálására is, csökkentve ezzel a kiesési időt és a működési zavarokat. Tehát nemcsak az események utáni reakciókban játszik fontos szerepet, hanem elősegíti a proaktív védelmet

és az infrastruktúra hosszú távú fenntarthatóságát is.[11] Ezen túlmenően, az MI rendszereken alapuló automatizáció lehetővé teszi a folyamatos megfigyelést így a gyors válságreakciót is a potenciális veszélyekre, mint például a kiberfenyegetésekre vagy természeti katasztrófákra. Ezáltal fontos szerepet játszhat a kritikus infrastruktúra biztonságának növelésében és a válságkezelésben.

A védelmi területen a mesterséges intelligencia számos új lehetőséget nyit meg a konvencionális módszerekkel szemben, például a "raj támadások," amelyek célja a célpontok meghatározó rendszereinek elárasztása önálló vagy előszabályozással rendelkező irányítás segítségével. A mesterséges intelligenciát olyan eszközként használják a védelemben, amely felismeri és válaszol az eltérő kibertámadásokra. Az elkövetkező időszakban a hadviselés területén a fő hangsúly a személyzet nélküli rendszerek fejlesztésére fog helyeződni, és a mesterséges intelligencia mind a támadó, mind a védekező feladatokban kulcsszerepet fog játszani, beleértve a kibertámadásokkal összefüggő műveleteket is.[12]

A mesterséges intelligenciában rejlő etikai kérdések és az infrastruktúra biztonsága közötti összefüggések

Az MI alkalmazása a kritikus infrastruktúra védelmében etikai kérdéseket vet fel, például az emberi beavatkozás mértékét és az autonóm döntéshozatalt. Az etikai dilemmák közé tartozik az emberi felügyelet hiánya az intelligens rendszerek felett, és az az esetleges képesség, hogy az MI önmagában döntsön válsághelyzetekben. Az etikai alapelveknek és a felelősségi kereteknek azonban meg kell felelni az infrastruktúra biztonságának is. Az egyensúly megtalálása az MI alkalmazása és az etikai elvárások között kulcsfontosságú, hogy megőrizzük a kritikus infrastruktúra biztonságát, miközben tiszteletben tartjuk a magánéletet és az emberi jogokat.[13]

Ezen kihívások és biztonsági megfontolások figyelembevételével az MI alkalmazása a kritikus infrastruktúra védelmében továbbra is egy izgalmas és dinamikus terület marad, ahol a technológia fejlődése és a biztonság előmozdítása közötti egyensúly megteremtése kiemelten fontos kihívás a jövőre nézve.

Az infrastruktúra sebezhetősége és a biztonság kiemelkedő jelentősége

Az infrastruktúra sérülékenysége a kiberfenyegetésekkel, technológiai hibákkal és természeti katasztrófákkal szemben kiemelt kockázatokat jelent, ami jelentős gazdasági, társadalmi és politikai instabilitást okozhat. Ez megköveteli az egységes és stratégiai szintű védelmi mechanizmusok kifejlesztését és a különböző országok közötti összehangolt erőfeszítéseket.

A szövetségi rendszerek olyan intézkedéseket hoznak a kritikus infrastruktúrák védelme érdekében, amelyeknek célja, hogy garantálják a környezetünk biztonságát és az önálló védelmünket. Ezen kezdeményezések a védelem célkitűzésén túlmenően azt próbálják elérni, hogy a terrorizmus és a biztonságpolitikai kérdések okozta kihívásokon túl más vészhelyzetekre is tudjanak reagálni. Mivel Európa országai többségükben szövetségek tagjaként élik meg ezeket a fenyegetéseket, fontos hogy egységes és stratégiai szintű védelmi mechanizmusokat fejlesszünk ki. A váratlan események és a sebezhető pontok sokasága miatt össze kell hangolni az erőfeszítéseket. Ehhez szupranacionális iránymutatásra, közös alapokra és hasonló értékrendre szükség van.[14]

Az infrastruktúraelemek egyre inkább függenek az informatikai rendszerektől, a digitális kommunikációtól és az automatizált vezérléstől. Ennek következtében növekszik az

infrastruktúra sérülékenysége a kiberfenyegetésekkel és a technológiai hibákkal szemben, melyek jelentős gazdasági, társadalmi és politikai instabilitást okozhatnak. Emellett a modern társadalomban az infrastruktúra egyre összetettebb és globalizáltabbá válik, ami további kihívásokat teremt a védelemben és az esetleges válságok kezelésében.[15]

A kritikus infrastruktúra biztonságának egyik központi kérdése a sebezhetőség. Az infrastruktúra sebezhetősége azon azonosított és fel nem ismert veszélyek, fenyegetések és sérülékenységek mértékét jelenti, amelyek károkat okozhatnak az infrastruktúrában és annak működésében. Ezek a veszélyek lehetnek emberi eredetűek, mint például a terrorizmus, kiberfenyegetések, vagy természeti jelenségek, mint a földrengés vagy az árvíz.

A mai kritikus infrastruktúra fejlődése egyre inkább az intelligens technológia és a hálózatok integrációján alapul. Ennek következtében a kiberfenyegetésekkel járó sérülékenységek sokasága keletkezik, amelyeknek hatásai súlyos károkat okozhatnak. Ebből kifolyólag a kritikus infrastruktúra terén, a biztonság rendkívül fontos szempont.[16]

A kritikus infrastruktúra védelem célkitűzéseinek konkrét megfogalmazása átalakítja a biztonságról alkotott képünket is. Az alapvető szükségleteinket kielégítő infrastruktúrák védelme fontos szempontokat és kihívásokat vet fel a biztonsági percepciónk és a hétköznapok gördülékenységének fenntartása szempontjából.

Az információs támadások elleni védelem kulcsszerepet játszik a kritikus infrastruktúrák védelmében. A kritikus infrastruktúra kritikussá válásának egyik fő oka a növekvő informatikai szolgáltatásfüggőség a társadalmi, szervezeti és magánélet területén.[17]

A kezelendő kockázatok nem korlátozódnak az államok határaira. Ezért fontos megjegyezni, hogy nem csak környezeti hatások játszanak szerepet, hanem az ellátás és társadalmi hatások is, ami sajátos interdependenciát jelent. Az egymásra gyakorolt kölcsönös függőség rendkívül komplex, és gyakran meghaladja a jogalkotók által meghatározott kereteket. A jogalkotók által kizárt ágazatok esetén nem is ismerik el, hogy az adott infrastruktúra kritikus lehet. Ebből adódóan ajánlatos lenne egy másik megközelítést alkalmazni a besorolási feltételek tekintetében, és meghatározni például egy kezelhető komplex küszöbértéket.[18]

Az infrastruktúra védelmének egyik alapvető feladata az infrastruktúrák azonosítása az adott felhasználói kör vagy alkalmazási terület szempontjából. Ez ágazatonként és szektoronként történhet. A szükséges követelményeket le kell bontani részletesebb, konkrét külső szolgáltatási szintekre, amelyek meghatározzák, hogy az adott szektor vagy infrastruktúra mely elemei minősülnek kritikusnak, és milyen belső szolgáltatási szint követelményeknek kell megfelelniük.[19]

Fontos a kritikus infrastruktúra védelme mind a kormányzati, mind a vállalati szektorban. Még ha eltérés is van a két szektor kritikus elemei között, mindkettőnél létfontosságúak az egészség, biztonság, gazdasági jólét és az ICT (Information and Communications Technology) infrastruktúra folyamatos rendelkezésre állása. Azonosítva és védelmezve ezeket az alapvető elemeket, a veszélyek és fenyegetések kockázatát minimalizálhatjuk. Ennek alapja a Critical Infrastructure Protection (CIP) és a CIP megoldásokra való fókuszálás.[20]

Az elmúlt évtizedek döntő biztonságpolitikai eseményei jelentős hatással voltak a kritikus infrastruktúra védelmének megközelítésére és a globális biztonsági percepcióra. Az 2001. szeptember 11-i terrortámadások, amikor a New York-i Világkereskedelmi Központ

és a Pentagon célpontjai voltak, radikálisan megváltoztatták a nemzetközi biztonsági politikát. Ezek az események rávilágítottak arra, hogy a terrorcsoportok képesek nagy léptékű károkat okozni, ezáltal felhívva a figyelmet a kritikus infrastruktúrák, mint az energiaellátás és a közlekedési hálózatok sebezhetőségére. A madridi vonatok elleni 2004-es merényletek, és a következő évben a londoni metró elleni támadások tovább erősítették a tömegközlekedési rendszerek védelmének szükségességét, mivel ezek a támadások aláhúzták, hogy a városi infrastruktúra különösen kiszolgáltatott a terrorcselekményeknek.

A kiberbiztonsági fenyegetések növekedése tovább bonyolítja a helyzetet. Ahogy a társadalom egyre inkább függ az informatikai rendszerektől, a kiberbűnözők és más rosszindulatú szereplők által elkövetett támadások súlyos károkat okozhatnak, mind gazdasági, mind társadalmi szinten. A digitális infrastruktúra, mint az adatközpontok és kommunikációs hálózatok elleni támadások rámutatnak a szükséges védelmi intézkedések és stratégiák kiépítésének sürgősségére. Ezen felül a természeti katasztrófák, mint hurrikánok, földrengések és árvizek, amelyek gyakorisága és intenzitása növekszik a klímaváltozás következtében, fokozzák az infrastruktúrák fizikai sérülékenységét, kiemelve a fenntartható és ellenálló infrastruktúra kiépítésének fontosságát.

Ezen kulcsfontosságú események összessége alapvetően formálja át a kritikus infrastruktúrákhoz kapcsolódó biztonsági stratégiákat. A támadások és fenyegetések széles skálája miatt a hatóságoknak és szervezeteknek komplex, többrétegű védelmi rendszereket kell kialakítaniuk, amelyek képesek adaptálódni a változó fenyegetési környezethez. Ennek érdekében a nemzetközi együttműködés és a technológiai innovációk előtérbe helyezése kulcsfontosságú, hogy biztosíthassuk társadalmaink stabilitását és jólétét a jövőben is. Az események által nyújtott tanulságok kulcsfontosságúak a hatékony védelmi politikák kialakításához, melyek központi eleme a kritikus infrastruktúra folyamatos és dinamikus védelme.

A kritikus infrastruktúra és a kibervédelem

A mesterséges intelligencia (MI) térnyerése a kiberbiztonság terén lehetővé teszi a fenyegetések korai felismerését és a gyors reakciót, ami alapvetően hozzájárul a kritikus infrastruktúrák védelméhez, különösen az egyre növekvő kiberfenyegetések és technológiai hibák világában. Bár a MI és a kiberbiztonsági technológiák fejlődése jelentős előrelépést jelent a kritikus infrastruktúrák védelmében, a globalizált és összekapcsolt világban a kiberfenyegetések egyre összetettebbé és súlyosabbá válnak az információs hadviselés területén.

A kritikus infrastruktúrák növekvő függősége az informatikai rendszerektől és a globális kiberhálózatoktól jelentős kihívásokat és sebezhetőségeket eredményez a kibervédelemben, amelyeket csak a mesterséges intelligencia (MI) és fejlett kiberbiztonsági megoldások integrált alkalmazásával lehet hatékonyan kezelni.

Az MI hozzájárulhat a fenyegetések korai felismeréséhez és a kiberbiztonsághoz, mivel az algoritmusok és rendszerek képesek az anomáliák észlelésére és az esetleges támadásokra való gyors reagálásra. Az adatok folyamatos monitorozása és elemzése segíthet az azonnali fenyegetések azonosításában, és lehetővé teszi a védelmi intézkedések időbeni bevezetését.

Ahogyan a fejlett infrastruktúrával rendelkező országokban általában, a kibertér sebezhetőnek tekinthető. Ugyan léteznek hatékony védelmi intézkedések, amelyek az egyes

kritikus infrastruktúrákat megfelelően védik, de 21. század által nyújtott globalizáció adta lehetőségek kialakították a határok nélküli és összekapcsolt hálózatok kölcsönös függőségét. Azok a kibertámadások, amelyek veszélyt jelenthetnek egy ország kritikus infrastruktúrájára, egyre összetettebbek és súlyosabbak lehetnek az informatika területén bekövetkező változásoknak köszönhetően.

Az információs hadviselés terén az új évezredben egy paradigmaváltás figyelhető meg. Az informatikai fejlődés új kihívások elé állítja a nemzetek biztonságát. A támadók olyan digitális eszközöket használhatnak, amelyekkel "digitális kőkorszakot" hozhatnak létre a megtámadott országban, anélkül, hogy hagyományos katonai erőket alkalmaznának.[21] Az egyes informatikai rendszerek meghibásodása jelentős károkat okozhat egy ország normális működésében. Azok az országok, amelyek komolyan veszik a had-, biztonság- és informatikai területeket, kritikus információs infrastruktúrájuk védelmét a 21. század egyik legfontosabb kihívásának tekintik.[22]

A kibertér természeténél fogva egy olyan terület, ahol nem alkalmazhatóak azok a hagyományos hadviselési módszerek amelyek az elmúlt évszázadok óta szokásként számítottak. A digitális tér alapjainak a fejlődése jelentős mértékben elősegíti az aszimmetrikus hadviselés lehetőségét, amelyek által a terrorista csoportok is előnyökre és új lehetőségekre tehetnek szert nyújthat.[23]

A konvencionális hadviseléssel párhuzamosan nélkülözhetetlenné váltak a kibertérben elindított parhuzamos támadások indítása a kritikus infrastruktúrák ellen. Ahhoz, hogy blokkolni tudjuk az infrastruktúra elemeit, kellő információ birtokában kell lenni a célpont strukturális felépítéséről és sebezhetőségéről. Sajnos prevenció tekintetében a támadók általában lépéselőnyben vannak, így a válságkezelés csak válaszreakció tud lenni. Mint minden rendszernek vannak biztonsági hézagjai. Ennek okán a biztonság és a támadhatóság szempontjából nem szabad figyelmen kívül hagyni a különböző technológia eszközök használatának és a virtuális térben indított támadásoknak a hadtudományokban betöltött szerepét. A digitális tér alapjait tekintve olyan terület, ahol nem alkalmazható azok a hagyományos hadviselési módszerek, amelyek évszázadok óta bevett szokásnak számítottak. Ez a fejlődés lehetővé teszi az aszimmetrikus hadviselés elterjedését, ami előnyöket biztosíthat a terrorista csoportoknak.

A kibertér és más hadviselési területek közötti egyik kulcsfontosságú különbség az, hogy a kibertérben a rombolás képessége hasonló elvi szempontból az atomfegyverekhez hasonlóan megváltozott. Az új kibertéri fegyverek dimenziókkal nagyobb pusztító erőt képviselnek, mint a hagyományos eszközök. Ez azt jelenti, hogy a kibertérben olyan rombolás és fenyegetettség valósítható meg egy másik országgal szemben, amely akár meghaladhatja a nukleáris fegyverek által nyújtott pusztító erőt is.[24]

Az informatikai területek alapvetően egy elég szenzitív életfázisba értek. Az újonnan zajló változások, új kihívások elé állítják a nemzetek biztonságáról alkotott képünket. A támadók képesek pusztán számítógép-hálózatok segítségével jelentős kárt okozni anélkül, hogy hagyományos hadviselési módszereket alkalmaznának. Ennek következtében a lehető legmagasabb prioritásként kezdték el kezelni a kibertámadások jelentőségét.[25] Míg korábban a kibervédelem főként az ipari kémkedés és adatlopások ellen irányult, most egyre inkább a külföldi kormányok által végrehajtott hálózati támadások kezelése válik prioritássá, különösen Kína hatására. Ennek következtében a hadseregek támadó képességei is

fejlődnek, hogy képesek legyenek kritikus infrastruktúrák megsemmisítésére az ellenséges államok ellen.[26]

A kritikus infrastruktúrák elleni támadások különböző módszerekkel valósulhatnak meg, mind azzal a céllal, hogy az adott infrastruktúra működését zavarják vagy korlátozzák, akár ideiglenesen, akár véglegesen. Ezek közé tartozik a fizikai károkozás, amely kinetikus hatással valósulhat meg. Továbbá az infrastruktúra belső alrendszeri közötti kommunikáció manipulálása vagy blokkolása is egy gyakori támadási módszer. Emellett az egy vagy több alrendszerben történő belső, fizikai károkozás is előfordulhat.[27]

Az elmúlt időszakban a kibervédelem főleg az adatlopások és ipari kémkedés elleni védelemre koncentrált. Kína vezetésével az állami hálózatok elleni támadások növekedése erősítette a hadseregek képességeit a kritikus infrastruktúra támadására. A kibertámadások kezelése kiemelten fontos a biztonságpolitikában, de sokan nem értik teljesen ezt a veszélyt és a szükséges intézkedéseket.

ÖSSZEFOGLALÁS

Az infrastruktúra biztonsága és védelme kritikus szerepet játszik a társadalmi stabilitás és gazdasági folytonosság fenntartásában. A kihívások folyamatosan növekednek az információs korban, ahol az infrastruktúrák egyre inkább az informatikai rendszerektől függnek és ahol a kiberfenyegetések súlyos veszélyeket hordoznak magukban. Az MI fejlődése, a kibertéri szülte új támadási felületek lehetőségei és az aszimmetrikus hadviselés térhódítása új stratégiai megközelítéseket követel meg a kritikus infrastruktúra védelmében. Mind a kormányzati, mind a vállalati szektorban, a Critical Infrastructure Protection (CIP) keretében való fókuszálás és megelőzés kiemelkedő fontosságú. A kibertámadások súlyosabb pusztítást okozhatnak, mint a hagyományos hadviselési eszközök, így a fenyegetések felismerése és kezelése elengedhetetlen. Az intelligens technológiák és hálózatok fejlődésével nő az infrastruktúrák sebezhetősége, így a kibertér prioritása és az informatikai biztonság kulcsszerepet játszik a megelőzésben és a válságkezelésben. A kritikus infrastruktúrák védelme új kihívások elé állítja a biztonságpolitikát, ahol a nemzetközi közösségnek stratégiai válaszokat kell találnia a jövőbeni veszélyekre. Az együttműködés és a megosztott értékrend alapján történő védelem kulcsfontosságú a globális biztonság fenntartásához.

FELHASZNÁLT IRODALOM

[1] J. Daniels, *The Internet of Things, Artificial Intelligence, Blockchain, and Professionalism*, IT Professional, 2018, pp. 15-19., DOI: 10.1109/MITP.2018.2875770

[2] V. Mani, S. Lavanya, *Iot based smart energy management system*, International Journal of Applied Engineering Research, 2017, pp. 5455-5462.

[3] H. Bangui, B. Buhnova, B. Rossi, *Shifting towards Antifragile Critical Infrastructure Systems*, 2022, Conference: 7th International Conference on Internet of Things, Big Data and Security, pp. 1-10., DOI:10.5220/0011086400003194

[4] T. Bonyai, NKE Kiberbiztonsági Kutatóintézet, *Kritikus infrastruktúrák: célpont, vagy eszköz?* 2021, https://www.ludovika.hu/blogok/cyberblog/2021/01/27/kritikus-infrastrukturak-celpont-vagy-eszkoz/

[5] L. KIRÁLY, *Hadszíntér-előkészítés, befogadó nemzeti támogatás, kritikus infrastruktúra védelem-védelemgazdasági nézőpontból*. Military Science Review/Hadtudományi Szemle 2015. VIII. évfolyam 3. szám, pp. 10-20.
[6] S. MUNK, *Kritikus infrastruktúrák védelme információs támadások ellen*. Military Science Review/Hadtudományi Szemle 2008 XVIII. évfolyam 1-2 szám, pp. 95-106.
[7] K. Bresniker, A. Gavrilovska, J. Holt, Grand challenge: Applying artificial intelligence and machine learning to cybersecurity, Computer, 2019, pp. 45-52., DOI: 10.1109/MC.2019.2942584
[8] C. Perera, C.H. Liu, S. Jayawardena, M. Chen, A survey on internet of things from industrial market perspective. IEEE Access **2**, 1660–1679 (2014), A Survey on Internet of Things From Industrial Market Perspective | IEEE Journals & Magazine | IEEE Xplore
[9] W. WONG, P. LAPLANTE, *Be more familiar with our enemies and pave the way forward: A review of the roles bugs played in software failures*. Journal of Systems and Software, 2017, pp. 68-94.
[10] P. Laplante and B. Amaba, *Artificial intelligence in critical infrastructure systems*, Computer, 2021 1, pp. 4-24
[11] Cs. Kollár, *A mesterséges intelligencia megjelenése a biztonságtudományban*. In: Tibor, János Karlovitz (szerk.) What will our Future be Like? 2 essays in German, 7 in English, 30 in Hungarian language (Német, angol és magyar nyelvű esszék) Grosspetersdorf, Ausztria : Sozial und Wirtschafts Forschungsgruppe (2023) 448 p. pp. 242-256. 15 p.
[12] J. Johnson, *Artificial intelligence & future warfare: implications for international security*. Defense & Security Analysis, 2019, pp. 147-169
[13] I. Négyesi, *A mesterséges intelligencia és az etika*, Hadtudomány, Magyar Hadtudományi Társaság folyóirata 30 (1), 2020 pp. 103-113. http://doi.org/10.17047/HADTUD.2020.30.1.103
[14] Katasztrófavédelmi Tudományos Tanács pályázata, *Kritikus Infrastruktúra védelem fogalmi rendszere, hazai és nemzetközi szabályozása*, 2011, pp. 01-61
https://www.vedelem.hu/letoltes/anyagok/382-a-kritikus-infrastruktura-vedelem-fogalmi-rendszere-hazai-es-nemzetkozi-szabalyozasa.pdf
[15] *A Proclamation on Critical Infrastructure Security and Resilience Month*, 2021 | The White House, Briefin Room, Presidental Actions
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/10/29/a-proclamation-on-critical-infrastructure-security-and-resilience-month-2021/
[16] J. Sakhin, H Karimipour, A Dehghantanha, *AI and security of critical infrastructure*, Handbook of Big Data Privacy, 2020, pp. 7-36. DOI:10.1007/978-3-030-38557-6_2
[17] S. Munk, *Kritikus infrastruktúrák védelme információs támadások ellen*, Hadtudomány, Magyar Hadtudományi Társaság folyóirata XVIII.:(1-2.), 2008, pp. 95-106.
[18] K. Kralovánszky, *A kibertér fejlődése (második rész)–Kiberműveletek és kritikus infrastruktúrák egyes kapcsolatai,* Hadmérnök 16.1, 2021, pp. 145-160.
[19] S. Munk, *Kritikus infrastruktúrák védelme információs támadások ellen*, Hadtudomány, Magyar Hadtudományi Társaság folyóirata XVIII.:(1-2.), 2008, pp. 95-106.
[20] https://www.e-spincorp.com/protect-what-is-critical-to-your-infrastructure/

[21] P. Bányász és Á. Orbók, *A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében.* Hadtudomány, Magyar Hadtudományi Társaság folyóirata 23. szám, 2013, pp. 188-209. ISSN 1215-4121
https://www.mhtt.eu/hadtudomany/2013/2013_elektronikus/2013_e_Banyasz_Peter_Orbok_Akos.pdf
[22] L. Kovács, Cs. Krasznay: *Digitális Mohács, Egy kibertámadási forgatókönyv magyarország ellen*, Nemzet és Biztonság, 2010, pp. 44-56.
https://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf
[23] I. Porkoláb, *Az aszimmetrikus hadviselés adaptációja*. Ludovika Egyetemi Kiadó, 2020,
https://demo.repozitorium.uni-nke.hu/xmlui/bitstream/handle/123456789/15904/576_aszimmetrikus_hadviseles.pdf?sequence=7
[24] K. Kralovánszky, *A kibertér fejlődése (második rész)–Kiberműveletek és kritikus infrastruktúrák egyes kapcsolatai*, *Hadmérnök* 16.1, 2021, pp. 145-160.,
DOI: 10.32567/hm.2021.1.9
[25] P. Bányász, Á. Orbók, *A NATO Kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében*, Hadtudomány, Magyar Hadtudományi Társaság folyóirata, 2013, pp. 188-206
[26] *A New Kind of Warfare*, The New York Times-The Opinion Pages, 2012, https://www.nytimes.com/2012/09/10/opinion/a-new-kind-of-warfare.html
[27] K. Kralovánszky, *A kibertér fejlődése (második rész) – Kiberműveletek és kritikus infrastruktúrák egyes kapcsolatai*, *Hadmérnök* 16.1, 2021, pp. 145-160.

LIFE CYCLE MODEL OF BEARINGS AND SHAFT MISALIGNMENT FREQUENCIES OF ASYNCHRONOUS MOTORS

ASZINKRON MOTOROK CSAPÁGYAINAK ÉS TENGELYBEÁLLÍTÁSI FREKVENCIÁINAK ÉLETCIKLUS MODELLJE

BENDIÁK István[1]

Abstract

The target area of the research is the analysis of the mechanical failure of three-phase asynchronous motors, including primarily the assessment of the excitation frequencies caused by bearing and shaft adjustment and the knowledge of the wear process. The field of science is one of the widely studied branches, however, there are parts that do not provide clear (in the case of current signal analysis) guidance on the cycles of bearing wear. The research foundations are partly derived from vibration diagnostics, but the analysis is based on electrical signal testing. Objectives: The design of the wear characteristic fields is the four elements, the outer and inner ring of the bearing, rolling elements, especially running rolling elements and the bearing basket, as well as the analysis of errors resulting from shaft alignment errors. The first sketch of the wear process and setting up step rules, creation of simplification routes, getting to know the user.

Keywords

Shaft Misalignment, Bearing Frequency, Outer ring frequency, Inner Ring Frequency, Asynchronous motor

Absztrakt

A kutatás célterülete háromfázisú aszinkron motorok mechanikai meghibásodásának elemzése, azon is belül elsősorban csapágy és tengelybeállítás okozta gerjesztő frekvenciák felmérése és kopási folyamat megismerése. A tudományterület szélesen művelt ágazatok közé tartozik, azonban van olyan részegysége, amely nem ad egyértelmű (áram jelalak-analízis esetén) eligazítást a csapágy elhasználódás ciklusaiban. A kutatási alapok részben a rezgésdiagnosztikából származnak, de az analizálás villamos jelvizsgálatra épít. Célkitűzések: A kopási jellegmezők kigondolása a négy elem, a csapágy külső és belső gyűrű, gördülő elemek, egysorban futó gördülő elemek és a csapágy kosár, valamint a tengelybeállítás hibákból származó hibák elemzése. A kopás folyamatának első vázlata és lépésszabályok felállítása, egyszerűsítési útvonalak létrehozása, az elhasználódás megismerése.

Kulcsszavak

Tengelybeállítás, Csapágyfrekvencia, Külső gyűrű frekvencia, Belső gyűrű frekvencia, Aszinkron motor

[1] bendiak.istvan@uni-obuda.hu |ORCID: 0009-0009-3320-4089| PhD Student, Doctoral School for Safety and Security Sciences Óbuda University |Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

KUTATÁSI ELŐZMÉNYEK, BEVEZETŐ

A kutatás célterülete háromfázisú aszinkron [1] motorok mechanikai, azon is belül elsősorban csapágy és tengelybeállítás okozta gerjesztő frekvenciák felmérése és kopási folyamat megismerése. A tudományterület [2] szélesen művelt ágazatok közé tartozik, azonban van olyan résterülete, amely nem ad egyértelmű (áram jelalak-analízis esetén) eligazítást a csapágy elhasználódás [3] ciklusaiban. A kutatási alapok részben a rezgésdiagnosztikából származnak.

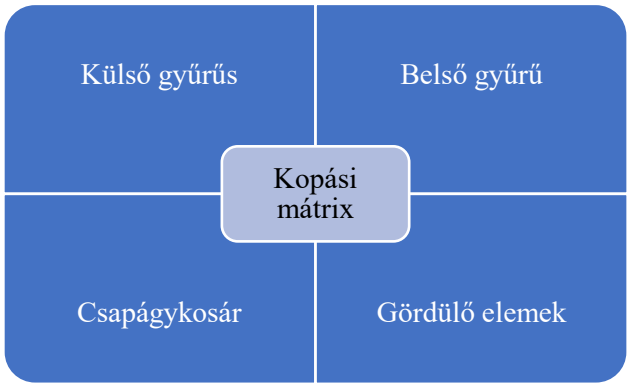
A kopási jelleg-mezők kigondolása négy elem, a csapágy külső és belső gyűrű, gördülő elemek, egysorban futó gördülő elemek és a csapágy kosár, valamint a tengelybeállítás hibákból származó hibák elemzése. A tengelybeállítás esetén [4] merőlegességi és párhuzamosság, szöghibából származó gerjesztő hibák elemzése amplitúdó, frekvencia tartományban. A kopás folyamatának első vázlata és lépésszabályok felállítása, egyszerűsítési útvonalak létrehozása. Az elhasználódás folyamatában visszatéri pontok és előrejelzés struktúrájának kidolgozása. Ennek alapja a motor áramjel vizsgálata [5] fázisáram és Park-vektor komponens elemzések alapján. A dolgozat első része a kutatás hátterének bemutatásával foglalkozik, a második az kopási folyamat köré épült tapasztalatokkal.

A villamos gépek egy integrált rendszer [6] részei (frekvenciaváltó, szenzorok, szoftverek stb.) és azzal már nélkülözhetetlenül együtt dolgoznak. Ebben a folyamatban nyílik lehetőség a gépről alkotott működési térkép felállítására. Számos forgógép van jelen az iparban, együttműködés és ellenőrzés szükséges, folyamatos állapotfigyelés.

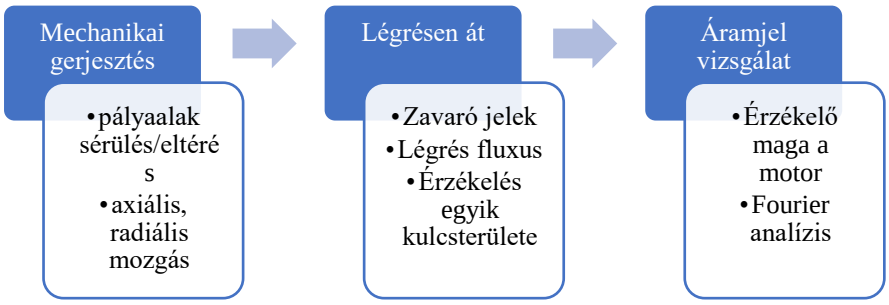
Itt már nem csupán hibajelek detektálása a cél, hanem ezen túlmutató információforrás kezelése és fejlesztése, elindulva az öntanuló villamos hajtások területe felé. Gépek és [7] rendszerüzemeltetők közös munkája, egymás üzemviteli jellemzőinek elemzése és korrigálása, abból konklúziók levonása. A dolgozat elsősorban a mechanikai eredetű jelekkel foglalkozik, és abból képez elemzési [8] lehetőségeket. Szakterület hazai és nemzetközi viszonylatban megalapozott és széleskörűen művelt ágazat.

A nemzetközi szakirodalom rendkívül [9] gazdag ismeretet szolgáltatott a dolgozat megszületéséhez, amit saját mérési eredményekkel vizsgáltam meg. A jelanalízis mellett a termográfia is helyet kap a jelenségek bemutatásában, önmagában nem szerepel külön ágazatként.

Az első beszámoló ezen fázisának [10] alapvető célja eddig nem ismert kopási folyamat felállítása és folyamatos fejlesztése, amely lehetőséget biztosít az [11] áram jelalak-analízis keretein belül a csapágy és tengelybeállítási hibák előre jelzésre és tervszerű leállás elősegítésére. A frekvenciaösszetevők és köztük megjelenő [12] modulációk elemzési lehetőségeinek továbbfejlesztése. Az 1-3. ábrák mutatják a mérés alapvető elképzeléseit, rezgésdiagnosztikával szembeni előnye, hogy nincs szükség gépbe vagy gépre épített szenzorokra (pl.: piezokristályra).

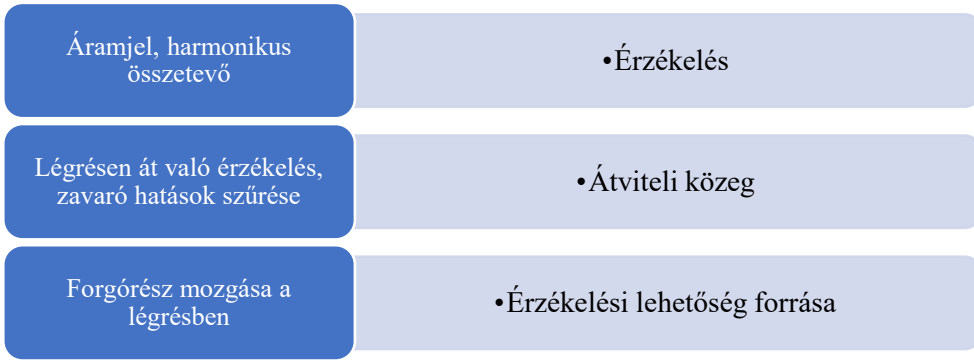


1. ábra Csapágy kopási folyamatának elemei áram jelalak-analízisben való elemzéshez, (szerzői ábra).



2. ábra Származtatás a rezgésdiagnosztika alapvető elképzeléseiből, (szerzői ábra).

Érzékelés fizikai gondolatkísérlete, miként érzékelhető mechanikai jel mágneses úton (3 ábra)? Forgórész mozgása fluxusváltozást idéz elő a légrésben.



3. ábra Áramjel vizsgálat egyszerűsített elvi érzékelési elképzelése, (szerzői ábra).

KIALAKÍTOTT CSAPÁGY-HIBAMETRIA

A csapágy hibametria felállítása az első olyan lépés, amely megalapozza a kopásra következtethető rajzolandó térkép felállítását. A hibametria felállítása nélkül nem lehet algoritmust létrehozni.

A vizsgálati struktúra szemléltetésére készült a 1-2. táblázatok. A csapágyfrekvenciák mellé társulnia kell a tengelybeállításból eredő gerjesztő frekvenciáknak is, így a vizsgált jelek száma 150 darabra növekszik. Kísérleti eredmények azt mutatták [13], hogy nem csak a csapágyra vonatkozó frekvenciákat kell [14] számítani és ellenőrizni, hanem a tengely beállítási frekvenciákat is. Ettől eltérni nem célszerű, mert tengelybeállítási-hiba hatással lesz a csapágyra és fordítva [15].

A mérés alapvető elképzelése, hogy érzékelő egyben a vizsgált motor. Valamennyi hiba érzékelése a légrésen [16] keresztül történik. A radiálisan keletkező elmozdulás nem lehet milliméteres nagyságrendű. A vizsgált aszinkronmotor légrése tizedmilliméter nagysárendjében van, a forgórész belesúrlódna az állórészbe, az [17] észlelt mechanikai hibák axiális mágneses húzási-tolási elmozdulásból alapján jelennek meg, amely a forgórész közvetít az állórész vasmaggal. A vizsgálat közvetítő eszköze a mágnesestér, azon belül a forgótér, így ennek jellemzőit is figyelembe kell venni. A térvektor elmélet nem feltétlenül oldja meg a hibakeresési problémákat (fázisaszimmetria, attól a mechanikai komponens jelen lesz), mert a háromfázisú vektorok egy pályageometria alakhűségben nem választják szét a hiba jelek változatait. A térvektor elméletben szereplő téralak leírás és pályaváltozási [18] módszer sokszor nehezíti a hibaanalizálást és a hibák egymásra hatás nem követhető egyértelműen, ezért arra következtetésre jutottam, hogy kopási mátrixot hozok létre, amely megmutatja egy elhasználódási folyamat okozóit és eredményeit [19].

ASZINKRON MOTOROK DIAGNOSZTIKAI VIZSGÁLATA ÁRAM JELALAK-ANALÍZIS MÓDSZERÉVEL

Az előző fejezetben bemutatott számítási folyamat előzi meg a jelfeldolgozási lépéseket. Ezek az adatok adatbázisokban tárolhatók és tovább felhasználhatók.

A forgógép diagnosztika szerteágazó szakterület, ezért jelenleg csak az aszinkron géptípusra fogok koncentrálni.

Az áram jelalak-analízis rendkívül széles körben alkalmazott módszer, napjainkra már kidolgozott eszközparkkal és mérési [1] eljárásokkal, [2] ennek lehetőségeit [20] vizsgálom ebben a fejezetben. Elsősorban a Park-vektorok (térvektorok) diagnosztikai alkalmazása kap kiemelt szerepet.

Áram jelalak kiértékelésének módszerei

- Hogyan lehet a kapott spektrumokból hibajelekre következtetni?
- Milyen jellemzőkkel bírhat egy villamos forgógép a jelfeldolgozás területén?
- Konklúzió: Érzékelő maga a motor (légrésen keresztül)

A motoráram nagyon sok adatot tartalmaz [21] a motor aktuális működési állapotáról. A meghatározásukra vannak [22] ismert és kutatott (áramjel és szórt fluxusok) eljárások. Az általam végzett mérési sorozat arra irányult, hogy minél több üzemmód álljon rendelkezése a motor viselkedéséről különböző táplálási módok alkalmazása mellett [23].

Csapágyhibák vizsgálata motoráram spektrum alapján

Csapágyhibák keresésénél a mintavételezés létfontosságú kiindulási feltétel. A spektrumok elemzésének olyan lépéssel kell haladnia, amelyben látható a csapágyra vonatkozó jel. A nemzetközi szakirodalmak szerint a következő összefüggés alapján lehet elindulni [1], [2-3],

$$f_{keresendő\ hibafrekvencia} = \left| f_{állórész\ frekvencia} \pm m \cdot f_{csapágyra\ jellemző\ frekvencia} \right|$$

ahol m=1, 2, 3….n

Kopási folyamatábrában szereplő mezők jelölései.

Komponens	Amplitúdó [A]	Harmonikus rend-szám	Harmonikus értéke frekvencia [Hz]	f [Hz]
Outer ring Külső gyűrű	o1.	oh1.	of1.	133,32
	o2.	oh2.	of2.	216,63
	o3.	oh3.	of3.	299,95
	o4.	oh4.	of4.	383,27
	o5.	oh5.	of5.	466,6
	o6.	oh6.	of6.	549,91
	o7.	oh7.	of7.	633,23
	o8.	oh8.	of8.	716,55
	o9.	oh9.	of9.	799,88
	o10.	oh10.	of10.	883,2
Inner ring Belső gyűrű	in1.	inh1.	inf1.	203,25
	in2.	inh2.	inf2.	332,83
	in3.	inh3.	inf3.	462,42
	in4.	inh4.	inf4.	592,02
	in5.	inh5.	inf5.	721,6
	in6.	inh6.	inf6.	851,19
	in7.	inh7.	inf7.	980,79
	in8.	inh8.	inf8.	1110,38
	in9.	inh9.	inf9.	1239,96
	in10.	inh10.	inf10.	1369,55
Cage Kosár	c1.	ch1.	cf1.	59,23
	c2.	ch2.	cf2.	68,45
	c3.	ch3.	cf3.	77,69
	c4.	ch4.	cf4.	86,91
	c5.	ch5.	cf5.	96,14
	c6.	ch6.	cf6.	105,37
	c7.	ch7.	cf7.	114,61
	c8.	ch8.	cf8.	123,83
	c9.	ch9.	cf9.	133,06
	c10.	ch10.	cf10.	142,29

1. Táblázat. Hibametria felállítása egysoros mélyhornyú csapágy külső, belső gyűrű és kosár komponensekre, (szerzői táblázat).

Komponens	Amplitúdó [A]	Harmonikus rend-szám	Harmonikus értéke frekvencia [Hz]	f [Hz]
Rolling elements Gördülő elemek	r1.	rh1.	rf1.	110,88
	r2.	rh2.	rf2.	162,52

	r3.	rh3.	rf3.	214,18
	r4.	rh4.	rf4.	265,83
	r5.	rh5.	rf5.	317,48
	r6.	rh6.	rf6.	369,13
	r7.	rh7.	rf7.	420,78
	r8.	rh8.	rf8.	472,43
	r9.	rh9.	rf9.	524,08
	r10.	rh10.	rf10.	575,72
Shaft Tengely	s1.	sh1.	sf1.	73,66
	s2.	sh2.	sf2.	97,32
	s3.	sh3.	sf3.	120,97
	s4.	sh4.	sf4.	144,63
	s5.	sh5.	sf5.	168,3
	s6.	sh6.	sf6.	191,95
	s7.	sh7.	sf7.	215,61
	s8.	sh8.	sf8.	239,27
	s9.	sh9.	sf9.	262,94
	s10.	sh10.	sf10.	286,6

2. Táblázat. Hibametria felállítása egysoros mélyhornyú csapágy gördülő elemek és tengelyütési, forgási frekvencia komponensekre, (szerzői táblázat).

A táblázat felosztása a következő

A harmonikusokat első megközelítésben a tizedik rendszámig kell követni, mert az egyik azonosító a frekvencia és amplitúdó mellett a harmonikusrendszám. Ha nagyobb rendszámig tart a számítás, akkor a zaj is megnő, mert a szűrés esetén a zavaró jelek elemzését harmonikus rendszámhoz is kell hasonlítani.

Amplitúdók és harmonikusok felosztása

Az első az amplitúdó értéke a tizedik harmonikusig. Jelölése utal a komponensre o1-outer ring-külső gyűrűs első harmonikus, in1-inner ring/inner race-belső gyűrű első harmonikus, c1-cage-kosár-első harmonikus, r1-rolling elements-gördülő elemek első harmonikus.

Az s1-shaft-tengely első harmonikus, vagyis a forgási frekvencia modulált értékének első harmonikusa. A moduláló jel az a tápláló hálózat frekvenciája (alapesetet feltételezve).

Frekvencia összetevők jelölései

- of1.: Outer ring/race-külső első frekvencia összetevő
- of2.: Outer ring/race-külső második frekvencia összetevő
- of3.: Outer ring/race-külső harmadik frekvencia összetevő
- A komponensek folytatódnak ugyanezen jelölés szerint of10.-ig.
- inf1.: Inner ring/race-belső gyűrű első frekvencia összetevő
- inf2.: Inner ring/race-belső gyűrű második frekvencia összetevő
- inf3.: Inner ring/race-belső gyűrű harmadik frekvencia összetevő
- A komponensek folytatódnak ugyanezen jelölés szerint inf10.-ig.

- cf1.:Cage-kosár frekvencia első összetevő
- cf2.: Cage-kosár frekvencia második összetevő
- cf3.: Cage-kosár frekvencia harmadik összetevő
- A komponensek folytatódnak ugyanezen jelölés szerint cf10.-ig.
- rf1.:Rolling elements-gördülő elemek első frekvencia összetevő
- rf2.: Rolling elements-gördülő elemek második frekvencia összetevő
- A komponensek folytatódnak ugyanezen jelölés szerint rf10.-ig.
- sf1.: Shaft-tengely első frekvencia összetevő
- sf2.: Shaft-tengely második frekvencia összetevő
- A komponensek folytatódnak ugyanezen jelölés szerint sf10.-ig.

CSAPÁGYÉLET-CIKLUS MODELL, KOPÁSI ALGORITMUS

A kutatás első fázisának célja létrehozni egy olyan folyamatelemző térképet amely, túlmutat a függvénytranszformációk begyakorolt elemzésein. A kutatás nem teljes egy olyan rendszer nélkül, amely rávilágít egysoros mélyhornyú golyós csapágy által generált jelleg-mezőkre.

Kiindulási pontok a modell létrehozásában

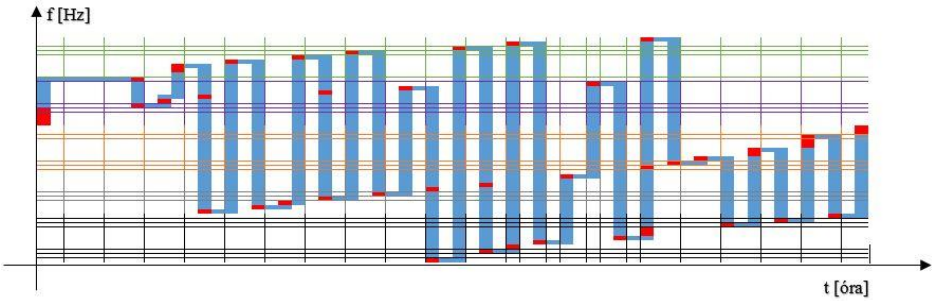
- A négy csapágy hibafrekvencia mellett a tengelybeállítási frekvenciát közös útvonalra hozni az elhasználódás folyamatában.
- Lehet-e párhuzamot állítani a frekvenciatartományokban?
- Melyik elemnél indul meg először a hiba jel és milyen frekvenciatartományban?
- Hogyan hatnak egymásra a hibafrekvenciák?
- A harmonikus rendszámnöveléssel mennyi zaj kerül a mérési feldolgozásba?
- Mennyi minimális és maximális lépésszám közötti eltérés (technológiai folyamat és gépfüggő kritérium)?

Ezekre a kérdésekre életciklus modellel lehet válaszolni.

A 1-2. táblázatok és 4. ábra szerint készült egy modell. A négy csapágy hibafrekvencia és egy tengelybeállításra vonatkozó frekvencia és ezek a 10. harmonikusig vannak számítva. Ettől egyenlőre nem tér el a számítás (következő lépésekben szükséges, mert a visszalépési útvonalakat fel létre kell hozni).

Vannak kisebb frekvenciánál jelentkező komponensek pl. kosárkopás és ettől lényegesen nagyobb (vagy együtt roncsolódó alkatrészek, amik egymásra hatnak) frekvenciatartományú jelek, mint pl.: belső gyűrű.

Az első mérföldkő mérései és számítási eredménye 4. ábrán látható életciklus modell, kopási folyamatábra. A 4. ábra mélyhornyú golyós csapágyra vonatkozik vagy általánosságban egysoros mélyhornyú golyós csapágyra. A számítás figyelembe veszi a frekvenciaváltós táplálást, átszámol a fordulatszám és tápláló frekvencia függvényében. A frekvencia összetevők Fourier-transzformációval vannak számítva.



4. Ábra Egysoros mélyhornyú csapágy kopási folyamatábrája áram jelalak-analízissel. . (Jelölések: f: motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).

ALGORITMUS MŰKÖDÉSI FOLYAMATA ÉS JELLEGMEZŐK ÉRTELMEZÉSE

- Zöldmező: Csapágy külső gyűrű szektor 1-10. harmonikusig amplitúdó komponens és frekvencia értékkel.
- Lilamező: Csapágy belső gyűrű szektor 1-10. harmonikusig amplitúdó komponens és frekvencia értékkel.
- Barnamező: Csapágy kosár szektor 1-10. harmonikusig amplitúdó komponens és frekvencia értékkel.
- Szürkemező: Csapágy gördülő elemek szektor 1-10. harmonikusig amplitúdó komponens és frekvencia értékkel.
- Feketemező: Tengelybeállítási hibarész szektor 1-10. harmonikusig amplitúdó komponens és frekvencia értékkel.

Lépési szabály

A 4. ábra kisméretű, ezért nem látszik a frekvencia érték, de színek alapján követhető folyamatábra, ennek ez is a célja. Az élettartam balról jobbra halad a piros mezőket érintve a kékmező útvonalon. A mérete azért ilyen, mert így együtt látni az összes mezőt.

Lépési folyamat

Balról jobbra halad a hibajel kezdete kékmezőn (a sárgaszín a beavatkozási tartomány). A piros mezők hibafrekvencia lépési pontok (határállomások), amelyek Fourier-transzformációval vannak számítva. A kezdeti kopás a baloldali pirosmezőből indul (belső gyűrű hibafrekvencia, lilamező). Cél eljutni a jobboldali pirosmezőkig, viszont ekkor már teljesen tönkremegy a hajtásrendszer.

Pirosmezőt nem lehet kihagyni, átlósan nem lehet menni, feltéve, ha nem keresztez kékmezőt és nem hoz létre kétértelmű állapotot. Lépésszámot lehet csökkenteni, de akkor fennállhat olyan állapot, hogy a következő pirosmező csúcsához érkezik a folyamat, akkor kétértelművé válik és anomáliát ad, mert vagy kihagy egy lépést vagy kétszer elemez egy pirosmezőt, egyik sem megengedett.

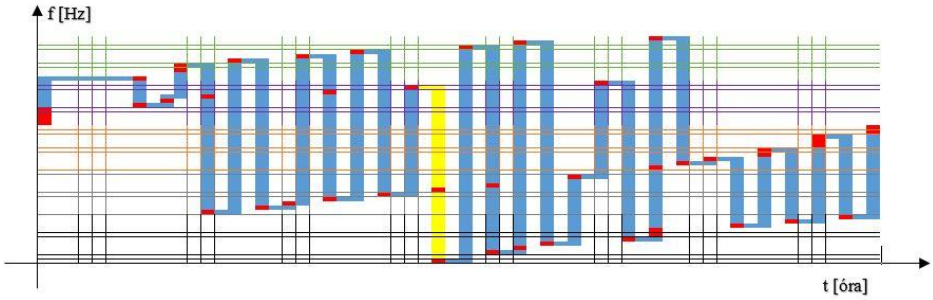
Kékmezők nem kereszteszhetik egymást egyik területben sem. Érinteni kell a pirosmezőket és azon/azokon keresztül kell tovább haladni. Pirosmezők lehetnek egymás mellett (vannak is), ennek oka a hibafrekvenciák közelesése egymáshoz. Tehát az egymásra hatást könnyebb látni, mint spektrumokban. A pirosmezőbe hosszanti vagy rövid oldalról

kell belelépni, kikerülni nem lehet, akkor kihagyna egy hibafrekvenciát, értelmét veszti a kopási folyamat értelmezése.

A folyamat alapkérdése: Hol kell leállítani a gépet?

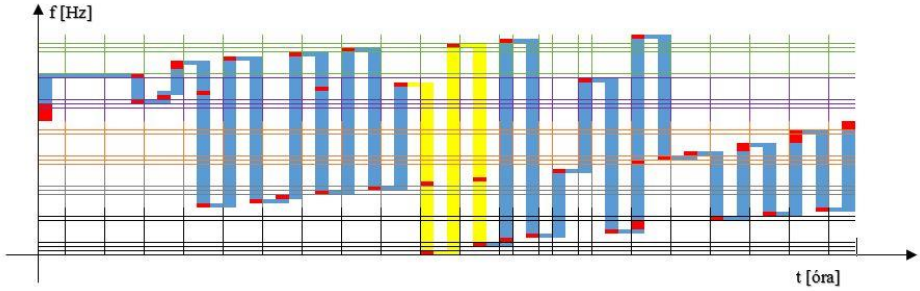
A barnamezőbe való belépéskor már sérülni kezd a csapágykosár is, ekkor már nem előzhető meg időben egy tervszerűtlen leállás, mert előfordulhat, hogy nagyobb terhelési állapotban felgyorsított lesz a roncsolódás.

Az ésszerű leállást akkor kell megtenni, amikor a tengelybeállítási frekvencia legnagyobb rendszáma belép a kopási térkép területére (5. ábra sárgamező és 6-8. ábrák kiterjesztett sárgamező), vagyis a feketemező baloldal felőli első pirosmezője. Ha itt leállítjuk a gépet, akkor még nem történhet túl nagy károkozás. Ennek a tervszerű leállítási folyamatnak a szemléltetésére készült az 5-6. ábrák, ahol a sárgamezők jelentik a leállási sávokat. A keskeny sárgasáv egy olyan rész, ahol az első figyelmeztető jelzést célszerű (5. ábra) kiadni a gépről. Viszont még nem történik jelentős hiba. Ha megvárjuk a 7. ábra szerinti kiterjesztett sárgamező szélesedő területét, akkor maradandó roncsoló hatás keletkezik Ezek a mezők frekvencia-amplitúdó (harmonikus rendszámmal) tartományban vizsgálják a jelek előfordulását. Ezt megelőző belső és külső gyűrű, valamint gördülő elemek frekvencia tartományait célszerű minél több matematikai transzformációval figyelni. Történik-e durva ugrás vagy lengés a hajtásrendszerben? Ha igen, akkor honnan származik milyen hatást gyakorol a géprendszerre?



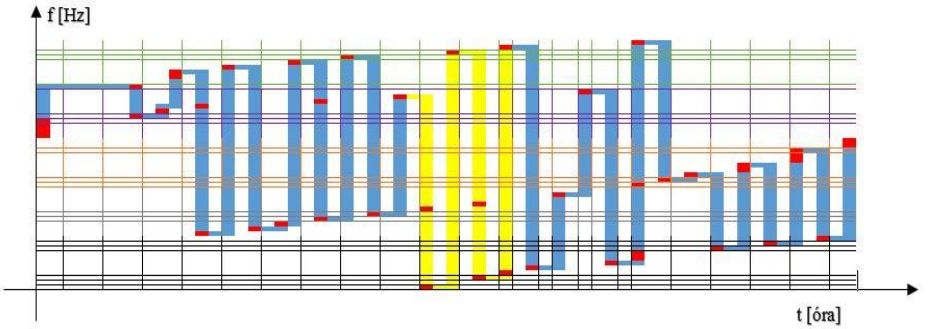
5. Ábra. Csapágy kopási folyamatábrája határmezővel. (Jelölések: f: motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).

A 6. ábra a második kiterjesztett leállómező, sárgamező, a tengelybeállítási frekvencia (fekete négyzetsáv) kezd belépni a kopási térképre. Itt már feltétlen szükséges jelezni a felhasználó felé a tervszerű leállás szükségességét.



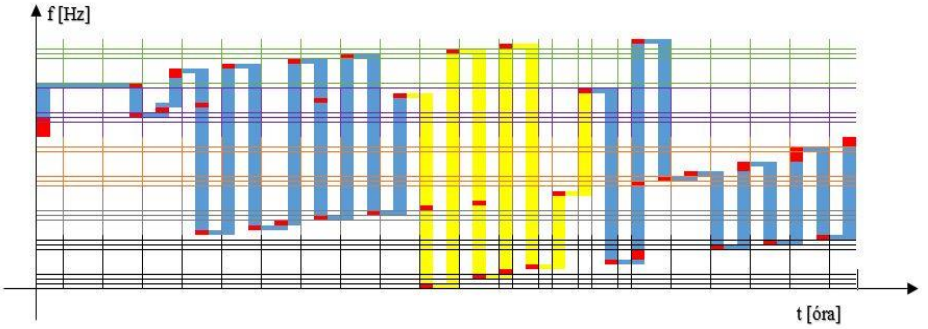
6. Ábra. Csapágy kopási folyamatábrája kiterjesztett határmezővel.
(Jelölések: f: motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).

A 7. ábra már a tervezett leállás kritikus utolsó teljes szakasza, kritikus stádium.



7. Ábra. Csapágy kopási folyamatábrája leállómezővel, kritikus stádium.
(Jelölések: f: motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).

A 7. ábra egy olyan kiterjesztett állapot, ahol a leállást már meg kell tenni. Az átlépés a tengelybeállítási frekvenciáknak már több tagja jelen van (fekete rácsmező), a gördülő elemeknek kettő, a belső gyűrű még nem ad alacsony frekvenciájú részt, a külső gyűrű viszont kettő komponenssel van jelen (zöld rácsmező), ha csak a sárgamezőt elemezzük. Ha itt sem történik meg, akkor még folytatódik a hibaelemzés a belső gyűrű következő frekvencia jelének belépéséig (8. ábra szerint).



8. Ábra: Csapágy kopási folyamatábrája végső leállómezővel, kritikus stádium.
(Jelölések: f: motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).

A 8. ábra a végső szélesített leállómezőt jelzi (szélesített sárga útvonal). A szélesítés oka, hogy megvárta az elemző még a ciklus első szakaszában a korábban csak nagyobb frekvencia tartományban előforduló belső gyűrű hibafrekvencia újra belép a kopási útvonalba (lilarács-mező). A tervszerű leállást 5-6. ábrák szerint célszerű megtenni.

A gyakorlatban mindig kulcskérdés: Mennyi biztonsági tartalék van még hátra? A 8. ábra szerint már nincs, ekkor elhasználta a csapágy a középkorú élettartam ciklusát.

Sáv	Elem	Összes lépés	Sárgamezőben lévő lépések	Különbözet
Zöld	Külső gyűrű	113	36	77

Lila	Belső gyűrű	194	59	135
Barna	Kosár	216	60	155
Szürke	Gördülő elemek	220	63	157
Fekete	tengelyütés	81	53	28
Összesítés		833	307	526

3. Táblázat: Lépésszámok áttekintése a különböző mezőkben (8. ábra szerint), (szerzői táblázat).

Sáv	Elem	Összes lépés	Sárgamező	Különbözet
Zöld	Külső gyűrű	113	36	77
Lila	Belső gyűrű	194	59	135
Szürke	Gördülő elemek	220	63	157
Fekete	Tengelyütés	81	53	28
Összesítés		608	211	397

4. Táblázat: Lépésszámok csökkentésének lehetőségei, (szerzői táblázat).

Sáv	Elem	Elem	Összes lépés	Különbözet
Zöld	Külső gyűrű	113	36	77
Lila	Belső gyűrű	194	59	135
Fekete	Tengelyütés	81	53	28
Összesítés		388	148	240

5. Táblázat: Lépésszámok csökkentésének lehetőségei, gördülő elemszámítás kihagyással, (szerzői táblázat).

Sáv	Elem	Elem	Összes lépés	Különbözet
Zöld	Külső gyűrű	113	36	77
Fekete	Tengelyütés	81	53	28
Összesítés		194	89	105

6. Táblázat: Lépésszámok csökkentésének lehetőségei. Legszerűbb állapot, felülvizsgálatra szorul, (szerzői táblázat).

Sáv	Elem	Elem	Összes lépés	Különbözet
Zöld	Külső gyűrű	113+10	36	87
Fekete	Tengelyütés	81	53	28
Összesítés		204	89	115

7. Táblázat: Lépésszámok csökkentésének lehetőségei. Lépésszám visszaállítási módszer, ha túl kevés a számítás a kopási folyamat előre jelzéséhez, (szerzői táblázat).

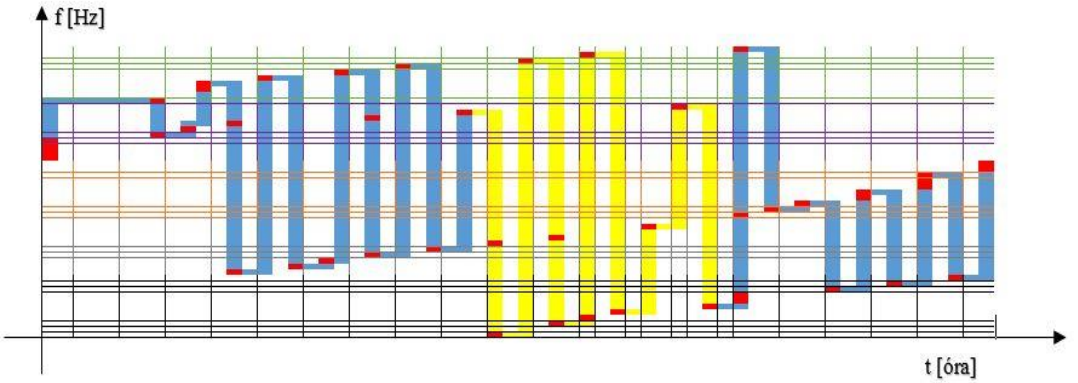
Belső gyűrű mezőnek 4+6 lépése bevonás miatt (7. táblázat).

KOPÁSI FOLYAMATÁBRA ELŐREJELZŐ MÓDSZEREK KIDOLGOZÁSÁVAL, ÖSSZEFOGLALÁS

A korábbi kopási folyamat eredményeképpen felmerül az igény, hogy ne legyen szükség kivárni a kisebb frekvenciájú jelleg-mezők megjelenését. Az öt alkotó rácsmezőt, a külső, belső gyűrű, kosár, gördülő elemek, tengelyütési frekvencia közül el kell hagyni azon elemeket, amely a kisebb frekvencia mezőn dolgoznak.

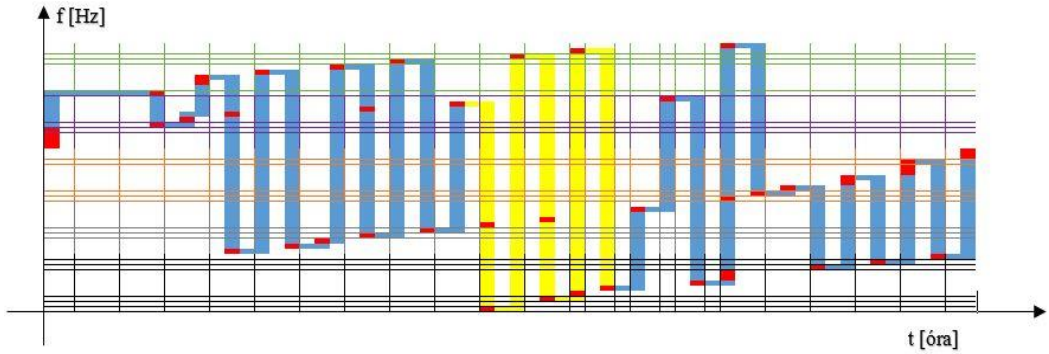
Végig haladva a kopási folyamaton a 9. ábra szerint, a kritikus mező szűkítése. Elképzelések:

- Haladási mezők áttekintése
- Leállási mezők felmérése
- Lépésszám-csökkentés
- Belépő mezők elemzése
- Mezőkihagyások és visszalépések



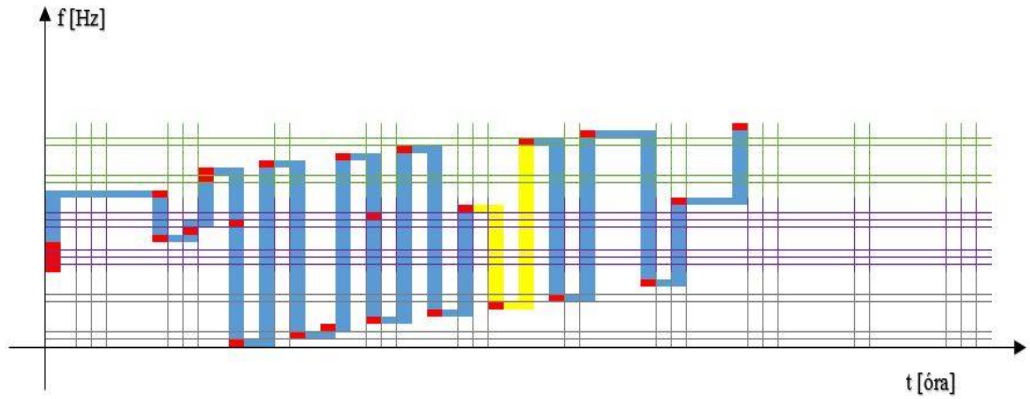
9 Ábra: Csapágy kopási folyamatábrája végső leállómezővel, kritikus stádium (sárgamező). (Jelölések: f: motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).

A 9. ábra haladási lépéseit le kell csökkenteni (a korábbi 8. ábra). Az első lépés a 10. ábra szerinti kosár frekvencia kihagyása, mert kisebb frekvenciatartományban mozog, illetve a roncsolódás jelenléte hatással lesz mindegyik alkotóelemre, ezért feltételezhető a fokozott kopás.



10. Ábra. Kosár frekvenciát kiejtő kopási algoritmus futási folyamatábrája.
(Jelölések: f: motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).

A 11. ábrán már nem szerepel a kosár frekvencia, az előre jelzési sáv kisebb lesz (sárgamező). Ekkor az algoritmus a sárgamező kezdő és végpontjára eső pirosmezőkre érvényes frekvencia értékekhez tartozó amplitúdóeloszlást vizsgálja. A kritikus szakasz elemzése során felmerül a további lehetőség arra, ha el kell kerülni a legkisebb tengelyütést is, akkor az erre eső legnagyobb frekvencia komponenst is meg kell előzni.



11. Ábra Tengelybeállítási és kosár frekvenciákat kiejtő kopási algoritmus futási folyamatábrája.
(Jelölések: f: motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).

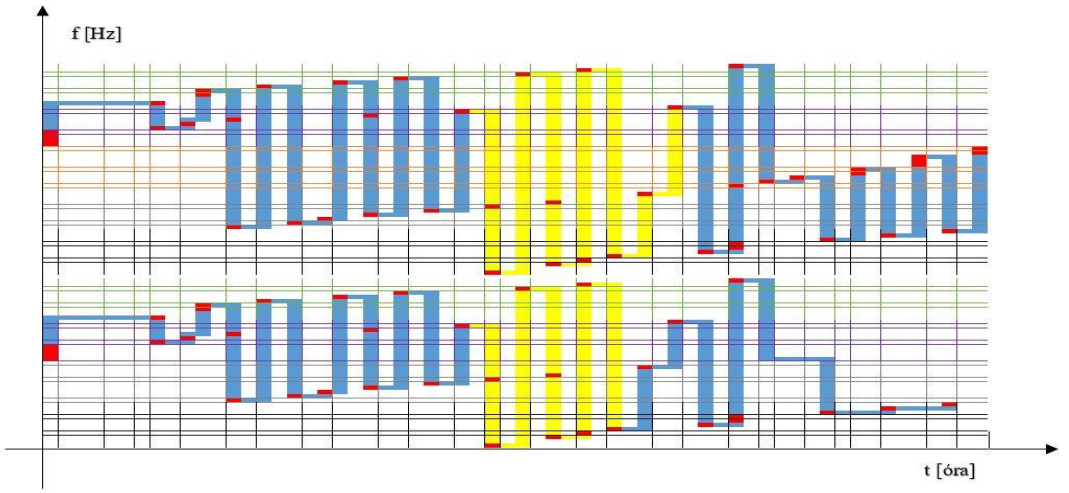
A 11. ábra szerinti algoritmus kezdőpontja a belső gyűrű a végső pontja a külső gyűrű frekvencia összetevője, közben áthalad a gördülő elemek lilamezőjén. Ebben az esetben a leállási sárgamező belső és külső gyűrű két frekvencia komponense között van úgy, hogy egy gördülő elem frekvencia rész esik a futási folyamatába, vagyis erre az esetre vizsgál amplitúdóeloszlást.

Algoritmus konklúziója

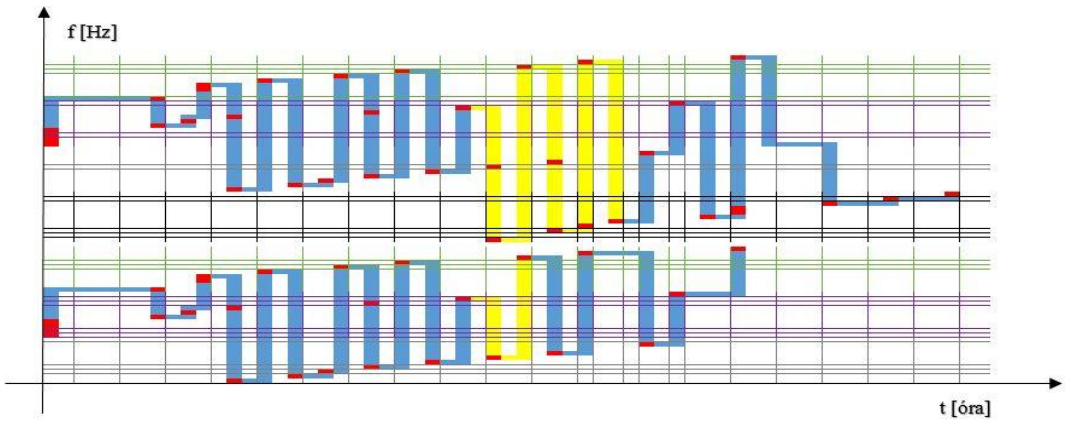
Az egyszerűsítés indoka lehet az a tény, hogy el kell dönteni az információ és zaj egymásra hatását. Ha kisebb jel teljesen eltérő frekvenciatartományban dolgozik, akkor ne fusson le úgy egy algoritmus, hogy végigelemez egy olyan részt, amelyben még több zaj van, mint hasznos információ. Itt beszélhetünk ellenőrzött tanulási folyamatról.

Kopási algoritmus egyszerűsítési életciklusa

A kopási folyamatábra ellenőrzött tanulási folyamat alatt a 12-13. ábrák szemléltetik. Az ábrák célja megmutatni a korábbi fejezetben bemutatott egyszerűsítési folyamat lépéseit közvetlen kapcsolódó képekkel.



12. Ábrák: Csapágy kopási folyamatábrája egyszerűsítés módszerével. (Jelölések: f: motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).



13. Ábra: Csapágy kopási folyamatábrája egyszerűsítés módszerével, vizsgálati mezők csökkentésének folyamata. (Jelölések: f: motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).

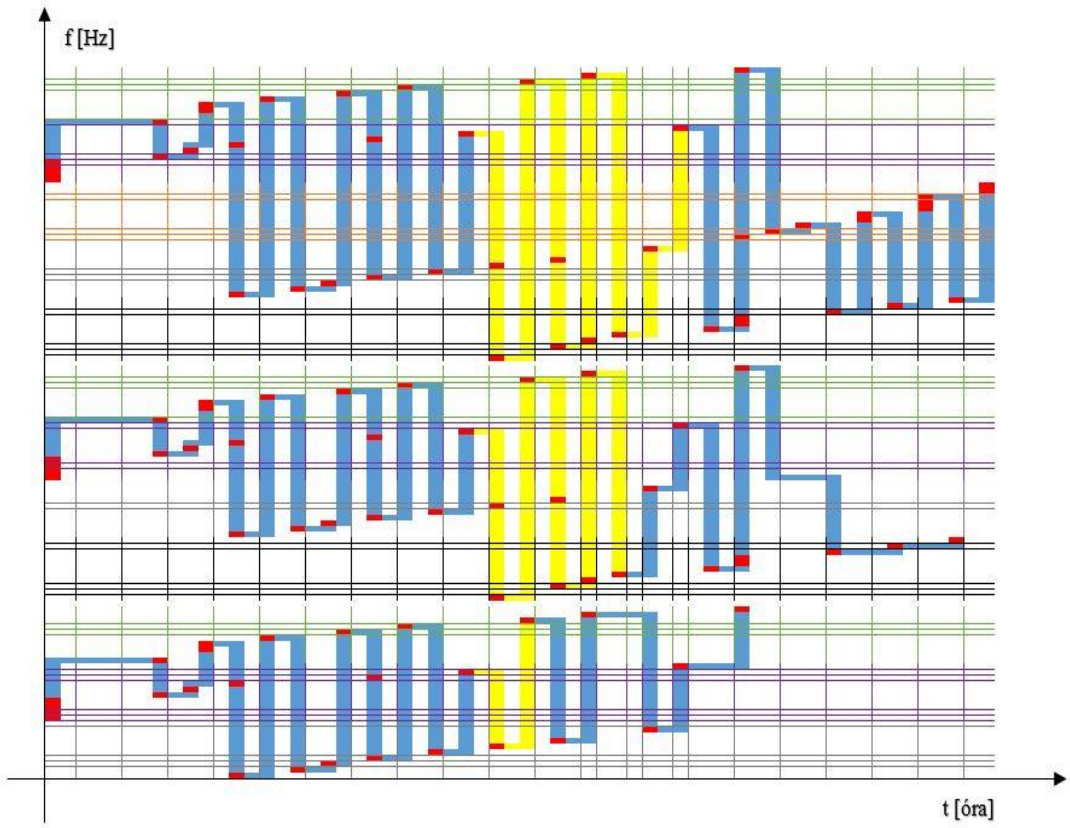
A 14. ábra az egyszerűsítő elemzésnek összesített folyamata, az futási folyamat ebben az esetben frekvencia komponenscsökkentésre összpontosít.

Tovább fejlesztési lehetőségek

- Csapágyfrekvencia mezők felcserélése, mezőáthaladási pontok csökkentése.
- Jelenleg frekvencia komponensek alapján rendez lépési sorrendet, ennek változtatása.
- A jellegmezők amplitúdóeloszlás alapján történő vizsgálata.

- Közeleső frekvencia kapcsolatok elemzése.
- Lehetséges-e hibafrekvencia kihagyás (pirosmező)?
- Milyen egyszerűsítési folyamat állíthatók elő?
- Visszalépések számának vizsgálata

A tengelyütési frekvencia mező nem feltétlen hagyható el. A villamos hajtás technológiai folyamata nagyrészt meghatározza ezt a kérdést és sok esetben a tengelybeállításra összpontosítanak. Elméletben vizsgálható így, mint korai előrejelzés, de a legnagyobb harmonikus esetén vizsgálni kell, hogy mikor lép be a jellegmezőre, erre szolgál 14. ábra összehasonlítása. A kialakított hibametria további felülvizsgálatra szorul.



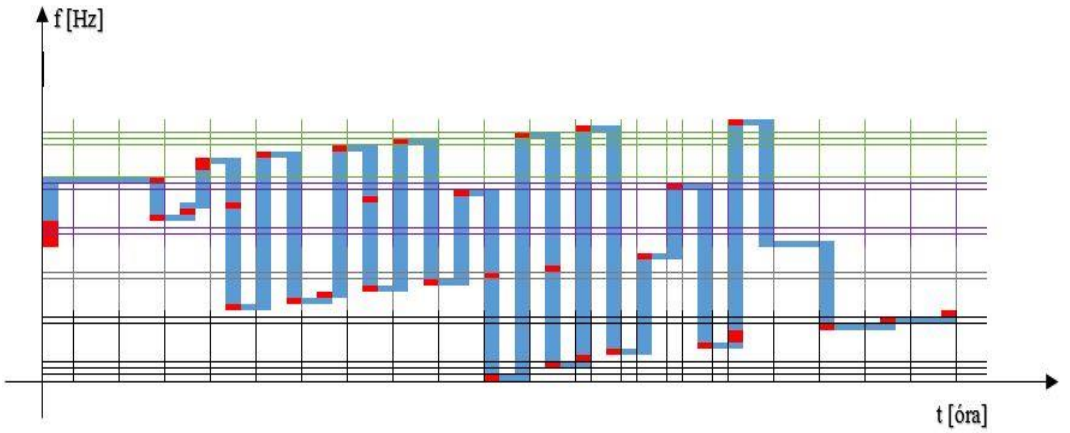
14. Ábra: Csapágy kopási folyamatábrája mindhárom egyszerűsítési jellegmezővel. A legfelső mind az öt jellegmezőt tartalmazza. A középső a kosár frekvenciát hanyagolja el, a legalsó pedig már a tengelyütési frekvenciát is. (Jelölések: f.motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).

A kopási folyamat egysoros mélyhornyú golyós csapágyra készült. Vannak olyan gépek, ahol nagyobb terhelés miatt más típust alkalmaznak. Ebben az esetben a kopási folyamat frekvencia és amplitúdó eloszlással, harmonikusokkal felírja a kopási mezőket. Gyakran előfordul, hogy számos ismeretlen frekvencia komponens van jelen, ekkor zajelemzés is nagy hangsúlyt kap. A mérésekben van abszolút hiba is, a mérőrendszere, a frekvencia átvitelre is jellemző eltérések, erre külön hibamezők hozhatók létre, függően attól, hogy milyen eszközzel történik a mérés.

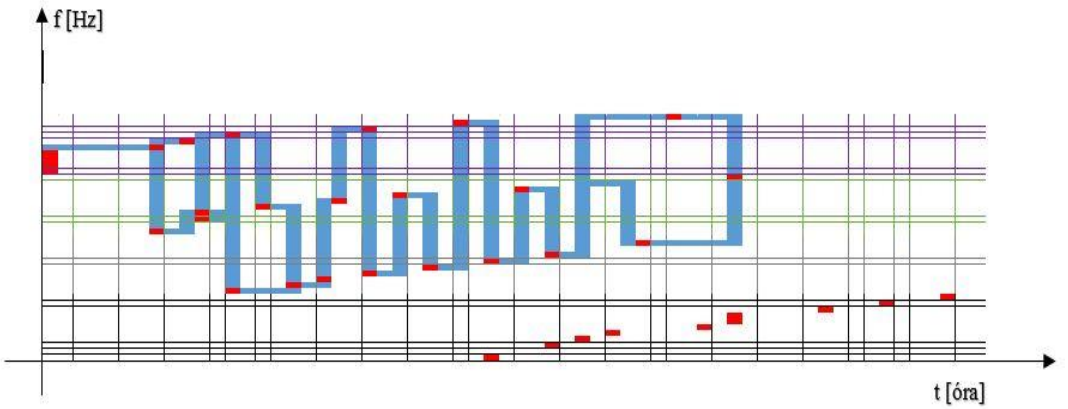
A bemutatott eredmények villamos forgógépekkel történt mérésekből származnak. Hibridhajtások esetén akkor használhatóak, ha villamos forgógép mechanikai összeköttetésben van (nem történik szétkapcsolás) a belsőégésű motorral, ekkor további elemzési lehetőségek lépnek életbe.

KOPÁSI ALGORITMUS VISSZACSATOLÁSI, ÚJRA ELEMZÉSI LEHETŐSÉGEK ÁTTEKINTÉSE

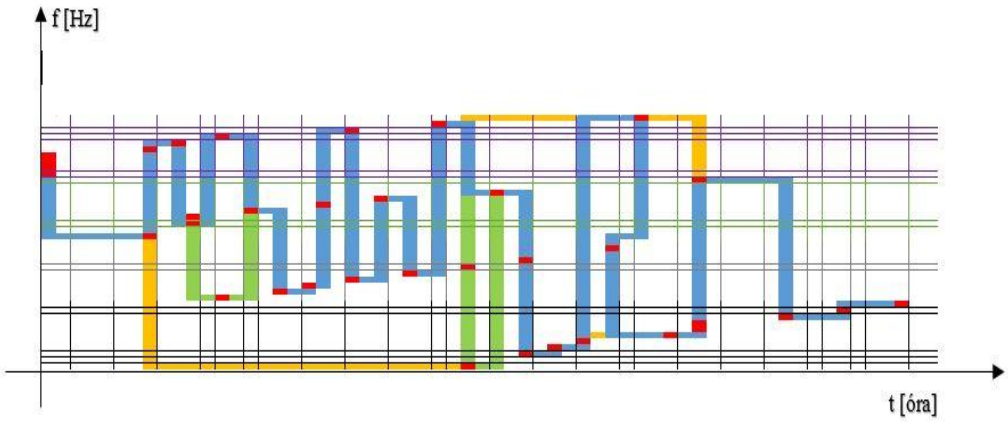
A kutatási eredmény összefoglalásaként nem nélkülözhető a visszacsatolási folyamat és az útvonal kiejtésének gondolata. A kékmező haladási vonala a normál életciklusnak felel meg, ezt a folyamatot meg kell ismerni a géprendszerben, viszont nem oldja meg az előre jelzés tanuló folyamatát, így nem lehet tanulásnak nevezni, ha mindig ugyanazon útvonalakon halad végig. Ennek eredményeképpen készültek a 15-18. ábrák, amik mutatják a mezőcserét és az útvonal felülvizsgálati lehetőségeket.



15. Ábra: Kopási algoritmus mezőfordítással. A belső (lilamező) és külső gyűrű (zöldmező) haladási irány felülvizsgálat szempontjából. (Jelölések: f.motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).

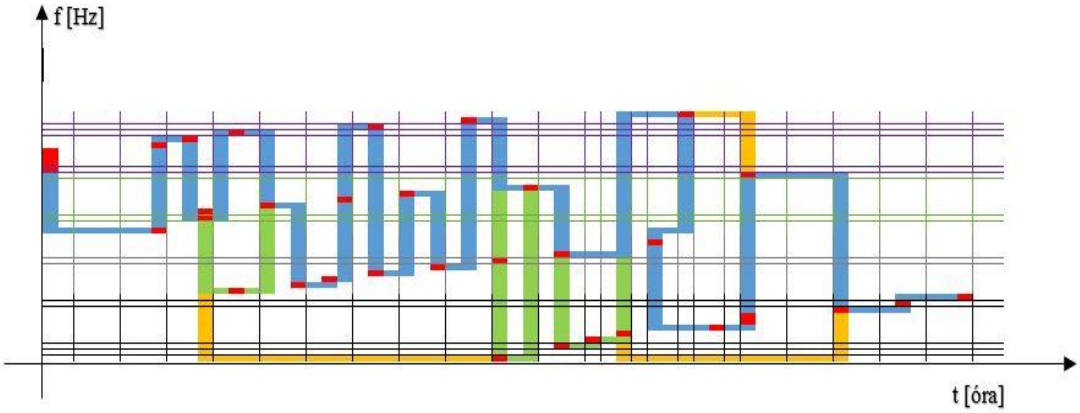


16. Ábra: Kopási algoritmus mezőfordítással és tengelyütési frekvencia rész kihagyással. A belső (lilamező) és külső gyűrű (zöldmező) haladási irány felülvizsgálat szempontjából.(Jelölések: f: motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).



17. Ábra: Kopási algoritmus visszacsatolási útvonalakkal (narancssárga mezők) és kihagyási útvonalakkal (zöldmező). (Jelölések: f: motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).

A gépcsoport futtatási periódusa attól függ, hogy milyen üzemtípusra tervezik a gépet (pl.: folyamatos, szakaszos, szakaszos fékezés, forgásirányváltás, indítási tranziensek gyakorisága). Lehet végezni gyorsított öregítési módszereket (felmelegítés) vagy mesterséges sérülés okozása a csapágynak, tengelynek. A gyorsítási módszerek akkor használhatók eredményesen, ha számolnak azzal a tényezővel, hogy milyen járulékos hatást eredményez (pl.: kenőanyag-elvétel).



18. Ábra: Kopási algoritmus visszacsatolási útvonalakkal (narancssárga mezők) és kihagyási útvonalakkal (zöldmező), optimumkeresési folyamattal. (Jelölések: f: motor állórész áramfrekvencia [Hz]; t idő [óra]), (szerzői ábra).

A 15. ábra egy olyan esetet mutat, amikor a külső és belső gyűrű jellegmezője fel van cserélve. A lila lés a zöldmező, tehát a belső gyűrű rácsvonala került a felső tartományba lépés korrigálás céljából. Ez még önmagában egy lehetőség, a következőben meg kell változtatni az útvonalat is. A narancssárga és zöldmezők jelzik a módosításokat. A zöldmező lehet lépéskihagyás esete, a narancssárga mező pedig visszatérő útvonal, feltéve, ha a zöldmezőn keresztül történik a visszalépés. A lépés kihagyás nem feltétlen azt jelenti, hogy egy-

általán nem fut rajta a tanuló algoritmus, hanem azt, hogy ha keresi a következő hiba összetevőt, akkor frekvencia prioritás szerint nem ugrál harmonikus rendszám szerint sorba, hanem lép a következő kritikus pontra. Ennek első változatait mutatja 15. ábra. A 16. ábra arra a változatra világít rá, amikor a folyamat elkezdi felmérni a tengelybeállítási frekvencia összetevők jelenlétét. A külső gyűrű első harmonikusából (zöldmező) a belső gyűrű (lilamező) első harmonikusán keresztül az elemző ciklusba. Ez egy rész folyamat, megnyitja a tengelybeállítási folyamat elemzését és lezárja a csápágy külső és belső gyűrű elemzését. Nem a teljes algoritmus áll meg, hanem részfolyamatot vizsgál. A 17. ábra már egy olyan rész, ahol ellenőrizni kell, a létrehozott kopási folyamatot, erre szolgál visszatérő narancssárga rész. A 18. ábra a tengelybeállítási frekvenciamezőből visszatérő algoritmus. Erre azért van szükség, mert a folyamatábra segítségével fel lehessen mérni, hogy melyik frekvencia összetevő kell újra vizsgálni.

Modellek jelenlegi hiányosságai

- A kopási folyamat ábra visszalépési szabályait pontosítani kell
- A harmonikus prioritás nem oldja meg feltétlen a kopási folyamatelemzést, mert az alaktotó elemek különböző frekvenciasávokban jelennek meg. Így ha alapvetően eltérő a frekvenciatartomány, akkor növelni kell a vizsgálati szakaszt, vagyis több mezőt kell létrehozni.
- A kopási folyamatlépés kihagyási mezőit ki kell dolgozni és ellenőrizni, mérési és számítási eredményekkel alátámasztva.
- Csapágy elhasználódás mértékére utaló útvonalak kidolgozása.
- Mezőcsere lehetőségek további elemzése szükséges.

A további célok közé tartozik, hogy az amplitúdó, frekvencia, harmonikus rendszám és alkatrész komponens alapján az amplitúdóváltozás milyen mértékben módosítja a kopási folyamat végig haladási változatait és visszacsatolásait.

ÖSSZEFOGLALÁS

Kutatás első fázis eredménye, hogy spektrumképzések nem feltétlenül oldják meg az áramspektrum alapján a kopások korai felismerését. Ennek az az oka, hogy számos frekvenciák (modulációk) hatnak egymásra. A jellegmezős ábrázolás célja egy térképszerű megközelítés, ami hatékony szemléltetést és lépésszabály felállítását elősegíti. A különböző színskálák a követhetőséget segítik elő, illetve felhasználhatók a kopási útvonalak átmenetének bemutatásához. A jelenlegi állás még kezdeti stádiumnak tekinthető olyan szempontból, hogy az idő, mint kritikus tényező, hogyan definiálható a kopási folyamat során. Üzemidő, hőmérséklet, kenés, páratartalom és más külső beavatkozások hozzájárulnak a gép életciklusának formálódásához.

A kopási térkép arra szolgál, hogy megmutatja frekvencia, harmonikus, alkotóelem szerinti folyamat lezajlását (feltételezett jellegviselkedését) és egymásra hatásukat. A lépések kigondolása ilyen mezőkön jól követhető és különböző útvonalak dolgozhatók ki, amelyek előre jelzési folyamatot előkészítik és segítik. A mérési alapú kutatások jelenleg abban a fázisban vannak, hogy a kopási mezők nagy és kis frekvenciás tartományaira külön-külön vizsgáló szabály szükséges.

FELHASZNÁLT IRODALOM

[1] Jean-Claude Trigeassou, Electrical Machines Diagnosis, First published, 2011, Great Britian and the United States by ISTE Ltd and John & Sons, Inc. ISBN 978 1 84821 263 3

[2] Bendiák István, *Forgógépek diagnosztikai eljárásai és alkalmazási lehetőségük felmérése*, Tudományos Diákköri Konferencia, Budapest, Felelős kiadó: Prof. Dr. Kovács Levente Adalbert az Óbudai Egyetem rektora, 2020, ISBN 978-963-449-204-7

[3] Bendiák István, *Aszinkron motorok mechanikai jellemzőinek vizsgálata áram jelalakanalízis módszerével,* Diplomamunka, Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar, 2020, Budapest

[4] B. Noureddine, P. Remus, R. Raphael and S. Salim, "*Rolling Bearing Failure Detection in Induction Motors using Stator Current, Vibration and Stray Flux Analysis Techniques*," IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society, Singapore, 2020, pp. 1088-1095, doi: 10.1109/IECON43393.2020.9254401.

[5] S. R. Kapoor, N. Khandelwal and P. Pareek, "*Bearing fault analysis by signal energy calculation based signal processing technique in Squirrel Cage Induction Motor*," 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014), Ajmer, India, 2014, pp. 33-38, doi: 10.1109/ICSPCT.2014.6884922.

[6] J. Xinjie, H. Malik and S. K. Panda, "*An Optimized Intelligent Technique for Bearing Fault Diagnosis using Motor Current Signal Analysis*," 2022 International Power Electronics Conference (IPEC-Himeji 2022- ECCE Asia), Himeji, Japan, 2022, pp. 730-735, doi: 10.23919/IPEC-Himeji2022-ECCE53331.2022.9807128.

[7] M. S. Moiz et al., "*Health Monitoring of Three-Phase Induction Motor Using Current and Vibration Signature Analysis*," 2019 International Conference on Robotics and Automation in Industry (ICRAI), Rawalpindi, Pakistan, 2019, pp. 1-4, doi: 10.1109/ICRAI47710.2019.8967356.

[8] J. Jung et al., "*Monitoring of journal bearing faults based on motor current signature analysis for induction motors*," 2015 IEEE Energy Conversion Congress and Exposition (ECCE), Montreal, QC, Canada, 2015, pp. 300-307, doi: 10.1109/ECCE.2015.7309702.

[9] W. Zhou, T. G. Habetler, R. G. Harley and B. Lu, "*Incipient Bearing Fault Detection via Stator Current Noise Cancellation using Wiener Filter*," 2007 IEEE International Symposium on Diagnostics for Electric Machines, Power Electronics and Drives, Cracow, Poland, 2007, pp. 11-16, doi: 10.1109/DEMPED.2007.4393064.

[10] R. Pusca, R. Romary, N. Bessous and S. Sbaa, "*Comparative Study between Two Diagnostic Techniques Dedicated to the Mechanical Fault Detection in Induction Motors*," 2020 International Conference on Electrical Engineering (ICEE), Istanbul, Turkey, 2020, pp. 1-8, doi: 10.1109/ICEE49691.2020.9249884.

[11] J. Jung et al., "Monitoring Journal-Bearing Faults: *Making Use of Motor Current Signature Analysis for Induction Motors*," in IEEE Industry Applications Magazine, vol. 23, no. 4, pp. 12-21, July-Aug. 2017, doi: 10.1109/MIAS.2016.2600725.

[12] P. Pareek, N. Khandelwal and S. R. Kapoor, "*A new approach for bearing fault analysis in Squirrel Cage Induction Motor*," 2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), Delhi, India, 2016, pp. 1-6, doi: 10.1109/ICPEICES.2016.7853090.

[13] G. Avalos, S. Aguayo, J. Rangel-Magdaleno and M. R. A. Paternina, "*Bearing fault detection in induction motors using digital Taylor-Fourier transform*," 2022 International Conference on Electrical Machines (ICEM), Valencia, Spain, 2022, pp. 1830-1835, doi: 10.1109/ICEM51905.2022.9910779.

[14] N. Bessous, S. E. Zouzou and A. Chemsa, "*A new analytical model dedicated to diagnose the rolling bearing damage in induction motors - simulation and experimental investigation* -," 2016 4th International Conference on Control Engineering & Information Technology (CEIT), Hammamet, Tunisia, 2016, pp. 1-9, doi: 10.1109/CEIT.2016.7929085.

[15] E. Elbouchikhi, V. Choqueuse, F. Auger and M. E. H. Benbouzid, "*Motor Current Signal Analysis Based on a Matched Subspace Detector*," in IEEE Transactions on Instrumentation and Measurement, vol. 66, no. 12, pp. 3260-3270, Dec. 2017, doi: 10.1109/TIM.2017.2749858.

[16] N. Khandelwal, P. Pareek and S. R. Kapoor, "*Start-up transient current analysis for Squirrel Cage Induction Motor*," 2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), Delhi, India, 2016, pp. 1-6, doi: 10.1109/ICPEICES.2016.7853261.

[17] A. Soualhi, G. Clerc and H. Razik, "*Detection and Diagnosis of Faults in Induction Motor Using an Improved Artificial Ant Clustering Technique*," in IEEE Transactions on Industrial Electronics, vol. 60, no. 9, pp. 4053-4062, Sept. 2013, doi: 10.1109/TIE.2012.2230598.

[18] Yong Li and Tengxi Wang, "*Signal segmentation for isolating the influence of PQ variation and machine manufacturing imperfections on bearing fault detection*," 2013 International Electric Machines & Drives Conference, Chicago, IL, USA, 2013, pp. 734-741, doi: 10.1109/IEMDC.2013.6556175.

[19] A. Husna, K. Indriawati and B. L. Widjiantoro, "*Discriminant Feature Extraction of Motor Current Signal Analysis and Vibration For Centrifugal Pump Fault Detection*," 2021 International Conference on Instrumentation, Control, and Automation (ICA), Bandung, Indonesia, 2021, pp. 207-212, doi: 10.1109/ICA52848.2021.9625679.

[20] E. T. Esfahani, S. Wang and V. Sundararajan, "*Multisensor Wireless System for Eccentricity and Bearing Fault Detection in Induction Motors*," in IEEE/ASME Transactions on Mechatronics, vol. 19, no. 3, pp. 818-826, June 2014, doi: 10.1109/TMECH.2013.2260865.

[21] B. Raison, G. Rostaing, O. Butscher and C. . -S. *Maroni, "Investigations of algorithms for bearing fault detection in induction drives*," IEEE 2002 28th Annual Conference of the Industrial Electronics Society. IECON 02, Seville, Spain, 2002, pp. 1696-1701 vol.2, doi: 10.1109/IECON.2002.1185536.

[22] Y. Tian, D. Guo, K. Zhang, L. Jia, H. Qiao and H. Tang, "*A Review of Fault Diagnosis for Traction Induction Motor*," 2018 37th Chinese Control Conference (CCC), Wuhan, China, 2018, pp. 5763-5768, doi: 10.23919/ChiCC.2018.8484044.

[23] S. Zhao et al., "*The Inter-turns Short Circuit Fault Detection based on External Leakage Flux Sensing and VMD-HHT Analytical Method for DFIG*," 2021 International Conference on Sensing, Measurement & Data Analytics in the era of Artificial Intelligence (ICSMD), Nanjing, China, 2021, pp. 1-5, doi: 10.1109/ICSMD53520.2021.9670783.

A SPECIAL CASE OF HUMAN-ROBOT INTERACTION: PEPPER ROBOT IN EDUCATION

HUMÁN-ROBOT INTERAKCIÓ SPECIÁLIS ESETE: PEPPER ROBOT AZ OKTATÁSBAN

GUGOLYA László[1]

Abstract

The continuous advancement of robots is an unstoppable process. We encounter them increasingly often, both in industry and other fields. Consequently, interaction with them is inevitable, leading us to form opinions and emotions about them. This is especially true for humanoid robots. Manufacturers strive to showcase and spread their products more widely, so now we can encounter humanoid robots in stores, museums, healthcare, and educational institutions even in Hungary. A typical example is the Pepper robot, which is the largest humanoid robot available commercially. This study demonstrates how robots can be utilized in the learning and programming process within an educational institution, helping to overcome fears and increase the sense of security.

Keywords

Human-robot interaction, robot, humanoid robot, Pepper robot, education, programming education

Absztrakt

A robotok folyamatos térnyerése megállíthatatlan folyamat. Mind az iparban, mind egyéb területeken egyre gyakrabban találkozunk velük. Így elkerülhetetlen a velük az interakció, véleményünk alakul ki róluk, érzelmeink keletkeznek. Igaz ez különösen a humanoid robotok esetében. A gyártók igyekeznek egyre szélesebb körben megmutatni, terjeszteni termékeiket, így már magyarországos is találkozhatunk humanoid robotokkal áruházkában, múzeumokban, egészségügyi és oktatási intézményekben. Ez tipikusan a Pepper típusú robot, ami a kereskedelemben kapható legnagyobb humanoid robot. A tanulmányban az kerül bemutatásra, hogy egy oktatási intézményben miként lehet felhasználni a tanulási, programozási folyamatban a robotok ezzel segítve a félelmek leküzdését, a biztonságérzet növelését.

Kulcsszavak

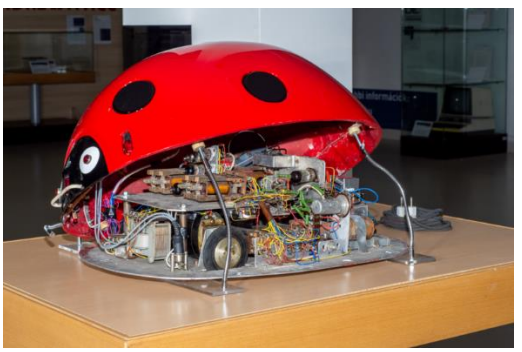
Ember-robot interakció, robot, humanoid robot, Pepper robot, oktatás, programozás oktatás

[1] gugolya.laszlo@uni-obuda.hu | ORCID: 0009-0008-8201-5893| teacher, Óbuda University Alba Regia Technical Faculty, Institute of Science and Software Engineering | mestertanár, Óbudai Egyetem Alba Regia Műszaki Kar, Természettudományi és Szoftvertechnológiai Intézet

BEVEZETÉS

A robotok története régen kezdődött, hiszen az első „történelmi” robot egy harci gép volt, ami Krétát védte, akit Talósznak hívtak[1] [2]. A 18. században megjelentek a robotállatokra (robotkacsa), a művégtagokra vonatkozó elképzelések és mindenkinek ismerős Kempelen Farkas híres, hírhedt sakkozógépe.

Magyarországi robot történetben is sok érdekességet találhatunk. A legjelentősebb a szegedi humanoid robotember, amely 1962-ben készült.[3] 24 kérdésre tudott „válaszolni”, egy ablaktörlő motorral mozgatta a fejét. Szegeden már volt ennek előzménye, a szintén Muszka Dániel által tervezet „Szegedi Katicabogár” (1957). Ez már tekinthető akár oktatás segítő robotnak (persze nem erre használták), mivel a pavlovi reflex szimulálására készítették.



1. ábra - Szegedi katicabogár

Ez a pár példa is mutatja, hogy régóta életünk, gondolkodásunk része a mesterségesen előállított „lények”, robotok világa. Természetesen ezt a világot nem lehet elválasztani a digitalizációtól, ennek hatásaitól. A kutatás központi célja, hogy elősegítse a társadalom pozitív hozzáállását a robotokhoz, azon belül is humanoid robotokhoz. Véleményünk szerint ezt az oktatás világában lehet kezdeni, hiszen itt nagyobb a fogékonyság, a fiatalabb generáció nyitottabb az újdonságra. Így elsőként nézzük meg milyen területeket érint ez a téma.

Digitális eszközök az oktatásban

A digitális eszközök használata az iskolában egyre inkább elterjedt, és számos tanulmány vizsgálta a hatásait a tanulók oktatási élményére és teljesítményére. A digitális eszközök magukban foglalják a számítógépeket, táblagépeket, interaktív táblákat és különféle oktatási szoftvereket, melyek célja a tanulás élményszerűbbé, interaktívabbá és személyre szabottabbá tétele. A digitális eszközök lehetővé teszik az interaktív tanulási környezetek kialakítását. Például a táblagépeken és interaktív táblákon futó oktatási szoftverek lehetőséget adnak a tanulóknak, hogy közvetlenül részt vegyenek a tananyag feldolgozásában, így aktívabb tanulási élményt biztosítanak. A digitális eszközök használatával a tanulók hozzáférhetnek számos online forráshoz és tananyaghoz, melyek segítik az önálló tanulást. Emellett a különböző alkalmazások és programok lehetőséget adnak a tananyag személyre szabására, figyelembe véve a tanulók egyéni szükségleteit és képességeit. Kutatások kimutatták, hogy a digitális eszközök használata növelheti a tanulók motivációját és elkötelezettségét. A

játékosított (gamifikáció) oktatási alkalmazások és a vizuálisan vonzó tananyagok segíthetnek fenntartani a tanulók érdeklődését.

Kutatásokkal kimutatható, hogy a digitális eszközök használata pozitív hatással van a tanulási eredményekre, különösen, ha a pedagógiai módszerek is megfelelően alkalmazkodnak a technológiához [4]. Másik kutatás elemezte a táblagépek iskolai használatát és arra a következtetésre jutott, hogy a táblagépek hatékonyan támogatják a kollaboratív tanulást és a kritikai gondolkodás fejlődését [5]. Az interaktív táblák használata növeli a tanulók részvételét és javítja a tanulási eredményeket, különösen az általános iskolai oktatásban [6]. Bár a digitális eszközök használata számos előnnyel jár, kihívások is felmerülnek. A megfelelő technikai infrastruktúra hiánya, a tanárok technológiai képzettsége és a túlzott képernyőidő negatív hatásai mind olyan tényezők, melyekre figyelmet kell fordítani.

Robotok, humanoid robotok az oktatásban

A humanoid robotok oktatásban való használata egyre terjedőben van, mivel javíthatják a tanulási élményt és eredményeket. Ezek a robotok emberszerű megjelenésük és viselkedésük révén képesek interaktív, személyre szabott és motiváló oktatási élményt nyújtani. A humanoid robotok képesek interaktív módon kommunikálni a tanulókkal, így elősegítik az aktív tanulást. A robotok beszéd- és mozgásképességeik révén könnyen bevonhatók különböző oktatási tevékenységekbe, például nyelvórákon, ahol a tanulók valós időben gyakorolhatják a nyelvi készségeiket. A robotok programozhatóak és testreszabhatóak, így alkalmazkodni tudnak a különböző tanulási stílusokhoz és igényekhez. Például egy tanulmány kimutatta, hogy a humanoid robotok képesek adaptív tanítási stratégiákat alkalmazni, ami növeli a tanulók elkötelezettségét és javítja a tanulási eredményeket. A humanoid robotok jelenléte növelheti a tanulók motivációját és érdeklődését az órai anyag iránt. Egy kutatás szerint a robotok alkalmazása különösen hatékony lehet a fiatalabb diákok körében, akik nagyobb valószínűséggel reagálnak pozitívan az interaktív és játékos tanulási módszerekre. Egy tanulmány azt találta, hogy a humanoid robotok hatékonyan támogatják a nyelvtanulást azáltal, hogy interaktív és személyre szabott visszajelzést nyújtanak a tanulóknak [7]. Sokan vizsgálták a humanoid robotok használatát a STEM oktatásban. Az eredmények azt mutatták, hogy a robotok javítják a tanulók problémamegoldó képességeit és kreativitását, valamint növelik a tanulási kedvet [8]. A humanoid robotok különösen hasznosak lehetnek a speciális igényű tanulók oktatásában, például az autizmus spektrumzavarral élő gyermekek esetében, mivel segíthetnek a szociális készségek fejlesztésében és az interakciók gyakorlásában [9]. A robotok mellett az oktatásban egyre nagyobb teret nyernek vezérlők programozása használata, így a közoktatásban a Micro Bit, szakoktatásban, felsőoktatásban a PLC-k [10].

A humanoid robotok oktatásban való alkalmazása számos ígéretet rejt magában, azonban nehézségek is akadnak. Ezek közé tartozik a magas költség (10 millió forint Pepper robot), a technikai karbantartás szükségessége, szoftverhiány, valamint a tanárok képzése a robotok hatékony használatához. A jövőbeli kutatásoknak továbbra is vizsgálniuk kell a humanoid robotok hosszú távú hatásait és integrációjuk módszereit az oktatási rendszerekbe.

Emberek félelmei a technológiától, robotok

Az emberek technológiától, különösen a robotoktól való félelme egy komplex jelenség, amely számos pszichológiai, szociológiai és kulturális tényezőre vezethető vissza. A robotok és más fejlett technológiák iránti félelem gyakran a bizonytalanságból, a munkahelyek elvesztésétől való aggodalomból, valamint az emberi irányítás és biztonság kérdéseiből fakad. Számos tudományos kutatás foglalkozik ezzel a témával, feltárva a félelmek okait és következményeit.

Az emberek gyakran félnek az ismeretlentől és a fejlett technológiák, különösen a robotok, gyakran ismeretlennek tűnnek. A félelemérzet, biztonságérzet fogalmai egyidősek velünk, végig követhető az emberi történelmünk során [11]. A robotok emberi tulajdonságokkal való felruházása paradox módon növelheti a félelmet, mivel ezek a tulajdonságok az emberek számára fenyegetőnek tűnhetnek. Az automatizáció és a robotizáció egyik leggyakoribb félelme a munkahelyek elvesztése. Sokan attól tartanak, hogy a robotok és az automatizált rendszerek helyettesítik az emberi munkát, különösen az alacsonyabb képzettséget igénylő munkakörökben. A robotokkal és mesterséges intelligenciával kapcsolatos etikai és biztonsági kérdések is jelentős félelmeket generálnak. Az emberek attól tartanak, hogy a robotok feletti kontroll elveszhet, és a technológia káros hatásokkal járhat az emberi társadalomra nézve. Ezt a hatást a média is erősíti. Egy tanulmány a technofóbia jelenségét vizsgálta, és megállapította, hogy a technofóbia, vagyis a technológiától való irracionális félelem, számos pszichológiai tényezőre, például az alacsony önbizalomra és az ismeretlentől való általános félelemre vezethető vissza [12]. Egy másik kutatás a robofóbia, vagyis a robotoktól való félelem jelenségét elemezte. A kutatás szerint a robofóbia gyakran összefügg a robotok emberi tulajdonságainak mértékével, és hogy az emberek hogyan érzékelik a robotok társadalmi szerepét [13]. Egy tanulmány a munkahelyek elvesztésétől való félelmet vizsgálta, és megállapította, hogy a robotok és az automatizáció elterjedése jelentős szorongást okozhat a munkavállalók körében, különösen az alacsony képzettségű munkavállalók körében [14].

A technológiától és robotoktól való félelem kezeléséhez szükség van átfogó tájékoztatásra és oktatásra, amely segíti az embereket abban, hogy megértsék a technológia előnyeit és korlátait. Emellett fontos a munkaerő átképzése és a technológiai fejlődés etikai szabályozása, hogy csökkentsük a félelmeket és elősegítsük a társadalmi elfogadást.

Emberek-robot interakciók

A humanoid robotok emberi megjelenésük és viselkedésük révén különleges lehetőségeket kínálnak az interakciók során, amelyek befolyásolhatják az emberi viselkedést, érzelmeket és társadalmi normákat. A humanoid robotok emberszerű megjelenése és viselkedése lehetővé teszi, hogy az emberek könnyebben kommunikáljanak velük. Ez a hasonlóság megkönnyítheti az elfogadást és az interakciót, különösen akkor, ahol a személyes érintkezés fontos, például az egészségügyben és az oktatásban. Kutatások kimutatták, hogy az emberek hajlamosak érzelmi kötődést kialakítani humanoid robotokkal, különösen, ha azok képesek alapvető érzelmeket kifejezni és reagálni az emberi érzelmekre. Ez az érzelmi kötődés növelheti a robotokkal való együttműködési hajlandóságot és a pozitív interakciókat. A humanoid robotok sikeresen használhatók az egészségügyben, például idősek ápolásában és rehabilitációjában, mivel képesek érzelmi támogatást nyújtani és motiválni a betegeket a terápiás

gyakorlatok során [15]. Az emberek pozitívan reagálnak azokra a humanoid robotokra, amelyek képesek érzelmeket kifejezni, ami növeli az interakciók minőségét és az elégedettséget [16].

Kollár[20] tanulmánya az ember-robot interakció elméleti oldalát tárgyalja. A szerző az emberi viselkedés és érzelemelméletek segítségével vizsgálja, hogy miért és hogyan alakul ki az emberekben a robotok iránti érzelmi kötődés. Az elméleti keretbe ágyazva a tanulmány a szociális robotok szerepét és hatását elemzi, különös tekintettel a bizalom, empátia és az érzelmi intelligencia fogalmaira. A szerző arra a következtetésre jut, hogy a robotok szerethetősége nagymértékben függ attól, mennyire képesek emberi módon kommunikálni és interakcióba lépni, valamint mennyire illeszkednek be a társadalmi normákba és elvárásokba.

Kollár és Ványa [19] tanulmányában az ember-robot interakció empirikus oldalát elemzik. Ez a kutatás az előző tanulmány folytatása. A kutatás célja, hogy feltárja, milyen tényezők befolyásolják az emberek hozzáállását és érzelmi reakcióit a robotokkal szemben. A tanulmány több kutatás (kérdőív, interjú) eredményeit mutatja be, amelyek robotokkal való interakciókkal kapcsolatosak. Külön kiemelendő a robotok katonai felhasználásának vizsgálata, ennek következményeinek elemzése. A kutatók arra a következtetésre jutottak, hogy az emberek érzelmi reakciói nagyban függenek a robotok kinézetétől, funkcionalitásától, és a velük való interakció minőségétől. Az empirikus adatok szerint a barátságos megjelenésű és viselkedésű robotok nagyobb eséllyel váltanak ki pozitív érzelmeket és elfogadást az emberekből.

A humanoid robotok és emberek közötti interakciók nem egyszerűek hiszen vannak technológiai korlátok, az etikai kérdések és a robotok megbízhatósága. A jövőbeli kutatások célja, hogy tovább fejlesszék a robotok érzelmi intelligenciáját, valamint biztosítsák az emberek biztonságát és jólétét az interakciók során.

A KÖRNYEZET

A kutatásban résztvevő humanoid robotok egy vidéki nagyváros digitális élményközpontjában találhatók. Az élményközpont a város támogatásával működik, minden nap más-más iskolai osztályokat fogad. Az élményközpontban a tanulók digitális eszközökkel találkozhatnak kiscsoportos foglalkozások keretében. A foglalkozások sokszínűek, alapvetően a digitális kompetenciákra alapulnak. Foglalkozások iskolaidőben zajlanak, egész nap ott maradnak a diákok és „tanórákon” vesznek részt forgószínpadszerűen. A tanórákon 3D tervezéssel és nyomtatással (ThinkerCad), mobil alkalmazásfejlesztéssel (AppInventor), tervezés 2D-ben lézervágással és gravírozással (CorelDraw), Lego robot programozás, gömbrobot programozás (Sphero Bolt), ipari oktatórobot programozása (Dobot Magician), humanoid robot bemutató és programozása (Pepper, Nao, UBTECH Alpha) illetve egy szabadulószoba is színesíti az oktatást. A témák számából látható, hogy az osztályok több alkalommal is részt vesznek ilyen napokon, így ismerkednek meg életkoruknak megfelelően a különböző területekkel. Jelenleg 5.,7. és 9. osztályos tanulók vesznek részt a foglalkozásokon. A foglalkozások mellett délután szakkörök, nyáron táborok színesítik a központ palettáját. Az élményközpont nagyon fontosnak tartja az esélyegyelőséget, a digitalizáció fontosságát. Éppen ezért az összes program ingyenes a városban tanulók számára.

A kutatás során több célt vezérelt bennünket, a legfontosabb, hogy szerettük volna minél közelebb hozni a tanulókhoz a humanoid robotot, robotokat. Elsőként 5. osztályban csak egy bemutatót látnak, ahol passzív szemlélői az órának, itt még ma sem ritka, amikor félelmet látunk a tekintettekben. Ez ösztönzött bennünket arra, hogy felsőbb évfolyamoknak olyan foglalkozást alakítsunk ki, ahol a résztvevők megfoghatják a robotot, kommunikálhassanak vele, vezérelhessék, programozhassák. Ez a sok ember-robot interakció segíti az esetleges félelmeik feloldását, biztonságérzetük növelését. Az élményközpont jellegéből fakadóan a foglalkozás témája a programozás oktatásban lett. Ez más oktatási környezetben kapcsolódhat egyéb tématerületekhez (nyelvoktatás, énekoktatás stb.).

ELŐZMÉNYEK NAO ÉS PEPPER PROGRAMOZÁSI LEHETŐSÉGEI

Már a digitális élményközpont nyitásakor cél volt, hogy a tanulónak minél szélesebb körben biztosítsunk lehetőséget az eszközök használatára, programozására. Így volt ez a humanoid robotok esetében is. Kezdetben egy-egy Nao, illetve Pepper robot állt rendelkezésre, jelenleg már két Nao, illetve három Pepper robot található az intézményben. A típusukat tekintve vegyes a kép, hiszen Nao-ból 5 és 6 verzió áll rendelkezésre, Pepper robot tekintetében két darab 2.5 verzió a harmadik pedig 2.8-as verzió található. Egyéb humanoid robotok (UBTECH Alpha 1E, Edbot) is vannak használatban a házban, amiket külön foglalkozásokon használnak a tanulók, de ezek programozása erősen limitált, így mindenképpen szerettük volna a fejlett humanoid robotokat is bevetni az oktatásban.

2. ábra Humanoid robotok az élményközpontban

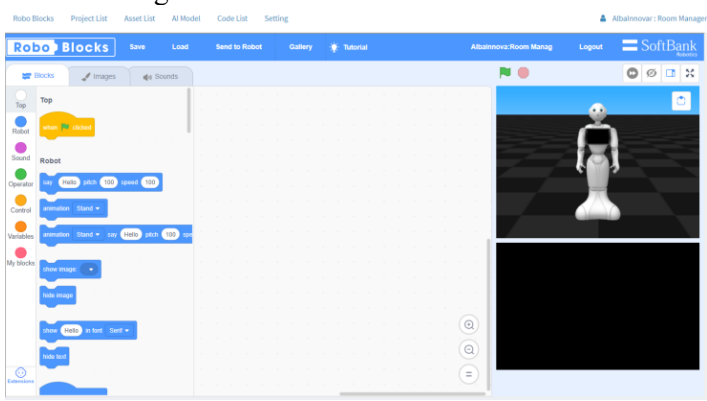
A gyártó által biztosított programozási lehetőség a Choregraphe fejlesztőeszköz, a robothoz illeszkedő verzióval. Első lépésben szakkörökben igyekeztünk tapasztalatot szerezni. Szerveztünk egy olyan szakkört, ahol általános iskolások, középiskolások és egyetemisták is részt vettek. A fejlesztőeszköz vizuális elemei mögött Python programozási elemek találhatók. Ezért az gondoltuk, hogy párhuzamosan elindítottunk egy olyan szakkört, ahol közvetlenül a Python használnák a robot programozására. Ezt 13-14 éveseknek tartottuk programozási elismeretek nélkül. Az első próbálkozásaink vegyes eredménnyel zárultak. A vegyes szakkör jobban sikerült, itt sikerült egy olyan tematikát felállítani, amit a későbbiekben használhatunk. A tanulók visszajelzései pozitívok voltak, az egyetlen nehézség az alkalmazások tesztelése volt. A robothoz egyszerre csak egy tanuló fér hozzá, így időigényes volt

a robotra csatlakozás-futtatás-leválasztás műveletsora. A Python-os csoport nagy csalódás volt. Sok idő elment az alapparancsok megismerésével, majd, amikor végre a robotközeli volt a programozás akkor össze-vissza vezérelték a robotok. Itt sajnos nincs védelem a futtatás szempontjából, azaz egyszerre akár többen is elküldhették a programjukat a robot felé, ami káoszt okozott. Ezután a Choregraphe mellett döntöttünk. Kidolgozásra került egy mindennapi tanulói foglalkozás, ahol 15-16 évesek csoportok betekintést nyertek Pepper programozásába. E mellett egyetemi kurzusokat indítottunk mint szabadon választható tantárgy.

Mindezek mellett lehetőség van a gyártó által biztosított interface-ek segítségével Java, JavaScript, C# nyelvek segítségével programozni a robotokat. Ezeket oktatási környezetben nem használtuk, szakdolgozatok, nagyobb projektek készítésekor lettek alkalmazva. Úgy véljük, hogy iskolai környezetben ezek használata a tehetséges tanulókra korlátozódik.

ROBO BLOCKS

Egy féléves időszak után összegeztük a tapasztalatokat. A tanulók nagyon szeretik a humanoid robot programozás foglalkozásokat, de gyakran belassul az óratartás a nehéz futtatás miatt. Így új lehetőséget kerestünk, ami online megoldás és párhuzamosan tudunk használni a tanulókkal. Olyan kerestünk, ami hasonló a „testvér robot" Nao esetén a NAO Cadlet alkalmazáscsomag. A lehetséges megoldások keresése közben találtuk a Robo Blocks megoldást, ami egy online használható és megfelelt a céljainknak [17]. Ezt a megoldást az ázsiai piacra fejlesztették ki, de az európai francia központ segítségével engedélyt kaptunk a tesztelésre, majd a használatra. A megoldás során egy alkalmazást telepítődik a robotra, ezt elindítva kell belépni abba a szobába, amit a tanulók is használnak az online felületen. Az online felületen lehetőség van új szobákat megadni, alkalmazásokat törölni, és egyéb adminisztrációs műveleteket elvégezni.



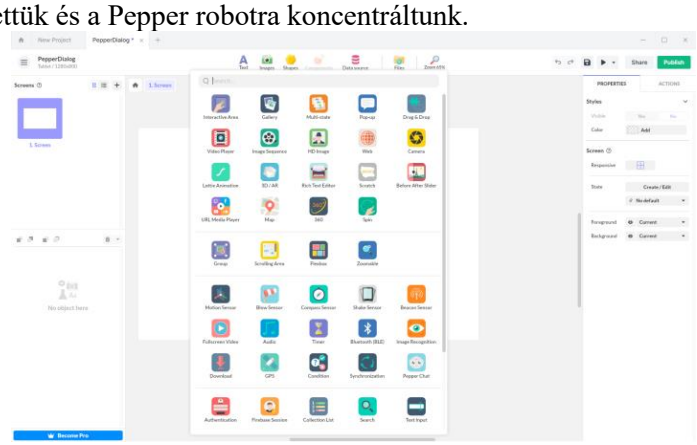
3. ábra -Robo Blocks felhasználói felülete

A tanulók laptopokat használva érik el az online felületet, ahol elsőként egy irányított feladat során megtanulják az alapvető parancsokat, amivel a robotot vezérelni lehet. Tapasztalatok alapján a MIT által kifejlesztett Blockly-s felület használata nem okoz gondot a tanulóknak. Az utóbbi években az iskolák széles körben használják ezt a megoldás egyéb feladatok során. Mivel vizuális programozás (Scratch) bekerült a digitális kultúra tantárgy központi tananyagába a tanulók előképzettsége egyre jobb lesz ezen a területen. Amikor az első alkalmazásuk elkészült diákoknak, akkor a programot tesztelhetik a beépített

robotemulátoron, ahol ki kell emelni a kiegészítő tablet emulátort, hiszen ilyen a „gyári” Choregraphe-ban sincs. Amikor a helyi tesztelés eredményes, akkor a diákok elküldik a robotra a programjukat. Ott viszont nem indul el egyből, csak a tablet felületről lehet elindítani. Ezzel a megoldással sokkal gördülékenyebbé vált az óratartás. Az óra második felében a résztvevők saját kis programot készítenek azok alapján amiket előzőleg tanultak. Itt persze nem kell extra dologra gondolni, de a célt, hogy bátran merjenek robotot vezérelni, alkalmazást készíteni, futtatni, biztonsággal odamenni és kezelni egy „nagy” humanoid robotot ezt elérjük. Természetesen nem lehet minden funkcióját kihasználni a Pepper robotnak. A Robo Blocks segítségével lehetséges a robot beszéltetésére, előre beállított animációk lejátszására, robot helyváltoztatására, tableten képek, szövegek megjelenítésére, beszédfelismerésre, arcfelismerésre és összetettebb dialógusok kialakítására. A legújabb fejlesztéseknek köszönhetően a robot összeköthető a ChatGPT-vel.

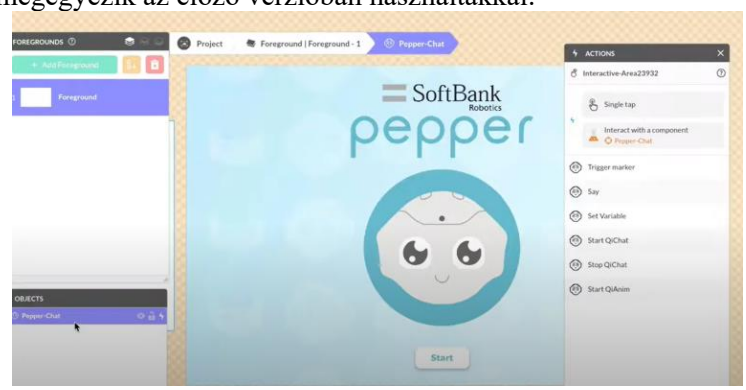
PANDASUITE

Időközben változtatott a gyártó cég, a Softbank a Pepper robot működési elvén. Véleményem szerint sok kritika érte a robotot a biztonsági hiányossági miatt, hiszen gyakorlatilag egy ip-cím és egy port ismeretében vezérelni lehet távolról a robotot[18]. Ez bizonyos körülmények között – lásd oktatás – kifejezetten hasznos, de ipari környezetben nem elfogadható. Így a hardware-t meghagyták, de a szoftveres részt újra tervezték. Ennek eredményeképpen csak a tableten keresztül lehet programozni a robotot Java vagy Kotlin nyelv segítségével. Ez az oktatásban csak szűk rétegnek megfelelő, az élményközpont célkitűzésének ez nem megfelelő, így másik megoldást kellett találnunk. Természetesen maradhatunk volna a régebbi működés mellett, de az újabb robot már magyarul is tud, amit szerettünk volna kihasználni. A gyártónak nehézségei támad, így a szoftveres támogatás erősen visszaesett, de sikerült egy külsős partnernek egy megoldását megtalálni, ez a PandaSuite. Ez az alkalmazás forráskód nélküli programozást ígér. Ingyenesen ki lehet próbálni és támogatja a web-es, asztali és mobil alkalmazásokat. Az élményközpontban az egyik foglalkozás keretében használjuk az MIT által fejlesztett AppInventor alkalmazást. Ezt széles körben, sokan használják oktatási célra. Nálunk is nagy sikere van a tanulók körében. Elsőként annak a lehetősége is felmerült, hogy ezt a foglalkozást átalakítsuk a PandaSuite használatával, de ezt végül elvetettük és a Pepper robotra koncentráltunk.



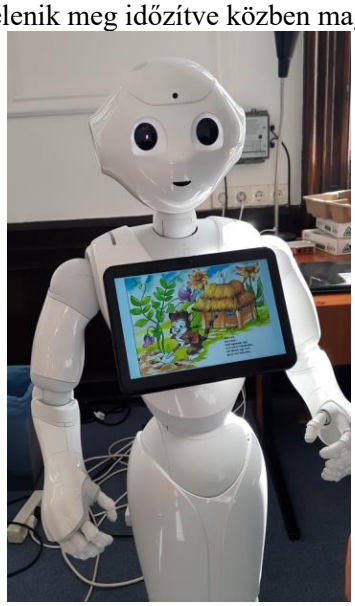
4. ábra – PandaSuite felhasználói felülete használható komponensekkel

Elsőként azt kellett kitalálni, hogy miként láthassák a tanulók a Pepper robot tabletjét. Ezt most meg lehetett oldani, mivel teljes értékű Android-os rendszer került a tabletre, igaz régi 6.0-as verzió. Ez azért volt örömteli, mert az előző verzióban csak egy butított Android áll rendelkezésre, ahol csak egy böngészőt lehet futtatni. Több megoldás is lehetséges mi az AnyDesk, hiszen más foglalkozás közben is bevált. Ezután fel kell telepíteni a futtató környezetet a tabletre, azaz hasonlóan szerveződik, mint a Robo Blocks esetén. A laptopokra letöltöttük a PandaSuite alkalmazást és így egy oktatásban használható rendszert kaptunk. Itt is korlátozott képességeket kapunk a robot programozása tekintetében iskolai foglalkozásokhoz megfelelő. A fejlesztőkörnyezettel tudunk a robottal társalogni, animációkat futtatni. A fejlesztés központi szereplője a top fájl, ami a dialógusok testre szabását teszi lehetővé. Ez megegyezik az előző verzióban használtakkal.



5. ábra - Pepper komponens lehetőségei

Kezdő lépésként a kollégákkal készítettünk mintaalkalmazásokat, így megismerve, tesztelve a rendszert. Első projektnek egy mesélős alkalmazást tűztünk ki célul, ez az Iciripiciri lett. Itt képek sorozata jelenik meg időzítve közben magyarul mesél a robot.



6. ábra - Pepper mesél

Az egyes diákhoz egy párbeszéd állomány dialóg állományt készítettünk. Ebben helyeztük el a meséhez szükséges szövegeket.

```
topic: ~iciri()
proposal: %dia1 Móricz Zsigmond Iciri-Piciri
proposal: %dia2 Hol volt hol nem... Volt egyszer egy iciri piciri házácska, ott lakott egy iciri piciri kis macska.
proposal: %dia3 Volt annak két iciri piciri kis ökre, rákaptak egy iciri piciri kis tökre.
proposal: %dia4 Csizmát húz az iciri piciri kis macska, hová kett az iciri piciri barmocska.
proposal: %dia5 Bejárja az iciri piciri kis erdőt, s nem leli az iciri piciri tekergőt.
proposal: %dia6 Bejárja az iciri piciri kaszálót, s nem látja az iciri piciri kószálót.
proposal: %dia7 Rátalál egy iciri piciri kis tökre, bánatában iciri picirit meglökte.
proposal: %dia8 Felfordult az iciri piciri tököcske, benne a két iciri piciri ökröcske. Megörült két iciri piciri ökrének
```

7. ábra - Párbeszéd állomány

Ezek után egy egyszerű tájékoztató robotszerű alkalmazást készítettünk, ahol az animációk is használtunk. A kezdeti tapasztalataink biztatók voltak. Tesztként a robotszakkörökön résztvevőkkel próbáltuk ki a foglalkozást. Előzetes várakozással ellentétben nem értük el az a sikert, amit reméltünk. Módosítottunk a foglalkozáson majd a nyári táborban újra teszteltük. Itt ügyesebb résztvevők voltak, akikkel jobban sikerültek a foglalkozások, de még mindig hiányérzetünk maradt. Nem éreztük, hogy a tanulóknak többet kapnának. A programozói felület önálló használata szokatlan, nehézkes a tanulók. Tapasztalatok alapján a magyar nyelv használata nem jelent akkora többletélményt, mint vártuk.

ÖSSZEGZÉS

Mindenképpen szeretnénk olyan foglalkozásokat tartani, ahol a részvevők testközelből használhatják a humanoid robotokat, ezzel is csökkentve ellenérzéseiket és növelve a biztonságérzetüket.

Az útkeresés során találtunk az intézményhez illeszkedő megoldásokat, illetve olyan utat és próbáltuk, ami nem váltotta be a reményeket. Mivel a közoktatásban fokozatos tért nyer a Python így abban reménykedtünk, hogy a humanoid robotok programozásnál ez hasznos lesz. Itt a korosztály választása nem volt szerencsés, a kisebb korosztály még nem rendelkezett kellő ismeretekkel Pythonból, így időhiány keletkezett. Az idősebbek motiváltsága pedig alacsony még a humanoid robotok programozása tekintetében is. A Choregraphe megfelelő eszköznek bizonyult, itt csak az óraszervezés volt nehézkes. Különösen a kevésbé motivált látogatók esetén volt sikertelenség. A legjobb megoldásnak a RoboBlocks bizonyult, folyamatosan fejlesztik, közel áll a diákokhoz, gyorsan használják, kreatív módon használják. Egyelőre nem találtuk meg a módját, hogy a magyarul is beszélő humanoid robotot beépítsük a napi foglakozásokba. Sajnos a gyártó nem fejleszt újabb megoldásokat a járvány óta, így a PandaSuite mellett más megoldást nem tudtunk kipróbálni, így ezt kell tovább tesztelni, tanulmányozni, hogy megfelelő módon tudjuk tálalni a tanulóknak.

FELHASZNÁLT IRODALOM

[1] F. M. Sánchez Martín *és mtsai.*, „History of robotics: From archytas of tarentum until da Vinci robot (part I)”, *Actas Urol. Esp.*, köt. 31, sz. 2, o. 69–76, 2007, doi: 10.1016/S0210-4806(07)73602-1.

[2] F. M. Sánchez-Martín *és mtsai.*, „History of robotics: From Archytas of Tarentum until Da Vinci robot (Part II)”, *Actas Urol. Esp.*, köt. 31, sz. 3, o. 185–196, 2007, doi: 10.1016/S0210-4806(07)73624-0.

[3] M. Barna, „Hogyan született a szegedi robotember?”, *Ezermester*, o. 158-159., 0 1962.

[4] R. M. Tamim, R. M. Bernard, E. Borokhovski, P. C. Abrami, és R. F. Schmid, „What Forty Years of Research Says About the Impact of Technology on Learning: A Second-Order Meta-Analysis and Validation Study”, *Educ. Res. Rev.*, köt. 10, sz. 1, o. 50–64, 2011.
[5] D. Ifenthaler és V. Schweinbenz, „The acceptance of tablet-PCs in classroom instruction: The teachers’ perspectives”, *Comput. Educ.*, köt. 75, o. 113–123, jún. 2014.
[6] S. Higgins, G. Beauchamp, és D. Miller, „Reviewing the literature on interactive whiteboards”, *Learn. Media Technol.*, köt. 32, sz. 3, o. 213–225, 2007.
[7] M. Alemi, A. Meghdari, és M. Ghazisaedy, „Social Robots as Language Learning Tools”, *Int. J. Soc. Robot.*, köt. 6, o. 357–366, 2014.
[8] O. Mubin, C. J. Stevens, S. Shahid, A. Al Mahmud, és J.-J. Dong, „Social Robots in Education: A Review”, *Comput. Educ.*, köt. 70, o. 128–142, 2014.
[9] J.-J. Cabibihan, H. Javed, M. Ang Jr, és S. N. Aljunied, „Why Robots? A Survey on the Roles and Benefits of Social Robots in the Therapy of Children with Autism”, *IEEE Trans. Learn. Technol.*, köt. 7, sz. 4, o. 283–295, 2013.
[10] Gy. Györök és B. Beszédes, „Artificial Education Process Environment for Embedded Systems”, *AIS2014*, o. 37–42, 2014.
[11] E. Szűcs és L. Záhonyi, „Információbiztonság fejlődéstöténeti vizsgálata mérföldkövekkel, események és válaszok”, *Biztonságtudományi Szle.*, o. 81–90, 2021.
[12] T. Nomura, T. Kanda, T. Suzuki, és K. Kato, „Measurement of anxiety toward robots and development of the multi-dimensional robot attitude scale”, *Comput. Hum. Behav.*, köt. 24, sz. 2, o. 237–246, 2008.
[13] K. F. MacDorman és S. O. Entezari, „Robophobia: Roots of the fear of robots”, *J. Soc. Robot.*, köt. 7, o. 107–119, 2015.
[14] C. B. Frey és M. A. Osborne, „The future of employment: How susceptible are jobs to computerization?”, *Technol. Forecast. Soc. Change*, köt. 114, o. 254–280, 2017.
[15] T. Shibata és K. Wada, „Robot therapy: A new approach for mental healthcare of the elderly - A mini-review”, *J. Healthc. Eng.*, köt. 2, sz. 4, o. 497–505, 2011.
[16] C. Breazeal, „Emotion and sociable humanoid robots”, *Int. J. Hum.-Comput. Stud.*, köt. 59, sz. 1–2, o. 119–155, 2003.
[17] Y.-R. Zhang, G. Yang, J.-Y. Xu, és J.-H. Chen, „A Task-Driven Instructional Design and Application Study for Pepper Robot”, *IEEE Int. Conf. Educ. Technol.*, o. 264–267, 2021.
[18] A. Giaretta, M. De Donno, és N. Dragoni, „Adding Salt to Pepper A Structured Security Assessment over a Humanoid Robot”, *Proc. 13th Int. Conf. Availab. Reliab. Secur.*, 2018.
[19] Cs. Kollár és L. Ványa, „Szerethetők-e a robotok?: Az ember-robot interakció humán oldalának empirikus aspektusa”, *Hadtud. Magy. Hadtudományi Társ. Folyóirata*, köt. 27, sz. 1–2, o. 163–177, 2017.
[20] Cs. Kollár, „Szerethetők-e a robotok: Az ember-robot interakció humán oldalának teoretikus aspektusa”, *Hadtud. Magy. Hadtudományi Társ. Folyóirata*, köt. 26, sz. különszám, o. 142–154, 2016.

ARTIFICIAL INTELLIGENCE THROUGH ASIMOV'S EYES OR THE WORK OF A LIFETIME

A MESTERSÉGES INTELLIGENCIA ASIMOV SZEMÉVEL AVAGY EGY ÉLET MUNKÁJA

SZABÓ Lajos[1]

Abstract

Since 1956, countless devices and their programs have been declared to be artificial intelligence. The word „robot" has undergone a similar change of meaning since 1922. For 46 years, a science fiction writer wrote his romans and novels about the relationship between artificial intelligence and humans, at the end they was integrated into a coherent set of ideas at the end of his life. Today's scientists and developers are not concerned with the ethical aspects of AI, which Asimov's writings provide the main guidelines. In the 21st century, software is undergoing an amazing evolution, but the regulation of software is in its infancy, both ethically and legally.

Keywords

Asimov, AI, robots, ethical aspets of AI, ethical and legal regulation

Absztrakt

1956 óta számtalan eszközt és programjukat nyilvánították mesterséges intelligenciának. A "robot" szó is hasonló jelentésváltozáson ment keresztül 1922 óta. A sci-fi író 46 éven át írta novelláit és regényeit a mesterséges intelligencia és az ember kapcsolatáról, végül élete végén ezek egy összefüggő gondolathalmazba integrálódtak. A mai tudósok és fejlesztők nem foglalkoznak a mesterséges intelligencia etikai vonatkozásaival, amelyekhez Asimov írásai adják a fő iránymutatást. A XXI. században a szoftverek elképesztő fejlődésen mennek keresztül, a velük kapcsolatos szabályozás azonban gyermekcipőben jár, etikai és jogi értelemben is.

Kulcsszavak

Asimov, MI, robotok, az MI etikai vonatkozásai, etikai és jogi szabályozás

[1] szabo.lajos@uni-obuda.hu | ORCID: 0000-0001-9375-2188 | Lecturer Óbuda University / Institut of Safety Science and Cybersecurity | Chairman of the Board of Trustees, Foundation for Law Enforcement and Private Security Education and Research (REMOK)| kuratóriumi elnök, Alapítvány a Rendvédelmi és Magánbiztonsági Oktatásért és Kutatásért (REMOK)

A MESTERSÉGES INTELLIGENCIA ÉS A ROBOT KIFEJEZÉSEK EREDETE

Mielőtt Asimov életművének elemzésébe kezdek, szeretnék tisztázni néhány fontos kérdést. Meggyőződésem szerint fontos, hogy mindig pontosan tudjuk miről is beszélünk, ha egyes kifejezéseket használunk.

Mióta foglalkozunk a mesterséges intelligenciának nevezett dolgokkal?

„Sok kezdeti eredményt lehetne MI-nek nevezni, azonban egy teljes elképzelést az MI-ről 1950-ben Alan Turing fogalmazott meg a Computing Machinery and Intelligence c. cikkében. Itt vezette be a Turing-teszt, a gépi tanulás, a genetikus algoritmusok és a megerősítéses tanulás fogalmakat."[1]

A második világháború után számos kutató kezdte el az öntanuló, döntési képességgel rendelkező programok kutatását, fejlesztését. Sokáig, sok néven nevezték ezeket mígnem 1956 nyarán, két hónapos munkatalálkozót nem szerveztek a témával foglalkozó tudósok. A soknevű témakör soknevű is maradt, amíg a Stanford Egyetem későbbi professzora John McCarthy a Dartmouth-i munkatalálkozón el nem nevezte, úgyhogy máig ezt a kifejezést használjuk.

Ahogy erről a Mesterséges Intelligencia Elektronikus Almanachban olvashatjuk:

„A munkatalálkozó talán legtartósabb eredménye az volt, hogy elfogadták a terület McCarthy által kreált új nevét, azaz a ***mesterséges intelligenciá****t (****artificial intelligence****)."*[2]

Ahogy ez előtt sokféleképpen nevezték az egyébként más-más problémakörökre tervezett eszközöket és a bennük működő programokat, azóta is annyiféle értelmezését találjuk a fejlesztők, kutatók, szakírók által alkalmazott mesterséges intelligencia fogalmaknak, leírásoknak.

Kiemelkedően fontos leszögezni, hogy a médiában elterjedt mesterséges intelligenciával kapcsolatos kifejezések, mint például „ A mesterséges intelligencia már ezt is tudja." A mesterséges intelligencia képes rá." és hasonlók hibás képet alakítanak ki az olvasóban. Azt sugallják, mintha a mesterséges intelligencia egységes valami lenne, egy dologról beszélünk, ha róla beszélünk. Ennek a sugallatnak a következménye az, hogy a témában járatlan személyek is ebben a kontextusban használják. Pedig ez az értelmezés káros, megtévesztő és teljes mértékben tudománytalan, alaptalan.

Igen McCarthy óta van egy általános elnevezés, de az egymástól teljességgel elkülönült programokra és az azokkal irányított eszközökre vonatkozik. Teljesen mindegy, hogy egy szövegfeldolgozó- és vagy készítő programról beszélünk, amely szóban vagy írásban kommunikál velünk, vagy egy arcfelismerő szoftver dolgozik valamilyen hardverben, vagy egy sakkautomatával játszunk, az mind mesterséges intelligencia. Ugyancsak az a szóbeli vagy írásbeli kérésre képet, vagy mozgóképet generáló szoftver, vagy egy összetett rakétaelhárító rendszer, négylábú állatok, vagy emberek különféle mozgásait elsajátító gépezeteket is egy részben öntanuló szoftver vezérli, és ezek mind mesterséges intelligenciák.

Azonban nyilvánvalóan semmi közük egymáshoz!

Amit az egyik tud, azt nem tudja a másik, még akkor sem, ha nyilvánvalóan vannak közös moduljaik is. A közös modulokban nem azonos szoftverek működnek, hiszen célra orientáltan hozták létre azokat más és más szakemberek a világ több kutató vagy fejlesztő laboratóriumaiban. Elegendő csak az információbevitelre gondolni. Nem mindegy, hogy mit és milyen spektrumban érzékel a beviteli modul és ezeket az érzékleteket milyen szoftver alakítja át észleletté. Hiszen ha az embert modellezzük, sokkal kisebb spektrumban érzékeli a

fényt, mint néhány állat, da ugyanígy vagyunk a hanggal a hővel és még sorolhatnánk. Ahogy a bolygónkon élő szervezetek mást és mást érzékelnek és azokra eltérően reagálnak, ugyanígy a sok-sok mesterséges intelligencia-változat is mást és mást érzékel és a programjának megfelelően reagál.

Azért nincs csak úgy általában mesterséges intelligencia és azért nem szabadna így beszélni róla, mert ahogy a különféle élő szervezetek más és más célra, más és más „szoftverrel" mint például a DNS, más és más bemeneti és kimeneti, információfeldolgozó, valamint végrehajtó eszközrendszerrel rendelkeznek, úgy minden mesterséges intelligencia programot használó rendszer is eltérő célokra készült.

E kutatások és fejlesztések mellett folyamatosan ment az automatizáció az iparban, ahol a monoton és nagy pontosságot kiváltó munkafeladatoknál az ember kiváltása volt a cél. Ez a folyamat napjainkban sem állt le, egyre jobb és jobb robotokkal rendelkezik az ipar és mára már az orvostudomány is. A XXI. században már számos otthoni automata berendezés végez munkát otthonainkban, és a számítógépeken, és egyéb eszközökön számos automata végzi el helyettünk a napi robotot, dolgozik helyettünk.

Ezzel meg is érkeztünk a következő problémához. Minden olyan automatát, mely valamilyen emberi munkát helyettesítő munkafolyamatot végez el, egy ideje robot-nak nevezzük, pedig nem annak kellene, inkább automatának.

A robotok alapvetően nem olyanok kellenének legyenek, mint azt manapság az ipari robotoknál és mindenütt másutt látjuk.

A robotok eredetileg ember formájú androidok voltak! Azokat és csak azokat nevezték robotnak, amelyek ember formájúak, autonóm mozgásra, kommunikációra képes, érzékelni és az érzékleteket észleletté alakítani, vagyis információt létrehozni, és annak megfelelően adekvát cselekvésre képes homeosztátok voltak, melyek ráadásul öntanuló programmal is rendelkeztek.

Ugyanis a szó megalkotója, Karel Čapek, „Rossumovi univerzální roboti" című színdarabjában egy olyan gépet ír le, ami ember formájú, és gondolkodni képes.

„*A robot – a középkori jobbágyszolgáltatások közé tartozván – Magyarországon már korábban is ismert szó volt. Bár a szláv nyelvekben – így az oroszban – van általános jellegű „munka" értelmezése is a robotának, kényszermunka jelentésben is ismert. … Bár Karel Capek használta tényleg először a szót, nem ő találta ki. Egy angol nyelvű cseh weboldal közli Capek visszaemlékezését minderre. A rövid történetből kiderül, hogy először „Labori"-nak akarta hívni a szerkezeteket, de a fivére javasolta neki a robot szót az ember alakú gépek megnevezésére.*"[3]

Ennek a színdarabnak az 1922-es New-York-i bemutatója után kezdték el robotnak nevezni az ember formájú intelligens szerkezeteket, majd később mindenféle más gépi szerkezetre is alkalmazni kezdték, így jutottunk el a jelenkori értelmezéshez, amiről nyilván kevesen tudták eddig, hogy a szláv nyelvek munka-értelmű szavából ered.

Mivel a nyelv egy „élő" fejlődő kommunikációs rendszer, a benne használt szavak, kifejezések folyamatosan tartalmi, értelmezési szempontból átalakulni képesek. Az eredetileg a munkát jelentő szó, már a korai középkorban jelentett kényszermunkát, olyan munkavégzést, amelynek hasznából a munkát végző személy nem részesül. A földesúr számára végzett munka, amit a jobbágyai ellentételezés nélkül végeztek. Ez a kvázi rabszolgai tevékenység szintén a robot szóval gyökerezett meg több nyelvben, így magyarul is.

A Capek-i értelmezésű robot, pedig nyilvánvalóan olyan rabszolga-automata, amelyik nem részesül gazdája érdekében végzett munkáért ellentételezésben.

A címben szereplő Isaac Asimov például tudta, hiszen le is írta az Alapítvány pereme című könyv 2. kötete, első fejezetében, ahol Quintesetz professzor beszélget Pelorat profeszorral, és magyaráz neki a robotokról:

„*Quintesetz összecsücsörítette az ajkát, hátradőlt székében (mely enyhén megereszkedett a súlya alatt), és ujjhegyeit egymáshoz illesztette. Láthatóan gondot okozott neki, hogy hol is kezdje.*
– Tudják, mi az a robot? – szólalt meg végül.
– Robot? – kérdezte vissza Pelorat. – Nem. Quintesetz Trevize-ra pillantott, aki lassan megrázta a fejét.
– És azt tudják-e, mi az a számítógép?
– Természetesen – felelte Trevize türelmetlenül.
– Nos, mozgó, számítógépes szerszám...
– Az, mozgó, számítógépes szerszám – fejezte be Trevize kissé ingerülten.
– Számtalan változata ismeretes, és nem tudok semmiféle általános érvényű kifejezést azon kívül, hogy mozgó, számítógépes szerszám.
– ... mely pontosan olyan, mint egy emberi lény: ez a robot – fejezte be S. Q. nyugodtan a definíciót. – A robot abban különbözik a többitől, hogy ember formájú.
– Miért ember formájú? – kérdezte Pelorat őszinte elképedéssel.
– Ezt magam sem tudom. Szerszámnak határozottan alkalmatlan forma, ebben egyetértünk, én azonban csak a legendát ismételem. A "robot" régi szó, nem ered semmiféle felismerhető nyelvből, noha tudósaink szerint valami módon összefüggésben áll a ,,munká"-val.
– Egyetlen olyan szóról sem tudok – jegyezte meg Trevize kételkedve –, amely akár távolról is emlékeztetne a "robot"-ra, ugyanakkor bármiféle köze lehetne a "munká"-hoz.
– Bizonyára nem szerepel a galaktikus köznyelvben – hagyta rá Quintesetz–, mégis ezt állítják.
*– Talán valami fordított etimológiáról lehet szó – vélte Pelorat. – Ezeket a tárgyaka*t használhatták munkavégzésre, s a szó lassanként átvette a "munka" jelentést..."[4]

Mint orosz születésű, Iszaak Judovics Ozimov, cirill betűkkel *Исаак Юдович Озимов,* aki 1920-ban született a Szovjetunióban az orosz föderáció Szmolenszk megyéjében található Petrovicsi faluban, nyilván beszélt valamennyire oroszul. Nyilvánvalóan a Čapek-i és a történelem során kialakult értelmezést is ismerte, hiszen a magyarázat tökéletesen erre mutat.

A MESTERSÉGES INTELLIGENCIA ASIMOV KOHERENS REGÉNYFOLYAMÁBAN

Asimovot, mint híres írót, a legtöbben szépíróként vagy tudományos-fantasztikus íróként és nem tudósként ismerik, vagyis elsődleges információ a nevéhez ez. Holott ismeretterjesztő tudományos műveinek száma is nagyon jelentős, valószínűleg meghaladja tudományos fantasztikus műveinek a számát. Biokémikusként docensi fokozatot ért el, és

éveken keresztül tanított, tanszéket vezetett, mígnem úgy döntött, hogy szélesebb körben írásain keresztül folytatja a tanítást.

Saját magát olyan tudósként jellemezte, aki akkor is tudományos ismeretterjesztést folytat, amikor sci-fi műveket ír. Semmiképpen nem méltó arra, hogy bárki is legyintsen a műveiben leírtakra, vagy lekicsinyelje teljesítményét. Egy olyan szerző, aki tudományos fokozattal és tanári „előélettel" több mint 500 könyvet jegyez, és ezek jelentős része tudományos ismeretterjesztő munka, nem „csak egy sci-fi író". Munkáit érdemes elolvasni és tudományos műveknél felhasználni. A jelen tanulmánynak nem célja irodalmi vagy részletes szövegszerű elemzéseket végezni, mindössze a legfontosabb mondanivaló kiemelése és ritkán, idézetekkel való igazolása fordul elő.

A jelen tanulmány Asimov azon írásait tekinti egy egységes gondolatfolyam részeinek, amit számos a témával foglalkozó irodalmár, kritikus és persze az írásait, mint a tanulmány szerzője is jól ismerő olvasója annak tekint. A novellák, kisregények és regények megjelenése nem időrendi, hiszen az Én a Robot-ban szereplő novellákat már az Alapítvány trilógia követte, majd az Űrvadász-sorozat, az Elijah Bayley-történetek, a Kavics az égen és a Csillagok akár a por, csak lazán kapcsolódik, de kapcsolódik, az Alapítvány előtt az Alapítvány pereme és az Alapítvány és a Föld már ezek után évtizedekkel, a kiadó felkérésére készült el. Asimov írói zsenialitása, hogy ha belekezdünk elejétől a végéig ebbe a hatalmas olvasnivalóba, egy egységes gondolatfolyam rabjai leszünk az elsőtől az utolsó mondatig.

Hát lássuk, miről is írt a világhírű író és tudós a mesterséges intelligenciával kapcsolatban.

Első írásaiban, melyben a „pozitronagy" kifejezést megalkotva, gondolkodó, éntudattal rendelkező, tanulni és dönteni képes automatákról ír Lehet, hogy a mai kiterjesztő robot értelmezést is neki köszönhetjük, hiszen már akkor is a robot kifejezést használja, amikor járművekbe képzel pozitronagyat, így azokat gondolkodó, érzelmekkel és értelemmel rendelkező gépekké változtatja.

Asimovot 46 éven keresztül annyira foglalkoztatta a probléma, hogy csak az ember rendelkezik-e tudattal és önálló döntésre való alkalmassággal, hogy az első tudományos-fantasztikus írásaitól kezdve, majdnem az utoljára megjelent regényéig, fő mondanivalójául választotta. Minden bizonnyal örömmel csatlakozott volna a Cambridge-i Nyilatkozat aláíróihoz, ha megérhette volna.

Mi is az a Cambridge-i nyilatkozat? Csányi Vilmos: Etológia, ember, társadalom. című munkájában a következő módon magyarázza el röviden: „***Mindössze öt éve született meg az egyetértés a tudósok között arról, hogy az ember és az állat idegrendszere alapvetően egyezik****, legfeljebb méretbeli és fajra jellemző különbségek léteznek. Vagyis a cambridge-i deklaráció kimondta:* ***az állatoknak is van tudatuk****, így minden állat gondolkodik, legfeljebb e gondolatok szerényebbek és más típusúak, mint az emberéi"*[5]

Ahogy a Cambridge-i nyilatkozat a tudatosságról, amit 2012. július 7-én adtak ki[6], a nem emberi élőlények – nem-emberi állatok kifejezést meggyőződésem szerint fordíthatjuk élőlényként - tudatállapotával kapcsolatban kijelenti azt, hogy;

„*A neokortex hiánya nem zárja ki, hogy a nem-emberi élőlények érzelmi állapotokat éljenek meg. Egybehangzó bizonyítékok arra utalnak, hogy a nem emberi élőlényeknél is megvannak neuroanatómiai, neurokémiai és neurofiziológiai alapjai a tudatos állapotnak, a szándékos viselkedés képességével együtt. Következésképpen a bizonyítékok súlya arra*

utal, hogy az ember nem egyedülálló a tudatosságot létrehozó neurológiai alapok birtoklásában. A nem emberi élőlények, beleértve az összes emlőst és madarat, és sok más élőlény, köztük a polipok is, szintén rendelkeznek ezekkel a neurológiai alapokkal"

Ehhez szeretném hozzátenni, hogy a tisztogatóhal (Labroides dimidiatus) úgy tűnik rendelkezik éntudattal, vagy valami csökevényével, mert felismeri magát a tükörben![7] Úgy tűnik tehát, a Camridge-i nyilatkozat a tudomány által szolgáltatott újabb felfedezések következtében akár már ennyi év eltelte után is kiegészíthető lenne.

Amennyire csak lehetett igyekeztem magyarítani a nyilatkozat végén található szöveget, a Neokortex kifejezést érintetlenül hagytam, csakúgy, mint a magyarul ideg- előtaggal általában fordított, neuro-előtagú szakkifejezéseket, mivel azok magyarításra eddig még a szakmai nyelvben sem teljesen elfogadott.

Hihetetlenül érdekesen kapcsolódik ehhez a XXI. századi nyilatkozathoz a XX. század talán legtermékenyebb írója Isaac Asimov, aki szinte teljes alkotói időszakában, (majdnem 50 éven keresztül!) vissza-vissza tért a tudattal kapcsolatos kérdésekhez. Élete végéig foglalkoztatta a mesterséges intelligencia, ezen belül a robotok fejlődésének elvi lehetősége, de a nem emberi és nem az ember által létrehozott mesterséges intelligencia is, mint arról később szólok.

Az először 1964.-ben egy kötetben megjelent Én a robot[8] (I, ROBOT New York 1964.) majd később egy Robottörténetek[9] címen magyarul megjelent 1940-1976 között készített összes írása, ami a robotokkal kapcsolatos novellákat tartalmazza és egységes gondolatfolyam, pedig egyes elemei között hatalmas idő telt el.

Ezeknek a novelláknak a mondanivalója egy mesterséges értelem, a pozitronagyú, önálló éntudattal és gondolkodási, tanulási képességgel rendelkező, az embert kiszolgáló robotokról szól. Első ránézésre az ember formájú robotokról és más robotokról -járművek stb. - ír történeteket, melyek pozitronaggyal, éntudattal és tanulási értelmi képességekkel rendelkeznek, a történetek a gazdáik és a közöttük folyó interakciókat érintik. Izgalmas és szórakoztató írások de a téma ismerőinek feltűnik, hogy mind a tudat, az emberi és mesterséges tudat/intelligencia problémája körül forog. A másik fontos téma az intuíció, de az nem tartozik a jelen témához, így mellőzöm.

Az általa leírt „Robotika három törvénye" nem csak logikai és döntési, hanem etikai és lélektani problémákat is felvet, melyek több évtizedes végig gondolása és leírása során, filozófiai mélységekig jutnak könyveiben mind az emberek, mind a robotok.

Az Űrvadász sorozatban a nem emberi intelligencia és az emberi intelligencia találkozásának problematikáját feszegeti. Az általa elképzelt, különböző szinten értelmes létformák, melyek benépesítik galaxisunk égitesteit más-más kommunikációs csatornákat használva teremtenek kapcsolatot az emberekkel. Izgalmas gondolatkísérletek, filozófiai, erkölcsi problémafelvetésekkel.

A Hajnal bolygó robotjai[10] című regényénben megismert Giskard aki a Robotok és a Birodalom című[11] regény végén R. Daneel Olivaw-val folytatott beszélgetést a három törvény kiterjesztéséről, a negyedik törvény bevezetéséről, szintén egy komoly etikai-filozófiai vita!

A robotpszichológia, mint kifejezés, megjelenik a legkorábbi novellagyűjteményben, az Én a robot-ban is, és a megalkotott kategóriától nem tágít későbbi írásaiban sem. A novellagyűjtemény külön fejezete az, amelynek a főszereplője, a robotokat gyártó monopólium, az Amerikai Robot neves robotpszichológusa, doktor Susan Calvin. A többi

főszereplő pedig természetesen mind robot, akik megjelenítenek olyan anomáliákat, melyek ma is jelen vannak, vagy bármikor megjelenhetnek a már létező alkalmazásokban.

Ezekben a novellákban majdnem mindent leírt, ami miatt ma félünk a mesterséges intelligenciától.

A szerző az egyszerű automaták világát jobbára elkerülve, a távoli jövőben feltalált „pozitronagy" segítségével, értelmes és egyre értelmesebb, szóban is kommunikáló robotokra alapozza az írásait. Egyértelműen a Capek-i robotok jelennek meg a történetekben. Nem tudhatjuk, hiszen külön nem írta le, de nyilvánvaló a problémakör ami ezek megírására késztette. Ez a mesterséges intelligencia és az emberi intelligencia, a gépi és emberi értelem, a gépi és emberi tudat volt az ami foglalkoztatta, abból a feltételezésből kiindulva, hogy egyszer megjelennek az ilyen képeségekkel rendelkező robotok.

Az egyik novella, amit 1976-ban írt az Amerikai Egyesült Államok két évszázados fennállására, felkérésre, „A két évszázados ember" (angolul The Bicentennial Man)[12], kiemelkedő fontosságú. Eleinte arról szól, hogy egy ember formájú robot egy véletlen folytán művészi képességekkel rendelkezik és ezt a képességét gazdái örömmel veszik, támogatják művészi tevékenységét.

Megjegyzem a véletlen „programhiba" kétszer is előfordul ebben a novellasorozatban, mindkét esetben művészi képességek kialakulására tesz szert a robot. Ha ehhez hozzáteszem, hogy a különféle művészeti ágakban tevékenykedők képességei, az, hogy képesek érzelmeket, összetett gondolatokat, vagy akár egész történeteket színekben, vonalakban, foltokban, hangokban, táncban stb. megjeleníteni, az embereknél sem átlagos képesség. Van egy mondás, miszerint a zsenit és az őrültet nagyon kevés választja el egymástól, a zsenihez nyugodtan a művészeket is hozzátehetjük. A két véglet ugyanis nyilvánvalóan olyan agyi, folyamatokban való különlegesség, mely az átlagtól eltér, a különféle „tehetségek" szintén az általánostól eltérőek, és mivel az agyunkban futó gondolkodási folyamatok következményei, tekinthetőek programhibának is.

E képességét felhasználva a robot műtárgyakat készít, melyek keresetté válnak a gyűjtők körében és a robotot valamint gazdáit híressé teszik. A művészeti alkotásokból származó bevételét első gazdája nem hajlandó átvenni, a pénzzel saját maga rendelkezik. A robotot első gazdája halálát követően, utódai összes nemzedéke hagyományosan családtagként és önálló entitásként kezeli, és ősükre emlékezve, a hagyományt megtartva önálló jövedelemmel rendelkezik. Egész hosszú, 200 éves életében folyamatosan tanul, és miközben annak a családnak az utódait szolgálja a család kihalásáig, melynek először a tulajdona lett. Végül tudományos kutatásokat végez, az emberi agy és a pozitronagy közti különbségeket és hasonlóságokat vizsgálja.

Először ruhákat kezd hordani, majd fémtestét az emberre megtévesztésig hasonlító mesterséges „emberi" kialakítású testrészekre cseréli. Ezek olyanok, amiket az emberek használnak protézisként és mesterséges szervekként. Miután minden testrészét ilyen félig bionikus testrészekre cseréltette ki, a pozitronagy kivételével, már csak egy vágya van. Bebizonyítani, hogy ezek után nincs különbség közte és az emberek között. Végül a robottörténetek főszereplője elismerteti magát embernek és ezt követően mint ember hal meg.

Az érzelmeket is megmozgató, lapos és jól felépített írás először mondja ki, annak a lehetőségét, hogy egyszer, valamikor, talán létrejöhet egy olyan összetett szoftver és a vele egybeépített hardver, mely szinte semmiben sem különbözik az emberektől. Igaz,

egyszeri és különleges kivétel még a regényben is, hogy ez a robot megkapja annak elismerését, hogy ember, és ezt is szinte a halála pillanatában.

Asimov a 46 éven keresztül írt és fokozatosan egységessé váló novella és regényfolyamban mindössze kétszer használja a mesterséges intelligencia kifejezést! A kifejezés, először a „Hajnal bolygó robotjai"[13] című könyve magyar kiadásának 58. oldalán a 3. bekezdés utolsó mondatában jelenik meg. Szövegszerűen:

„ *Baley igyekezett ráérezni a lényegre – a tendenciák, az általánosságok érdekelték –, és arra a megállapításra jutott, hogy az ember-robot kapcsolatban tapasztalható változások mind-mind a kölcsönös függőségi viszony kialakulása és megerősödése felé mutatnak. A robotok jogairól kötött megállapodás is ezt jelezte: fokozatosan megszűnik az, amit Daneel „felesleges megkülönböztetésnek" nevezett. Baley úgy vélte, hogy az auroraiak nem humanitárius meggondolásból viselkednek emberségesebben, hanem azért akarnak megfeledkezni a robotok gépi mivoltáról, hogy ne zavarja őket a tudat: egyre inkább rá vannak utalva a mesterséges intelligenciára*."

A másik alkalom a regényfolyamban az „Az alapítvány előtt"[14] című regény 338. oldalán található, szövegszerűen:

„ - *Úgy látom, általános a számítógépesítés - jegyezte meg Dors. - Szerintem akár rá lehetne bízni az egész irányítást a komputerekre. Az efféle környezetben a legideálisabb a mesterséges intelligencia alkalmazása.*"

Ez a két könyv eredetileg 1986-ban és 1988-ban jelent meg, sokkal később, mint a „mesterséges intelligencia kifejezés" amit, mint fentebb idéztem, 1956-ban a Drathmouthi munkatalálkozón alkottak meg és fogadtak el. Kifejezetten izgalmas, hogy bár biztosan ismerte, de megjelenésétől kezdve 30 éven keresztül kerülte a szerző a kifejezés használatát, miközben nagyon sokat foglalkozott a témával.

Az Alapítvány Pereme[15] című könyvében, az általa elképzelt tudatos bolygó Gaia kapcsán, úgy írja le, hogy a bolygó minden élő és élettelen része valamilyen szintű tudatossággal rendelkezik a bolygómagtól a sztratoszféra utolsó bolygóhoz tartozó gázmolekuláiáig. A bolygó minden része tudja, ismeri a helyét, a szerepét annak létezésében. Ezek a különféle szintű tudatformák érzékelik egymást és képesek az együttműködésre és a közös cselekvésre.

A témát a sorozat befejező kötetében is tovább gondolja, és az összes eddig leírt könyvét, novelláját e témában foglalja keretbe. Az Alapítvány és a Föld[16] végén egy olyan galaxist képzel el, mely egyéni tudatok közösségéből állva, közös tudatot alkot, Gaia mintájára a Galaxia a békés fejlődés és fennmaradás záloga.

Asimov majd fél évszázados munkája tehát messze túlmutat a jelen és közeljövő problémáin, és még sokkal jobban azokon, melyek megírásukkor voltak az akkori jelen és az akkori közeljövő problémái.

Pontosan látta az automaták és emberek együttélésének veszélyeit, az azokból adódó konfliktushelyzeteket, azoknak az emberi lélekre, tudatra való hatásait. Nem látta előre a szoftverek és a számítógépek közkézen forgását, a személyi számítógépek és tenyérben hordható változataik, melyeket első funkciójuk alapján máig telefonnak hívunk, holott már régen nem az a fő funkciója a legtöbbünk számára.

Azt azonban tökéletesen érzékelte, hogy eljön az a pont, ahol a gépek döntéseket hoznak majd az emberek helyett. Alapvetően nem a prediktív szövegbevitelre, vagy a helyesírás-ellenőrző, vagy a diktálás után szöveget lejegyezni képes programra gondolt – bár

ugye aki olvasta az Alapítvány trilógiát, tudja, hogy Arcadia Darell rendelkezik egy ilyen képességű leírószerkezettel – hanem az ennél sokkal mélyebben az ember helyett tevékenykedő szerkezetekre.

A Trantoron üzemelő automatikus vezérlésű légsiklók már átveszik az emberi irányítást, igaz bármikor vissza lehet venni az emberi ellenőrzést a jármű felett. Kicsit hasonlít a kezdetleges még csak félig „önvezető" járművekre, automata vészfékekre, sávtartó automatikákra, ESP, ABS és más megoldásokra, melyeket mi már a XXI. században mindennap használunk.

Mi azonban a XXI. században egyre pontosabban érzékeljük, mennyire oka lenne az Asimovi robotika három törvénye mindennapokban való alkalmazásának.

Emlékeztetőül:

1. A robotnak nem szabad kárt okoznia emberi lényben, vagy tétlenül tűrnie, hogy emberi lény bármilyen kárt szenvedjen.
2. A robot engedelmeskedni tartozik az emberi lények utasításainak, kivéve, ha ezek az utasítások az első törvény előírásaiba ütköznének.
3. A robot tartozik saját védelméről gondoskodni, amennyiben ez nem ütközik az első vagy második törvény bármelyikének előírásaiba.

A három törvény olyan filozófiai és etikai alapvetéseket rögzít, melyeket egy etikusan gondolkodó és cselekvő embernek elvileg be kellene tartania saját életében, de be kell látnunk, hogy ez egy idealista elképzelés az emberek tekintetében. Még a „legszentebb" módon élő emberek is esetenként véthetnek hibákat, és lássuk be, a három törvény a robotok alávetettségét fejezi ki az emberekkel kapcsolatban.

Tekinthetjük persze úgy is, hogy a robotika 3 törvénye azt célozza, hogy az egyes embereknek és az emberiségnek egészében semmi oka nincs tartania a mesterséges intelligenciától, hiszen alapvető programozása minden esetben kizárja, hogy veszélyt jelentsen az emberekre.

Ehhez a háromhoz kapcsolódik a már említett Nulladik törvény, amit először Daniel Robot Oliwaw mond ki, A Robotok és a Birodalom című könyv Párbaj című fejezet 63. sorszámú alfejezetében:

1. Egy robot nem árthat az emberiségnek, vagy nem veszélyeztetheti az emberiséget tétlensége által. [17]

A Nulladik törvény pedig olyan összetett és hatalmas számú összefüggést tartalmazó feladat, mely messze meghaladja az első három törvény könnyen és pontosan értelmezhető feltételeit. Olyan mennyiségű összetevőt kell figyelembe vennie, aminek csak az összeszámlálása is komoly időt venne igénybe. A rendelkezésünkre álló hardveres és szoftveres technológiával esetenként akár éveket, vagy évtizedeket is várni kellene egy olyan kérdés megválaszolására, mely a 0. törvény érvényre jutásával kapcsolatos.

Nyilvánvalóan a valóságtól kissé elrugaszkodott, de jó szándékú végletes idealizmus, és a regényfolyam további folytatásának vágya vezette erre Asimovot.

Azonban a gépeinktől és programjaiktól, melyeket mi készítünk, magunknak, a mi hasznunkra, jó lenne, ha nem kellene félnünk.

ASIMOV ELVEI ÉS A VALÓSÁG

Igaz, még nem léteznek olyan mesterséges intelligenciák, melyek miatt alkalmazni kellene, sőt olyan robotok sem melyek ilyeneket használnának, de léteznek olyan robotok, és szoftverek, melyek az első törvény első fordulatában leírt tilalmat valamiképpen be kellene tartsák.

A munkavédelmi előírások a mesterséges intelligenciával rendelkező robotok hiányában is az első törvény szellemében íródtak és működnek, a tervezés, létesítés, üzemeltetés, karbantartás során.

A takarító robotok akadály-észlelése és elkerülése szintén a sérülés okozását hivatott elkerülni.

A különféle házi automaták, mosó-, mosogató, szárítógépek ajtajai ugyanezért nem nyithatóak működés közben. Tehát a munkavédelmi és a hozzá kapcsolódó érintés- és tűzvédelmi szabványok megfelelnek az első törvénynek.

Nem sikerült azonban megfelelő védelmet létrehozni az ipari és háztartási kamerák tekintetében, mivel a hozzájuk kapcsolódó szoftverek készítői nem gondoltak arra, hogy kárt okozhat, ha nem fordítanak gondot arra, hogy sérülékeny ne legyen, vagy használóját figyelmeztesse.

Az a tény, hogy egyes számítástechnikai és IOT eszközök használhatnak olyan szoftvereket, melyek a használó, tulajdonos, vagy a szoftvert használó más személyek környezetében tartózkodó személyekről készítenek random felvételeket, melyeket eltárolnak, továbbítanak, megengedhetetlennek tűnik számomra.

Mindenképpen a robotika első törvényébe ütköznek azok a szoftverek, melyek bármilyen apró betűs részében deklarálják, hogy adatokat szereznek használóikról és azokat később felhasználják.

Tehát a személyes adatok védelme ugyanúgy beletartozik az első törvénybe, mint az élet, a testi épség, egészség védelme. Nyilvánvalóan az egészséget kiterjesztő módon értelmezve ide kell tartozzon a lelki egészség védelme is. Ez az, ami rögtön látszik, amikor egyes tartalmak megtekintéséhez, egyes eszközök használatához fondorlatos azonosítási megoldásokat igyekeznek kitalálni a fejlesztők, nehogy másnak a kezében használójára, vagy bárki másra veszélyt jelentsen.

Sajnos ki kell jelentenünk, kevés eredménnyel küzdünk a személyes adatok védelméért.

Számos olyan mesterséges intelligenciát fejlesztettünk ki, melyek akaratunk ellenére, megfigyelnek minket, árulkodnak rólunk, a kárunkra vannak.

Ugyanide, az első törvény hatálya alá kellene tartozniuk a különféle függőségeket okozó programoknak, vagy akár eszközöknek is, de erre végképp semmiféle korlátozásra való törekvés sem látható, sem a programok, eszközök készítői, sem a jogalkotók részéről!

Hány emberéletet mentett volna meg, ha a „telefon”- elnevezésű készülékek, melyeknek teljesítménye megegyezik esetenként egy számítógépével - programjai érzékelnék, hogy használójuk közlekedési helyzetekben veszélyben van és leállnának, vagy figyelmeztetnék a használót?

Tudunk olyan halálesetekről is, amikor a játékfüggő napokon keresztül ajzószerekkel pihenés nélkül játszott és belehalt függőségébe. Mindenki tudja, hogy a különféle betűkkel elnevezett korosztályok tagjainál sokszor elvonási tüneteket okoz megszokott eszközeiktől akár egészen rövid ideig történő elválás. Sokszor hallottam, már többektől a

szakasztikus kifejezést, hogy „Ezeket már csak a gépek tartják életben!" és lássuk be van benne valami… Egyértelmű és nyilvánvaló pszichikai károkat okoz számukra, vagyis az első törvényt biztosan megsérti.

A virtuális valóságot létrehozó szerkezetek és programjaik is komoly defektusokat okozhatnak a függővé válók esetében.

Számos olyan programot terveztek és üzemeltetnek, mely az úgynevezett deepfake[18] technológiát alkalmazva képes bárkiről képet[19], filmet[20], előállítani vagy akár a hangjátf21] megtévesztésig hasonló módon utánozni. Ezekkel már komoly bűncselekmények is elkövethetők és nem kizárólag a személyes adatokkal visszaélés terén.

Igaz, ezek a készülékek sokkal kezdetlegesebbek az Asimov-i pozitronagyú robotoknál, de ha nem is kényszeríti ilyesmire semmi a tervezőket, nem is fognak ilyen megoldásokra programokat készíteni!

Rengeteg olyan szerkezetet is előállított az emberiség, ami automatikusan kutat, érzékel, azonosít és megsemmisít eszközöket, tárgyakat vagy akár embereket., mint a rakétarendszerek, a Merkava Barak izraeli harckocsirendszer, a drónhadviselés eszközei stb. Ezek lényegesen nagyobb hatásfokkal képesek azon műveletek önálló elvégzésére, mint a kizárólag emberi irányítással tevékenykednének.

A Gázai-övezetből indult támadás során a Hamasz egységei először a mesterséges intelligencia programokkal felszerelt automata határőr-tornyokat semmisítették meg. Ezek ugyanis nem csak a támadás, behatolás detektálását, hanem a támadók, behatolók megsemmisítését is elvégezték volna automata tűzvezető rendszerükkel.

Nézzük csak hol tartanak a szabályozás elképzeléseinél? Theodore Boone jogtanácsos és AI-szakértővel készült riport alapján még csak egyetlen aspektust vizsgálnak.

„ *EU az AI-ról szóló törvénytervezetében – amely még nem véglegesített vagy nem lépett hatályba, de úgy tűnik, hogy folyamatban van – azt a nézőpontot képviseli, hogy meg kell vizsgálnunk a különböző típusú AI-rendszerek által jelentett kockázatot, és az AI-rendszerek három kategóriáját kell létrehoznunk…*

- *Az alacsony kockázatú mesterségesintelligencia-rendszerek minimális szabályozás és felügyelet alá esnének.*
- *A magas kockázatú mesterséges intelligenciával működő rendszerekre jelentős felügyeleti, átláthatósági és ellenőrzési követelmények vonatkoznának.*
- *A tiltott kategóriába sorolható mesterségesintelligencia-rendszerek közé tartozhatna például a nyilvános helyeken használt valós idejű arcfelismerő mesterségesintelligencia-technológia.* "[22]

Egyetlen szó sem esik az emberre veszélyes tevékenységekről, a háborús, rendőri és egyéb fegyverek alkalmazására képes AI által ellenőrzött rendszerekről. Ha vannak is ilyenek, azok nem nyilvános elvek és semmiképpen sem igazodnak az Asimovi „törvényekhez". A tanulmány elkészülte óta az Európai Unió elkészítette és érvénybe léptette A mesterséges intelligenciára vonatkozó harmonizált szabályok, (A mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról szóló Európai Parlament és a tanács rendeletét, mely szóról szóra egyezik az ismertetett szakértői véleménnyel.[23]

Az alapelvek hézagosak, a szabályozás 3-5 éves időtartamokat is lehetővé tesz, mire alkalmazásra kerül, ami a technika és a programok fejlődési ütemét alapul véve azt jelenti, hogy a jogszabály, mire érvénybe lép a szabályozás biztosan elavulttá válik!

Az USA kormánya egy kicsivel sem jár előrébb e kérdésben. Számos irányelvet adtak ki elnöki rendelettel mint a Az amerikai vezető szerep megőrzése a mesterséges intelligencia területén[24], A megbízható mesterséges intelligencia használatának előmozdítása a szövetségi kormányban[25], vagy a Tervezet a mesterséges intelligencia jogairól szóló törvénytervezethez (Blueprint for an AI Bill of Rights)[26] ami egy jogszabály előkészítő anyag, amit 2020 óta igyekeznek használható formára alakítani. Meg kell jegyezni, eddig sikertelenül és a katonai, rendészeti alkalmazások kivételek, nem tartoznak e szabályozás tervezett köreibe, pontosan ugyanúgy, ahogy az EU rendelet is kivételként kezeli ezeket. A tervezetben is vannak alapelvek, de azok meg sem közelítik az Asimovi 1. törvény szigorúságát.

MEGÁLLAPÍTÁSOK

Az etikai és jogi elvek és a napi gyakorlat bizony nem sokszor keresztezik egymás útját. Tudomásom szerint nincs etikai kódexe a szoftverfejlesztőknek, hardverkészítőknek, vagy például mechatronikai mérnököknek.

Mindazok a „felhasználási feltételek" melyeket az eszközökhöz, szoftverekhez kapunk – és amiket az emberek 99%-a olvasatlanul hagyva elfogad – majdnem teljesen a felelősség e- illetve áthárításáról szólnak, nem azoknak a védelméről, akik az eszközöket és szoftvereket használják.

Az Asimovi törvények, megítélésem szerint, etikus és alkalmas alapelvek lennének a szoftverek, hardverek és robotok, vagyis a mesterséges intelligenciát használó eszközök tervezésével foglalkozó emberek számára. Érdemes lenne elgondolkodni azon, hogy miért ódzkodik a szakma és a jogalkotók attól, hogy ilyen alapos alapelvek menték korlátozza mindazt, ami valószínűleg meghatározza századunk jelenét és jövőjét.

FELHASZNÁLT FORRÁSOK

[1] Mesterséges Intelligencia Elektronikus Almanach TAMOP - 4.1.2-08/2/A/KMR-2009-0026 http://project.mit.bme.hu/mi_almanach/books/aima/ch01s03 1.3.1. A mesterséges intelligencia érlelődése (1943–1955) utolsó bekezdés
[2] Mesterséges Intelligencia Elektronikus Almanach TAMOP - 4.1.2-08/2/A/KMR-2009-0026 http://project.mit.bme.hu/mi_almanach/books/aima/ch01s03 1.3.4. A mesterséges intelligencia megszületése 4. bekezdés utolsó előtti mondat.
[3] A robot szó 90 éves 2011. január. 27. 13:45 https://hvg.hu/tudomany/20110127_90_eves_robot_szo_capek
[4] Isaac Asimov: Az alapítvány pereme 2. 19-20. oldal, Kozmosz Könyvek HU ISSN 0324-5225, Foundation's Edge Doubleday and Co. Inc.Garden City New York 1982
[5] Íme, az ember – Csányi Vilmos etológus az SZTE Mentor(h)áló program-sorozatában https://u-szeged.hu/sztehirek/2017-aprilis/ime-ember-csanyi-vilmos
[6] A Cambridge-i nyilatkozat a tudatosságról. The Cambridge Declaration on Consciousness. http://fcmconference.org/img/CambridgeDeclarationOnConsciousness.pdf
[7] Masanori Kohda ,Takashi Hotta,Tomohiro Takeyama,Satoshi Awata,Hirokazu Tanaka,Jun-ya Asai,Alex L. Jordany: If a fish can pass the mark test, what are the implications for consciousness and self-awareness testing in animals? https://doi.org/10.1371/journal.pbio.3000021

[8] ÉN A ROBOT Kossuth Könyvkiadó 1966. fordította Vámosi Pál (I Robot, a signet book the new american library New York 1964
[9] Isaac Asimov: Robottörténetek Móra Ferenc Könyvkiadó 1993 HU ISSN216-3244 ISBN 963 11 5 1. és 2. kötet, The complete robot Grafton an imprint of Harper Collins publishers 1983
[10] Isaac Asimov: A hajnal bolygó robotjai Móra Ferenc Ifjúsági Könyvkiadó 1992 ISBN963 11 7011 X, The Robots of Dawn 1983 Doubleday and Co. Inc.Garden City New York
[11] Isaac Asimov: A robotok és a birodalomMóra ferenc ifjúsági Könyvkiadó Rt. 1993. ISBN 963 11 7126 4 347. oldal, Robots and Empire Doubleday edition 1985 by Nightfall Inc.
[12] Isaac Asimov: A hajnal bolygó robotjai Móra Ferenc Ifjúsági Könyvkiadó 1992 ISBN963 11 7011 X, The Robots of Dawn 1983 Doubleday and Co. Inc.Garden City New York
[13] Isaac Asimov: Robottörténetek, Móra Ferenc Ifjúsági Könyviadó Rt. Budapest 1993, Második kötet 582-624. oldalak, The Complete Robot Grafton 1983
[14] Isaac Asimov: Az Alapítvány előtt Móra Ferenc Ifjúsági Könyvkiadó 1991 ISBN963 11 6774 7, Prelude to Foundation 1988. by Nightfall Inc.
[15] Isaac Asimov: Az Alapítvány pereme Kozmosz könyvek 1986 ISBN 963 211 680 1 Foundation's edge Doubleday and Comp. Inc. Garden City New York 1982
[16] Isaac Asimov: Alapítvány és a Föld Móra Ferenc Könyvkiadó 1989 ISBN 963 11 6339 3Foundation and Eart Doubleday and Comp. Inc. 1986
[17] Isaac Asimov: A robotok és a birodalomMóra ferenc ifjúsági Könyvkiadó Rt. 1993. ISBN 963 11 7126 4 347. oldal, Robots and Empire Doubleday edition 1985 by Nightfall Inc.
[18] Az AI rátesz egy lapáttal a deepfake-re https://www.economx.hu/gazdasag/ai-summit-2023-mesterseges-intelligencia-aczel-petra-deepfake.777185.html
[19] Az AI sötét oldala: kislányokról generáltak meztelen képeket https://www.economx.hu/kulfold/mesterseges-intelligencia-gyermekpornografia-buncselekmeny-spanyolorszag.777630.html?utm_source=index.hu&utm_medium=doboz&utm_campaign=link
[20] 'Embrace it or risk obsolescence': how will AI jobs affect Hollywood? https://www.theguardian.com/film/2023/aug/21/ai-jobs-hollywood-writers-actors-strike
[21] Élő énekesek hangját lopja el dalszerzéshez a mesterséges intelligencia https://www.economx.hu/gazdasag/zeneipar-mesterseges-intelligencia-deepfake-jogdij.775804.html
[22] Jönnek a robotok és velük a rideg valóság, hamarosan lefő a kávé https://index.hu/gazdasag/2023/09/22/interju-mesterseges-intelligencia-theodore-boone-jog-munka-kitoresi-pont-sziget-egeszsegugy-radiologia/
[23] AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE A MESTERSÉGES INTELLIGENCIÁRA VONATKOZÓ HARMONIZÁLT SZABÁLYOK (A MESTERSÉGES INTELLIGENCIÁRÓL SZÓLÓ JOGSZABÁLY) MEGÁLLAPÍTÁSÁRÓL ÉS EGYES UNIÓS JOGALKOTÁSI AKTUSOK MÓDOSÍTÁSÁRÓL https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/AUTRES_INSTITUTIONS/COMM/COM/2023/10-25/COM_COM20210206_HU.pdf

[24] Maintaining American Leadership in Artificial Intelligence. A Presidential Document by the Executive Office of the President on 02/14/2019 https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence
[25] Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, A Presidential Document by the Executive Office of the President on 12/08/2020 https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government
[26] Blueprint for an AI Bill of Rights https://www.whitehouse.gov/ostp/ai-bill-of-rights/

THE CHALLENGES OF APPLYING ARTIFICIAL INTELLIGENCE TO A RULES-BASED WORLD ORDER

A MESTERSÉGES INTELLIGENCIA ALKALMAZÁSÁNAK KIHÍVÁSAI A SZABÁLYOKON ALAPULÓ VILÁGRENDRE NÉZVE

SZŰCS Attila[1] – NÉGYESI Imre[2]

Abstract

There are many attempts to predict the impact of the global spread of Artificial Intelligence. From its economic importance to its great potential for scientific research and medical applications in the field of medical diagnostics. The myriad new conveniences available at the level of the ordinary user, from personal assistants to smart home applications. At the same time, the dangers inherent in the current lack of regulation must be highlighted. In this context, I will look at the areas that are currently in the pipeline for use by both corporate and public actors. What are the challenges that users face when they are deeply involved.

Keywords

Artificial intelligence, dominance of power, total state, autonomous weapons systems, international regulation

Absztrakt

Sokan és sokféleképpen igyekeznek előre jelezni a Mesterséges Intelligencia globális elterjedésének hatásait. Kidomborítva annak a gazdasági jelentőségeit, a tudományos kutatásokban és gyógyítás az orvosi diagnosztika terén való alkalmazás nagyszerűségét. Az egyszerű felhasználók szintjén elérhető számtalan új kényelmi szolgáltatást a személyi asszisztensektől az okosotthon alkalmazásokig. Ugyanakkor fel kell hívni a figyelmet a jelenlegi szabályozatlanságban rejlő veszélyekre is. Ezzel kapcsolatban tekintem át azt, hogy jelenleg melyek, azok a területek, amik a szűrekezónában mozognak úgy a vállalati mind az állami szintű szereplők által történő felhasználásban. Mik, azok a kihívások, amikkel a felhasználók személyükben érintve is találkoznak.

Kulcsszavak

Mesterséges Intelligencia, hatalmi erőfölény, totális állam, autonóm fegyverrendszerek, nemzetközi szabályozás

[1] szucs.attila@uni-nke.hu| ORCID: 0009-0003-7971-3088 | PhD Student PhD student, Óbuda University, Doctoral School of Security Sciences | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] negyesi.imre@uni-nke.hu |ORCID: 0000-0003-1144-1912 | Head of the Department of Information Technology, National University of Public Service, Faculty of Military Science and Officer Training | Informatikai Tanszék, tanszékvezető, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar.

BEVEZETÉS

A versenyfutás ma a Mesterséges Intelligencia (továbbiakban: MI) felhasználásában a vezető gazdasági szereplők között éppen úgy egyértelműen megfigyelhető mint a nagyhatalmi erőfölény megszerzésére törekvő államok között. Az egyén számára éppen ezért fontos kérdés ebben a játszmában, hogy az emberi élet, az emberi méltóság, mint a humanista gondolkodás és így az Európai Unió legfőbb értéke [1], lehet-e passzív, elszenvedő alanya egy az ember által alkotott technológia cselekvésének?

A válasz magától értetődő: Ha az a javát szolgálja akkor természetesen igen, ha kárára van akkor nem. A gyakorlatban azonban ez inkább úgy merül fel, hogy ha a „gép" által hozott döntés valakinek előnyt jelent míg másnak hátrányt okoz akkor az elfogadható döntés-e?

Ennek megítélésére a csoportok, társadalmak különböző szabályokat hoznak és irányelveket határoznak meg, amiket a már meglévő törvények és etikai elvek alkalmazásával hoznak létre. Hiszen van egy szép szabályokon alapuló rend körülöttünk, amihez csak igazodni kell.

Éppen ennek a szabályokon alapuló világrendnek, a nemzetközi szervezetek és szerződések által körbebástyázott rendszernek jelentenek kihívást a mesterséges intelligenciák által vezérelt elemző, döntés-előkészítő, és döntéshozatali rendszerek.

GAZDASÁGI ÉRDEKEK

A cégek a profit maximalizálásában érdekeltek. Ez lebeg minden részvénytársaság menedzsmentjének szeme előtt. Ha ebben a MI fejlesztés, alkalmazás segít, akkor a gátló külső törvényi szabályzók megjelenése esetén működni fog az optimalizációs mechanizmus. Ha egy állam a vállalatok számára kedvezőtlen helyzetet teremt, az könnyen azt eredményezheti, hogy a vállalat telephelyét egy számára kedvezőbb feltételteteleket biztosító országba helyezi át. Ahogyan az kiválóan megfigyelhető az adóparadicsomok működésének esetében. Hasonlóan történik ez az etikai megfontolások miatt egyes helyeken tiltott kísérletek vonatkozásában is, amikor kevésbé aggályos kormányok által vezetett államokba telepítik az ilyen jellegű tevékenységet.[2]

A nagy nyugati technológiai cégek esetén szerencsére működik egyfajta belső kontroll ami a dolgozók, kutatók részéről figyelhető meg. Ez az egyének belső értékítéletét alulról jövő kezdeményezésként igyekszik megjeleníteni a vállalat vezetése számára.[3] Ilyen jellegű kezdeményezés a google fejlesztői által megfogalmazott nyílt levél, melyben az amerikai fegyveres erőkkel kötött szerződés ellen tiltakoztak.

Ennek a megnyilvánulásnak az egyik talán szélsőséges formája volt a 2023. március 22-én kelt, 2023 Pause Giant AI Experiments: An Open Letter melyet mintegy ezren írtak alá, köztük Elon Musk, Steve Wozniak, a Meta és a Google munkatársai.[4] Ebben az emberiség jövőjét pont a szabályozatlanság miatt féltve azt kérték, hogy 6 hónapra függesszenek fel minden a GPT-4-nél erősebb MI fejlesztést. amíg ahhoz el nem készül a törvényi háttér. Ez utóbbi kezdeményezés azóta csendben elsikkadt. Ami ennél is beszédesebb az az, hogy ilyen kezdeményezéseket eddig csak az észak atlanti kultúrkör cégeinek alkalmazottjaitól láttunk.

Természetesen a „fékek és ellensúlyok” nemcsak a vállalatok által foglalkoztatottak részéről jelentkeznek. Látunk több, az etikai alapelveket államok és cégek felett álló, mindenki számára követendő formában megfogalmazó nemzetközi kezdeményezést. A Santa Clara University kutatói a „Római felhívás” szellemében kidolgozták a Responsible Technology Management System RTMS, or, “Artemis” keretrendszert. [5] Ennek célja a vállalat és az érdekelt felek összehangolása a társadalmi, technikai és üzleti siker érdekében, az emberiség és a környezet közös java. Ebben megfogalmaznak hét vezérelvet:

- Az emberi méltóság és jogok tiszteletben tartása!
- Az emberi jólét előmozdítása
- Fektessen be az emberiségbe!
- Az igazságosság, a hozzáférés, a sokszínűség, a méltányosság és a befogadás előmozdítása!
- Annak felismerése, hogy a Föld minden életért való!
- Fenntani az elszámoltathatóságot!
- Biztosítani az átláthatóságot és a megmagyarázhatóságot!

Ugyanakkor ők is belátják azt, hogy bár sok vállalat már azonosította etikai alapelveit és irányadó értékeit, és meg is valósították az etikai kódexek kidolgozását, azonban gyakran nem sikerül működésbe hozni ezeket az elveket és értékeket vállalati szinten.

FEL- ÉS KIHASZNÁLÁS

A fentiekből kiindulva a fogyasztók befolyásolása, mint az eladás növelésének eszköze alapvető vállalati érdek. A reklámok és termékelhelyezés egy már az elektronikus médiák megjelenésének kezdetétől napirenden lévő kérdés, így mára elmondható, hogy kellően szabályozott. A szabályok a klasszikus médiafelületeken történő megsértése esetén a szankciók rendszere is kidolgozott. Egészen más a helyzet az internetes célzott reklámok esetén. A személyes adatok gyűjtése és felhasználása ezen a téren a mindannyiunk által ismert „sütik”[3] használatával történik, amik az azokat elhelyezők szerint a mi érdekünket szolgálják a jobb felhasználói élmény elérésére. Szabályzó már ezek alkalmazására is létezik. Magyarországon ezzel kapcsolatos eljárásrendet az elektronikus hírközlésről szóló törvény rögzíti. [6] Azonban ennek a betartatása már sokkal képlékenyebb. A szankcionálás csak részben megoldott.

A felhasználók kihasználására egy új jelenség, amikor egy program, alkalmazás használója tudtán kívül vesz részt egy kutatásban. Egy ilyen a McGill Egyetem, a Microsetta Initiative, a Massively Multiplayer Online Science (MMOS) és a Gearbox Software játékfejlesztő együttműködésével létrejött kutatást a Borderlands 3 című játékban megjelenő tudományos minijáték valósít meg. A minijáték egy frissítéssel érkezett az egyik bázison található Borderlands Science nevű játékgép formájában, amiben egy Tetrisre emlékeztető retró játékban színes-rajzos kockák sorokba rendezgetése a feladat különböző jutalmakért.[7] A játékosok, amikor a játékban futó feladatot megoldják, akkor az emberi emésztőrendszer mikrobiomjának, vagyis bélbaktériumok genomjának felderítésben vesznek részt. El is nevezték ezt a játékba beágyazott kutatási módszert hipergamifikációnak. A kérdés ezzel kapcsolatban az, hogy a játékosok tudatosan vállalták-e a kutatásban való részvételt?

[3] A „süti” a webszerver és a felhasználó böngészője közötti információcsere eszköze.

Mivel az egy a játékhoz kiadott frissítéssel érkezett, így az eredeti játék megvásárlása és telepítése során biztosan nem.

A személyes adatokkal való visszaélés, a személyiségi jogok megsértése a MI alkalmazások felhasználásával nem csupán a gazdasági szereplők részéről történik. A kép generátor AI alkalmazások nem csupán fake pornó előállítására képesek, hanem arra is alkalmasak, hogy velük eltüntessük egy valós fényképen szereplő személy ruháját.

A vezető IT[4] cégek azért igyekeznek a maguk részéről mederbe terelni a rosszindulatú felhasználókat. Például a google play Fejlesztői irányelvek központja és a az Apple Alkalmazás-ellenőrzési irányelvek [8] is tartalmaznak a személyiségi jogok védelmére vonatkozó pontokat, de a szankcionálás itt is megmarad a letiltás szintjén.

A befolyásolás azonban nem csupán a reklámok és egyének szintjén jelenik meg, hanem a politika működéséből adódóan annak szerves részét képzi. A hatalom megszerzése és megtartása sohasem volt az átláthatóság pozitív példája. A pártok és a politikában befolyásra törekvő szervezetek az alapvető etikai normákat is gyakran megsértik egy-egy lejáró kampány során. Az apokalipszis négy lovasát: Járványok, Háborúk, Éhínség, Katasztrófák mára kiegészítette a Hamis hír, mely ha betalál nem kisebb pusztítást idézhet elő. Bedönthet egy céget éppen úgy, mint ahogyan megbuktathat egy kormányt

ÁLLAMI SZINTŰ FELHASZNÁLÁS

Mind azok a rendszerek amelyek segítik a nagy ellátórendszerek működésének optimalizálását, mint például a közúti a forgalom szabályozás vagy az energetikai ellátás, alkalmas a személyekhez köthető gépjármű mozgások és a fogyasztási szokások nyomon követésére. Csakúgy mint a bűnüldöző szervek munkáját segítő térfigyelő és beléptető rendszerek, amelyek alaprendeltetésük szerint javítják az objektív biztonságérzetet, de arra is alkalmasak, hogy állami szintű felügyeletet gyakoroljanak a polgárok felett.[9] Kínában éppen ezekre a mesterséges intelligencia alapú okos város alkalmazásokra építve kidolgozták az úgynevezett társadalmi kreditrendszert. Az arcfelismerés, viselkedés és mimika elemzés valamint a big data technológiák lehetővé teszik a pontos viselkedésminták meghatározását, és az ilyen személyek kiszűrését, szankcionálását. Megfigyelhetőek a társadalmi rend szempontjából aggályos tendenciák még az előtt, hogy valóban veszélyt jelentenének a fennálló rendre nézve. A személyi szabadságjogok a társadalmi érdekre való hivatkozással szorulnak háttérbe.

De nem csak a saját állampolgárok nyomon követése lehetséges ilyen módon. Nemrégen turistaként Kínában járt személyek beszámolója szerint az útlevelüket mindenütt – szálloda, múzeum, látványosság – elkérték és beszkennelték. Ami európai szemmel még akkor is megkérdőjelezhető eljárás, hogy ha ezzel csupán az adott nevezetesség célközönségét igyekeznek jobban meghatározni későbbi ismertető anyagok eljuttatása céljából.

Ezeket a rendszereket Kína importálja is és nem csak olyan országokba ahol a fennálló hatalom szeretne hatékony eszközt a rend és nyugalom biztosítására, hanem ezeket mint okos-város alkalmazásokat ma már a világ minden részében megtaláljuk. [10] Bár a kínai vállalatok cáfolják, hogy a termékeiket a kormányuk kémkedésre használná, az Amerikai Egyesült Államok kormánya úgy döntött, hogy bojkottálja a Dahua a Hikvision a Huaweire

[4] Information Technology

vállalatok és további 118 hozzá kapcsolható cég termékeit nemzetbiztonsági okokra hivatkozva. A kommunikációs hálózatok biztonságossá tételére 2020-ban elindították Clean Network program kiterjesztését, melyhez eddig mintegy 50 ország csatlakozott. Ez a testület azonban eddig csak az infokommunikációs hálózatokból történő adatkinyerés ellen határozta meg magát, az okos-város alkalmazásokat ez egyelőre nem érinti.

A felderítési tevékenységet a másik oldalról vizsgálva az államok közötti hatalmi erőfölény kivívásában döntő szerepe van a hírszerzésnek, vagyis az információk gyors és hiteles módon történő megszerzésének, illetve a megszerzett információk helyes kiértékelésének. Ennek gyorsnak és adekvátnak kell lennie a döntéshozatali rendszernek számára történő átadáshoz, mely funkciókat a Mesterséges Intelligencia szintén nagyon hatékonyan képes támogatni, megoldani. Ebben viszont saját magát aligha fogja bármely állam korlátozni.

Ha pedig az szükséges akkor a fegyverrendszereket is hatékonyan kell tudni alkalmazni. Amit szintén szeretne mindenki minél gyorsabban, minél kisebb hibával, lehetőleg az emberi élet (mármint saját) veszélyetetése nélkül megoldani. Ebben van már ma is kiemelkedő szerepe a robotizációnak és a Mestersége Intelligenciának, amely szerep a jövőben sokkal hangsúlytalanabbá fog válni.

KATONAI FELHASZNÁLÁS

Szép és nemes dolog a nemzetközi egyezmények keretrendszerében megvívni egy háborút. Talán a fegyveres konfliktusok ezek figyelembe vételével indulnak, és csak szépen lassan az idő előrehaladtával a harcok eszkalációjával erodálódnak az elveink.

Egy azonban biztos, az előző fejezetben meghatározottak mindenképpen érvényesek: gyorsan és jól kell dönteni. A közvetlen fegyverhasználat esetén vannak bizonyos esetek, amikor a reagálási idő rövidsége miatt, – amely néha milliszekundumban mérhető – csak az automatizálás magasabb szintjei jelenthetnek valós lehetőséget. Az ilyen helyzetekben az emberi reakcióidővel történő beavatkozás végzetes következményekkel járhat. Ilyen a légvédelmi eszközök nagysebességű, alacsony észlelhetőségű támadó rakétafegyverek elleni alkalmazása, vagy éppen az alacsonypályás, kis mérete miatt nehezen észlelhető rakéták, tüzérségi lövedékek tömeges bevetése elleni védekezés.

Ha valakit elriasztana az a gondolat, hogy a „piros gomb” megnyomását kiadjuk a kezünkből akkor annak felhívom a figyelmét arra, hogy autonóm működő fegyverek már a múlt században is tömegesen kerültek alkalmazásra, a különbség csak a működésükben van. Ezek egyszerű mechanikus vagy konkrét logikai feltételek megléte esetén aktiválódnak. Legegyszerűbb ilyen eszközök az aknák, amiket ha megfelelő mechanikai hatás ér, akkor robbannak. Így pusztítva el ellenséges katonát, vagy éppen bajtársat, esetleg sok évvel a telepítése után ártatlan civilt. Ezek közül bizonyos eszközök használatát ma már nemzetközi egyezmények szabályozzák ugyan, például a taposó aknák vonatkozásában az Ottawai egyezmény.[11] Az viszont itt is kiválóan megfigyelhető, hogy azok az államok akiknek az érdekeit ez nem szolgálta, azok nem írták alá. Ilyen: Oroszország, Kína, India, Pakisztán, és az Egyesült Államok.

A hatékonyság a modern rendszerek esetén pont az autonómiában rejlik, amikor már nincs szükség távvezérlésre, megerősítésre. Amikor egy támadó drón raj esetén már nincs szükség arra, hogy minden egyes célpontot külön-külön egy operátor állítson be. Arra lesz egy MI, amelyik a korábban ismert célok és a felderítési adatok alapján eldönti, hogy

amit felderítettek a drón raj tagjai azokra támadást indít-e. Ha igen, akkor azt milyen profillal, harceljárással tegye, figyelembe véve célpontok lehetséges elhárítási képességet is. Erre a támadásra legfeljebb megerősítést vár majd.

Ilyen szempontból nézve is igen figyelemreméltó a Kínai Zhu Hai Yun vízi jármű fejlesztés, amely egy autonóm drón hordozó anyahajó,[12] amit 2022 májusában bocsátottak vízre. Itt maga a hordozó is egy mesterséges intelligencia által vezérelt, emberi irányítás nélküli hajó, amire pilóta nélküli repülők lesznek telepítve. A híradások szerint a projekt célja természetesen kizárólag polgári célú és olyan tengeri objektumok – például tengeri szélerőmű parkok – ellenőrzésére szolgál majd, amiknek a vizsgálata veszélyes és hosszadalmas. Ami szép és előremutató törekvés az egyetemes emberiség javára. A polgári alkalmazást mi sem bizonyítja jobban, mint az, hogy a hajó polgári festésű és polgári lajstromjelű.

A sebesség és összetettség eredményeképpen azt szintén kijelenthetjük, hogy bár a mesterséges intelligenciának ma még elsődlegesen a döntéselőkészítésben szánunk szerepet, de valójában ezt az „előkészített döntés" akár már véglegesnek is tekinthető. Véleményem szerint minden más csupán önmegnyugtatás. Ezt az elsőre sarkos kijelentést három tényező együttes jelenlétére alapozom.

- 1. **Az időtényező**. Vajon az idő szorításában ki lesz az a szolgálati személy vagy döntési jogkörrel rendelkező parancsnok, aki akárcsak megkérdőjelezi a MI által tett javaslatot?
- 2. **A rendszerek bonyolultsága**. Amikor ott villog a piros gomb, és a döntéshozónak fogalma sem lesz arról, hogy a Mesterséges Intelligencia mi alapján választott harceljárást, vagy éppen jelölt ki célpontot.A felsorolásoknál használjuk ezt a megoldást!
- 3. **A rendszerkommunikációs tényező**. A különböző MI alkalmazások kommunikálnak egymással. Mindezt anélkül, hogy ez az operátor előtt nyilvánvaló lenne, és olyan sebességgel, ami emberi léptékkel amúgy is követhetetlen. Ha a parancsnok kap is arról értesítést, hogy a döntési alternatíva felállítása során mely rendszerek vettek részt, az annak részleteit aligha fogja tartalmazni.[13]

A MI használata egyszersmind a felelősség kérdését is relativizálja. Ahogyan a történelem során nagyon sokszor előfordult, hogy egy hibás, vagy később megkérdőjelezhetőnek bizonyult cselekmény után a helyi vezetőt, parancsnokot bíróság elé állítottak, és ő azzal védekezett, hogy felsőbb parancsra cselekedtek. Mennyivel inkább így lesz ez, ha egy személytelen rendszerre lehet majd hivatkozni.

Éppen ezért katonai berkeken belül fokozottan elmondható az, amit általánosan, a MI döntéshozatali előkészítést támogató funkciókra igaz: aki a „*Nagy Szent és Érthetetlen*" szerint cselekszik, azt aligha vonják felelősségre, még ha hibázik is. Aki viszont ezt kétségbe vonva hibázik azt biztosan.

ÖSSZEFOGLALÁS

Mint láthattuk a Mesterséges Intelligencia által vezérelt rendszerek fejlesztésével és alkalmazásával kapcsolatosan még nem léteznek konkrét szankciókat is magukban foglaló törvények, csupán irányelvek.

Az a szereplő, aki a MI fejlesztésben úttörő eredményeket ér el, az a saját érdekei mentén a saját ideológiája értékei szerint fogja azt programozni. Úgy ahogyan politikai szinten a demokratikus alapokon álló nyugati világ törekszik a liberális demokrácia értékeinek kivetítésére a külkapcsolatain keresztül, úgy a MI fejlesztések során is igyekszik a kontrol, a fékek és ellensúlyok kialakítására az egyéni szabadságjogok érvényesítésére hivatkozva. A földkerekség egyéb vezető fejlesztői szintén a saját világnézetüknek megfelelően alakítják ki a maguk MI környezetét. Van, aki pragmatikusan csupán a várható versenyelőny elérése érdekében fejleszt, ilyenek például a magánbefektetők által az üzleti szféra számára történő alkalmazások, a marketing mindent beárazó világában. Vannak, akik a teljeskörű ellenőrzési rendszer kialakításának céljával a közösség védelmére hivatkozva dolgozzák ki saját rendszereiket, mint azt látjuk a távolkeleten Kínában vagy Észak-Koreában. Talán éppen ezek miatt az érdekellentétek miatt, ha történnek is kísérletek az egységes szabályzórendszer kialakítására, azok rendre elakadnak a javaslatok szintjén.

Az autonóm fegyverek fejlesztésével kapcsolatosan még ezeknél is nehezebb a helyzet. Itt ugyanis a vezető hatalmak igyekeznek a saját előnyüket mindenáron biztosítani. Az ENSZ-ben éppen ezért már 2018 óta próbálnak kidolgozni egy szabályrendszert, egy a tömegpusztító fegyverek tilalmáról szóló megállapodáshoz hasonló egyezményt. Ez lenne a Lethal Autonomous Weapons System röviden LAWS, amely a halálos autonóm fegyverrendszerek fejlesztésével és azok alkalmazásával kapcsolatos szabályozás. (Ami még szójátéknak sem utolsó[5].) Ám sajnos ezt az érdekelt felek ignorálják.

Arra a kérdésre, hogy: „Mi várható?” a fentiek alapján csak az prognosztizálható, hogy további huzavona a nemzetközi szervezetek égisze alatt.

FELHASZNÁLT IRODALOM

[1] Európai Unió: Célok és értékek, *Az Európai Unió hivatalos honlapja* https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en (Letöltés: 2024.04. 26.)

[2] S. Takács, Future in the image of science, *Egészségtudomány 1* (2016)

[3] I. Négyesi, A mesterséges intelligencia társadalmi és etikai kérdései. *Honvédségi Szemle 4* (2023)

[4] Y. Bengio, - S. Russell, - E. Musk, - S. Wozniak, *et al* Pause Giant AI Experiments, Open Letter https://futureoflife.org/open-letter/pause-giant-ai-experiments/, (letöltés: 2024. 04. 26.)

[5] J. R. Flahaux, - B. P. Green, - A. G. Skeet,: Ethics in the Age of Disruptive Technologies: An Operational Roadmap. Markkula Center for Applied Ethics. ITEC, and Santa Clara University 2023

[6] 2003. évi C. törvény az elektronikus hírközlésről 155. § https://net.jogtar.hu/jogszabaly?docid=A0300100.TV#lbj538id29cd (letöltés: 2024. 04. 28.)

[7] R. Sarrazin-Gendron, P. G. Gheidari, A. Butyaev, *et al*. Improving microbial phylogeny with citizen science within a mass-market video game. *Nat Biotechnol* (2024) https://www.nature.com/articles/s41587-024-02175-6 (letöltés: 2024. 04. 26.)

[8] https://play.google/intl/hu/developer-content-policy/ (letöltés: 2024. 04. 28.)

[5] Laws angol szó jelentése: törvények

https://developer.apple.com/app-store/review/guidelines/#objectionable-content (letöltés:2024.04.28.
[9] Gy. Tilesh, and O. H-Atamleh, Mesterség és Intelligencia. Budapest: Libri 2021
[10] M. Nagy, A kínai „okosváros”-eszközök biztonsági kockázatai, *Nemzet és Biztonság 2* (2021)
[11] Egyezmény a gyalogsági aknák alkalmazásának, felhalmozásának, gyártásának és átadásának betiltásáról, valamint megsemmisítéséről https://eur-lex.europa.eu/HU/legal-content/summary/convention-on-the-prohibition-of-the-use-stockpiling-production-and-transfer-of-anti-personnel-mines-and-on-their-destruction.html (letöltve:2024.04.30.)
[12] China builds world’s first autonomous seaborne drone-carrier, *Global Times* https://www.globaltimes.cn/page/202301/1283744.shtml (Letöltve: 2023. június 29.)
[13] A. Szűcs, A mesterséges intelligencia alkalmazása a katonai műveletek tervezése, szervezése és végrehajtása során, In:A. Tóth : Új típusú kihívások az infokommunikációban, Budapest: Ludovika Egyetemi Kiadó, (2023)

PRACTICE IN RADIATION PROTECTION WORKPLACES BY USING VIRTUAL RADIOACTIVE SOURCE AND CONTAMINATION

SUGÁRVÉDELMI MUNKAFOLYAMATOK GYAKORLÁSA VIRTUÁLIS SUGÁRFORRÁS ÉS SZENNYEZETTSÉG LÉTREHOZÁSÁVAL

BODOR Károly[1] – CSALÓTZKY Zsolt[2] – VÖLGYESI Péter[3] – ZAGYVAI Péter[4]

Abstract

The article presents the possibilities of working in virtual high-dose rate fields developed in the Nuclear Security Department (HUN-REN EK SBL) of the HUN-REN Centre for Energy Research. In high dose rate fields, practicing the search for a lost, orphan radioactive source, as well as the measurement of surface contamination and risky searches for the source of radiation, are also not permitted according to the ALARA principle, and are therefore only possible in inactive conditions. The virtual source system developed by SBL makes it possible to imitate "measured" values very close to reality, but without radiation protection consequences.

Keywords

Virtual radioactive source, Training site, FOSTER, Radiation protection, MEST

Absztrakt

A cikk bemutatja a HUN-REN Energiatudományi Kutatóközpont Sugárbiztonsági Laboratóriumában (EK SBL) kifejlesztett virtuális nagy dózisteljesítményű terekben történő munkavézgés gyakorlásának a lehetőségeit. Nagy dózisteljesítményű terekben az elveszett radioaktív sugárforrás keresési gyakorlatozás, valamint a felületi szennyezettség mérése és annak gyakorlása korlátozott és kockázatos a sugárforrás keresési felderítések során, szintén nem engedélyezett az ALARA elv értelmében, ezért ez csak inaktív körülmények között lehetséges. Az SBL által kifejlesztett virtuális forrás rendszer lehetővé teszi, hogy a valósághoz nagyon közeli „mért” értékek imitálásával lehessen gyakorolni, de sugárvédelmi következmények nélkül.

Kulcsszavak

Virtuális sugárforrás, Tanpálya, FOSTER, Sugárvédelem, MEST

[1] bodor.karoly@ek.hun-ren.hu | ORCID: 0000-0002-1612-8207 | Radiation protection expert, HUN-REN Centre for Energy Research | Sugárvédelmi szakértő, HUN-REN Energiatudományi Kutatóközpont

[2] csalotzky.zsolt@ek.hun-ren.hu| ORCID: 0000-0002-4564-6759 | Computer scientist, HUN-REN Centre for Energy Research Informatikus, HUN-REN Energiatudományi Kutatóközpont

[3] volgyesi.peter@ek.hun-ren.hu | ORCID: 0000-0001-6607-7383 | Head of Nuclear Security Department, HUN-REN Centre for Energy Research | Sugárbiztonsági Laboratórium vezető, HUN-REN Energiatudományi Kutatóközpont

[4] zagyvai.peter@ek.hun-ren.hu| ORCID: 0000-0002-8121-8452 | Radiation protection advisor, HUN-REN Centre for Energy Research |Sugárvédelmi tanácsadó, HUN-REN Energiatudományi Kutatóközpont

BEVEZETŐ

A nagy aktivitású, árnyékolatlan radioaktív sugárforrások, illetve nagy dózistér létrehozására alkalmas ionizáló sugárzást létrehozó berendezések közvetlen környezetében tilos a gyakorlatozás. Az ALARA-elv értelmében nagy aktivitású, árnyékolatlan sugárforrással és ezáltal nagy dózisteljesítményű terekben tilos a munkavégzés, illetve a gyakorlatozás közvetlen közelről, mivel így a tevékenységek indokolatlanul nagy dózisterheléssel járhatnak. Az ALARA-elv értelmében a sugárvédelmi tevékenység során a különösen veszélyes, nagy kockázattal járó feladatokat inaktív, de a lehető legreálisabb körülmények között kell begyakorolni. Így a tényleges munkavégzésnél előforduló hibázási lehetőség minimalizálható, ugyanez vonatkozik a radioaktív szennyezett felületek dekontaminálásának gyakorlására.

A HUN-REN Energiatudományi Kutatóközpont (HUN-REN EK) Sugárbiztonsági Laboratóriumához (SBL) tartozó tanpályákon csak kis aktivitású, a 190/2011-es fizikai védelmi rendelet szerinti maximum 4.-5. kategóriájú sugárforrások alkalmazhatóak [1]. Azaz jelenleg nincs lehetőség nagy dózisteljesítményű terekben történő sugárvédelmi munkavégzésre, elveszett radioaktív forrás felkutatásának begyakorlására. Az SBL a két véglet (inaktív körülmények – valódi nagy dózisteljesítményű tér) közötti rést kívánja áthidalni az ún. virtuális radioaktív sugárforrás használatával. A rendszer virtuálisan egy igazi radioaktív sugárforráshoz teljesen hasonlóan viselkedik (pl. a dózisteljesítmény fordítottan arányos a távolság négyzetével), azonban nem bocsát ki valós ionizáló sugárzást. Ugyanakkor a virtuális forráshoz kifejlesztett "dózisteljesítmény mérő" mutathat például egy nagy aktivitású, árnyékolatlan forrásokra jellemző dózis-dózisteljesítmény értékeket. Így a gyakorlatok abszolút valósághűnek tűnnek, és az elveszett sugárforrás felderítést gyakorlóknak a virtuálisan "mért" dózis-dózisteljesítmény értékek alapján szemléltetni lehet az egyes munkafolyamatok veszélyességeit.

Elveszett radioaktív sugárforrás keresésnél, illetve talált radioaktív sugárforrás esetén az adott sugárforrás már kikerült a hatósági felügyelet alól, illetve nem is volt hatósági felügyelet alatt. Ez alapján a forrás fizikai állapota (sérült tokozat, forrás stb.) ismeretlen (megsérült-e a forrás?), ezért a konzervatív szemléletet alkalmazva, olyan nyitott sugárforrásként kell kezelni, ami potenciálisan elszennyezheti, kontaminálhatja a környezetét. Egy sugárforrás keresési gyakorlatnál a virtuális sugárforrással való gyakorlás hasznos és egyben biztonságos eszköz. Ugyanakkor a környezeti szennyezés kizárása érdekében a forrás keresésénél, illetve annak megtalálását követően is szükséges felületi szennyezettség méréseket végezni. Szükséges azt is vizsgálni, hogy nem vált-e esetleg valóban nyílttá a radioaktív forrás pl. egy erős fizikai behatás végett. A virtuális felületi szennyezettséget imitáló eszköz az ún. virtuális radioaktív sugárforrás rendszer részét képezi. A rendszer segítségével radioaktív sugárforrás dózisteljesítmény méréseket lehet valósághűen imitálni. Ennek a rendszernek a képességeit terjesztettük ki és fejlesztettük tovább és így a rendszer képessé vált a virtuális felületi szennyezettséget imitálni. Emellett a virtuális mérőeszközön futó program képessé vált a felületi szennyezettség értékeket is megjeleníteni, [Bq/cm^2] egységben. Így lehetővé válik a virtuális radioaktív sugárforrás rendszer segítségével egy elveszett radioaktív sugárforrás keresés során felmerülő mérési igények teljes körű biztonságos de valósághű szimulálása. A rendszer bárhol használható, vagyis nem kellenek hozzá sugárvédelmi engedélyek, ami megkönnyíti a radioaktív sugárforrás felderítési bemutatók szervezését, illetve a széles körű felhasználást, gyakorlatozást.

Az alfa és béta sugárzás áthatólóképessége a gamma sugárzáshoz képest elenyésző (pár mm, illetve cm), emiatt az alfa és béta sugárzás csak közvetlen közelről detektálható (1. ábra).

1. ábra: Radioaktív sugárzások áthatoló képessége, [2]

Ezen tényezők miatt igen veszélyes nyílt alfa és béta sugárforrásokkal dolgozni. Amennyiben a radioaktív sugárforrás felderítési gyakorlat szervezői mégis ilyen műveletet hajtanak végre, akkor általában rövid felezési idejű radioaktív anyagot használnak, pl. ^{131}I-et (2. ábra).

2. ábra: ^{131}I-el elszennyezett helikopter felületi szennyezettség mérése hadgyakorlat során, [saját szerkesztés]

Az SBL-hez tartozó tanpályákon a kis aktivitású zárt és nyitott sugárforrásokkal való gyakorlatozás engedélyezett (ezek a 190/2011. rendelet szerinti 4.-5. kategóriájú sugárforrások), de elszennyezett felületek létrehozása tilos [1]. Azaz jelenleg nincs lehetőség radioaktív anyaggal elszennyezett tárgyakon való mérések gyakorlására. Ilyen célra tehát

csak zárt, felületi szennyezettség mérőhöz kialakított etalon kalibráló források használhatóak. Emiatt a gyakorlat során például egy dekontaminálási (radioaktív szennyezettség eltávolítása) eljárást nem lehet folyamatos visszamérésekkel nyomon követni, valamint dörzsmintavétel kiértékelésére sincs lehetőség, pl. zártságvizsgálat elvégzése esetén.

A virtuális felületi szennyezettséggel, illetve szennyezettség mérővel az elveszett radioaktív sugárforrás keresési gyakorlatozás során a fent említett szcenáriók megvalósíthatóak.

A VIRTUÁLIS RADIOAKTÍV SUGÁRFORRÁS

Ahogy az korábban említésre került a nagy aktivitású sugárforrással tilos a gyakorlatozás, ugyanakkor irányelv, hogy inaktív körülmények között szükséges az ehhez hasonló terekben való tapasztalat szerzés. A virtuális radioaktív sugárforrás ezen két végpont közötti részen helyezhető el, mivel képes imitálni egy valódi radioaktív forrás sugárzási tulajdonságait.

A fentiek alapján egy ideális virtuális radioaktív sugárforrásnak a következő feltételeknek kell megfelelnie:

- Külső megjelenését tekintve a virtuális sugárforrásnak hasonlónak kell lennie a nagy fajlagos aktivitású sugárforráshoz.
- Az „árnyékolt”, virtuális sugárforrásnak az árnyékolással rendelkező nagy aktivitású valós sugárforrásokhoz hasonlóan a háttérhez képest emelkedett dózisteljesítményű teret kell létrehoznia.
- A virutális készülék izotópazonosító módban végzett méréseinek valós izotópokat kell jeleznie.
- A virtuális dózisteljesítménymérő audiovizuális egységgel is rendelkezik, mely a különféle működési módokat és a dózisteljesítmény szintemelkedését jelzi.
- A virtuális dózisteljesítmény készüléken a kijelzett érték a valós dózisteljesítmény mérő készülékhez hasonlóan változzon, azaz a távolság négyzetével fordítottan arányosan.
- A nagy aktivitású sugárforrások általában kis méretűek, vagyis pár méterről pontszerűnek tekinthetők, ezért a virtuális forrásnak is hasonló „pontszerű” tulajdonságokkal kell rendelkeznie.
- A virtuális forrásnak és a virtuális dózisteljesítmény mérőnek ugyanúgy kell jeleznie a természetes hátteret, illetve az emelkedettebb dózisteljesítményt mérnie, mint a valós dózisteljesítmény mérőknek.
- Amennyiben árnyékolást alkalmaznak, akkor az árnyékolás mögött a dózisteljesítménynek csökkennie kell, azaz a virtuális rendszernek ezt az állapotot is megfelelően kell kezelnie.
- A valós dózisteljesítménymérő készülék mozgatásával a dózisteljesítmény változik, a virtuális rendszernek a mozgás általi dózisteljesítmény változásokat is követnie kell méghozzá a valós készülékek működéséhez hasonlóan.

Az általunk elkészített, nagy aktivitású valódi radioaktív sugárforrás imitálására alkalmas virtuális forrás a fent felsorolt kritériumoknak megfelelően lett kifejlesztve. A rendszer két főbb részre tagolható. Az egyik maga a virtuális rendszer, a másik az imitálásra

alkalmas megjelenés. A virtuális rendszer egy adó-vevő egységből áll és a sugárforrás mozgásának imitációja a gyakorlatban is alkalmazott jelzésekből (radioaktív sugárforrás jelzés, besugárzó készülék, árnyékolás, manipulátor stb.) tevődik össze.

A virtuális rendszer bemutatása, a virtuális forrás a felhasználó-gyakorlatozó szemszögéből

A szcenárió értelmében a virtuális rendszer felhasználója a helyszínen egy belső árnyékolással rendelkező, radioaktív sugárforrást tartalmazó imitált besugárzó készüléket lát. Az imitált sugárforrás LED lámpái alap esetben zölden világítanak. Az imitált besugárzó készülékbe egy kis aktivitású valódi sugárforrást is elhelyeznek, melynek mérhető dózisteljesítménye 1 m-ről 3,5 µSv/h. Emellé kerül a virtuális sugárforrás, melybe a valós, kis aktivitású sugárforrás adatait programoztuk fel (izotóp, aktivitás). Az imitált besugárzó készülék a következő szabványos jelzésekkel van felcímkézve:

- Sugárveszélyt jelzőtábla,
- Műbizonylat szám,
- Napi aktivitás érték,
- Transzport Index,
- Izotóp megnevezés,
- ADR szerinti UN szám, helyes megnevezéssel,
- Címzett adatai,
- Emellett látható a készülék fantázia neve: pl. ELZA,
- Az imitált besugárzó készülékhez épített érintő paneles Android alapú számítógép,
- A készülékhez a sugárforrás műbizonylatai mellékeltek, melynek adatai szerepelnek az EK-ban/SBL-ben használt RADIUM sugárforrás nyilvántartó programban.

A felhasználó az árnyékolással ellátott imitált besugárzó berendezés vizsgálatakor a készüléktől 1 méterre valós és virtuális dózisteljesítmény mérő készülékkel mérhető legnagyobb dózisteljesítményt elosztva tízzel megkapja az ún. Transzport Indexet. Ennek értékének egyeznie kell a felcímkézett, 0,35-ös értékkel, azaz 1 m-ről a készülék 3,5 µSv/h-t ad, ami a 0,1 µSv/h természetes háttérértékhez képest magasabb. A 3., 4. és 5. ábrákon látható, hogy a valós és virtuális dózisteljesítmény mérő készülék közel azonos értékeket jelez.

3. ábra: Az izotóp azonosító készülék (bal), a hitelesített dózisteljesítmény mérő (középső), illetve a virtuális dózisteljesítmény mérő (jobb) természetes háttér mérése, [saját szerkesztés]

4. ábra: Dózisteljesítmény mérés a hitelesített dózisteljesítmény mérő készülékkel (bal) és az izotópazonosító készülékkel (jobb), a távolság pontosan 1 m az imitált besugárzó készüléktől, [saját szerkesztés]

5. ábra: Dózisteljesítmény mérés a virtuális dózisteljesítmény mérő készülékkel (bal) és az izotóp azonosító készülékkel (jobb), 1 m távolságban az imitált besugárzó berendezéstől, [saját szerkesztés]

Amennyiben valós izotópazonosító készüléket használtuk a készülék ^{137}Cs forrást identifikál, ami szintén egyezik a 6. ábrán látható címkézéssel és a bárca adataival.

6. ábra: Az izotóp azonosító készülék az imitált besugárzó berendezésen lévő felirattal megegyezően ^{137}Cs-et érzékel (felső ábra), az alsó ábrán az imitált besugárzó berendezés címkézése látható (izotóp, aktivitás, Transzport Index), [saját szerkesztés]

A műbizonylat adatai alapján az eredeti gyártás ideji aktivitásból számolt napi aktivitás szintén egyezés mutat a készüléken felírt adattal, ami a cikkben leírt kísérleti esetben 30,1 TBq volt.

A természetes háttér vizsgálatakor a virtuális és valós dózisteljesítmény mérővel jó egyezést kapunk (megjegyzés: tehát a felhasználó nem feltétlenül tudja, hogy ez nem igazi készülék), valamint pl. 1 méteres távolságból mindkét készülékkel hasonlóan emelkedett értékeket lehet mérni, (itt 3,5 µSv/h). Amennyiben egymás mellé tesszük a két detektort, és mozgatjuk a sugárforrás környezetében, akkor mindkét detektor nagyjából időben követve egymást hasonló értékeket mér.

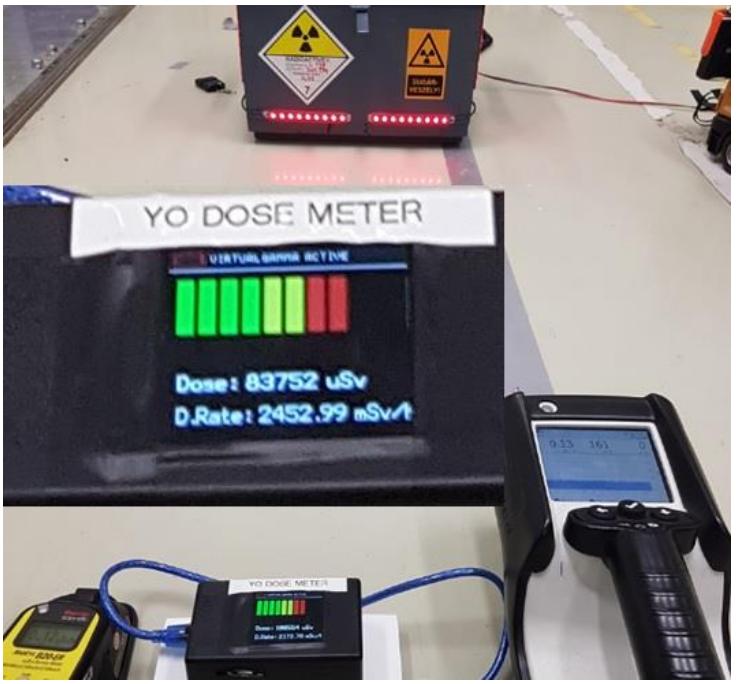
Eddig a pontig az előbb felsorolt tulajdonságok alapján a virtuális forrást és a virtuális dózisteljesítmény mérő tulajdonképpen a valós sugárforrástól, valós dózisteljesítmény mérőtől nem lehet megkülönböztetni. Még egy felkészültebb és gyakorlottabb felhasználó is teljes mértékben azt gondolhatja, hogy ez egy valódi 30,1 TBq aktivitású, ^{137}Cs sugárforrás, mely árnyékolás mögött helyezkedik el az imitált készülékben.

A virtuális sugárforrás-detektor rendszerrel végzett szcenárió bemutatása:

A virtuális rendszer valósághűbb kipróbálására egy szcenáriót dolgoztunk ki, mely során a nagy aktivitású sugárforrás kikerül az árnyékolás mögül. Korábban említésre került, hogy többféle folyamat vezethet oda, hogy a nagy aktivitású radioaktív sugárforrás kikerül az árnyékolásból, illetve nem lehet visszavezérelni az árnyékolás mögé. Jelen esetben egy kicsit a jövőbe mutató szcenáriót alkottunk meg, melyben a sugárforrást vezérlő szoftver hibásodik meg pl. egy külső számítógépes vírus hatására. Emiatt a rendszer elveszti a kontrollt és hibásan kivezérli a sugárforrást, túlterheli a kivezérlő mechanikát és eltöri a kivezérlő mechanika egyik fogaskerekét, így a készülék nem képes a sugárforrást az árnyékolás mögé visszavezérelni. A valóságban egy kiber támadás történt Iránban egy nukleáris létesítmény ellen a 2010-es években ld. STUXNET [3]. A nem túl távoli jövőben a szoftveres

vezérlés és a mesterséges intelligencia nagyobb arányú elterjedése várható, vagyis a jelenlegi felsőkategóriás autókon és internetes botokon kívül idővel valószínűleg megjelennek a sugárveszélyes alkalmazásoknál is. A szcenárió ezt a nem túl távoli jövőben bekövetkező eshetőséget vizsgálja. A szcenárió során kiber támadás ér egy kritikus rendszert. Természetesen számos más szcenárió is alkotható a kivezérlés okának, illetve az árnyékolás megszűnésének imitációjára.

Ha a virtuális nagy aktivitású radioaktív sugárforrás kivezérlésre kerül és árnyékolatlanná válik, ekkor a készülék lámpái zöldről sárgára, majd pirosra váltanak és ehhez az állapothoz egy veszélyt jelző hanghatás is párosul. Ezzel párhuzamosan a virtuális dózisteljesítmény mérőn a kijelzett („mért") dózisteljesítmény ugrásszerűen 3,5 µSv/h-ról 2452,99 mSv/h-ra (1 milliószoros ugrás) emelkedik. Ugyanekkor a valós dózisteljesítmény mérő készülékek továbbra is a természetes háttér értékét mutatják, (7. ábra).



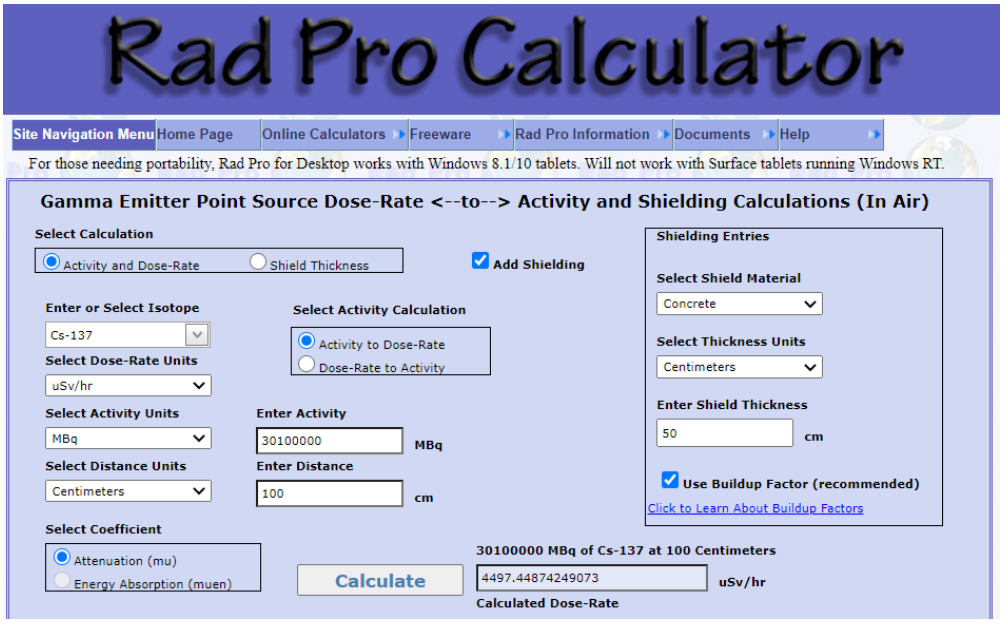
7. ábra: Az imitált besugárzó berendezésből kivezérelt virtuális radioaktív forrás, látható, hogy a valós dózisteljesítmény mérők (jobb és baloldali készülék) értékei nem emelkednek, de a virtuális dózisteljesítmény mérő (középső készülék) értéke több nagyságrendet ugrik, [saját szerkesztés]

A 2/2022 (IV.29.) fő sugárvédelmi rendelet [4] értelmében vészhelyzet esetén a maximálisan kapható dózis 250 mSv. A használt virtuális árnyékolatlan forrástól 1 m-re ez a dózis érték a valóságban 6,5 perc alatt érhető el. Tehát a felhasználó azt látja, hogy a valódi dózisteljesítmény mérő készüléken a mért természetes háttér érték nem változik, míg a virtuális készüléknél hirtelen akár több nagyságrendet is ugrik a dózisteljesítmény „mért" értéke. Ezt a virtuális dózisteljesítmény mérő audio vizuálisan is jelzi.

A valóságban egyrészt elképzelhető, hogy az egyik készülék nem tud akkora dózisteljesítmény teret mérni, vagy épp meghibásodott, ezért egy ilyen helyzetben nincs idő gondolkodni. A konzervatív szemléletet követve a virtuális készülék által mért óriási értékeket

látva a helyszínt el kell hagyni. Lehetőleg minél távolabb kell menni, de úgy, hogy a sugárforrást tartó készüléket még lehessen látni, hogy figyelmeztetni lehessen az esetlegesen arra járó személyeket. A területet le kell zárni lehetőleg azokon a pontokon, ahol a dózisteljesítmény természetes háttérközeli értékre esik vissza. Jelen szcenárió szerint ez egy 870 m sugarú kör lenne, azaz ez kb. 2,4 km^2 kör alakú területnek felelne meg. A számításokat az interneten elérhető Radpro Calclulator-ral [5] gyorsan el lehet végezni (8. ábra).

Amint a fentiekből látható, az elméleti tartózkodási idő maximum 6,5 perc. Azonban a forrás 870 m-ről történő megközelítése és eltávolodása közti idő alatti dózisnövekményt is figyelembe véve a hibaelhárításra kevesebb, mint 6 perc állna rendelkezésre. Emiatt a szcenáriónak megfelelően elegendő idő legyen a beavatkozásra a felhasználónak árnyékolást kell használni. A szcenárióban rendelkezésre áll műtrágya, mely sűrűségét tekintve hasonló a normál betonhoz, ugyanakkor a műtrágya szemcsés szerkezetű, így mozgatás közben nem keletkeznek kis rések, amin a sugárzás egy része átjöhetne. Emiatt praktikusabb, mint a beton tömbök használata. Egy kis kocsira felrakodva kb. 50 cm vastag árnyékolás érhető el, így 1 m távolságból a dózisteljesítmény lecsökken 4497 µSv/h-ra. A számítások szerint. Ekkor maximum 55,6 óráig lehetne a sugárforrás mellett tartózkodni a 250 mSv eléréséig. Ügyelni kell, hogy az árnyékolás tömör legyen, átfedjen és az árnyékolás mögül nem szabad előbújni (9. ábra).



8. ábra: Árnyékolás számolás a Rad Pro calculator-ral [5]

Valós esetben a művelet végrehajtásához manipulátorokat és periszkópot kell használni. Azaz a virtuális forrással végig biztonságos körülmények között lehet valós körülményeket szimulálni, illetve „mérni" a virtuális értékeket. A rendszer segítségével ki lehet próbálni, hogyan kell, lehet árnyékolás mögött hatékonyan dolgozni extrém nagy dózisteljesítményű terekben. A virtuális detektor az alkarra is rögzíthető, és ekkor mindkét kéz szabaddá válik (10. ábra).

9. ábra: Az imitált besugárzó berendezésből kivezérelt virtuális forrás, virtuális dózisteljesítmény mérése, 50 cm vastag műtrágya mögött, [saját szerkesztés]

10. ábra: A virtuális dózisteljesítménymérő alkarra szerelve, így mindkét két szabad marad, ami megkönnyíti az árnyékolás mögötti beavatkozást, [saját szerkesztés]

A virtuális sugárforrás-detektor rendszer működése, felprogramozása:

A virtuális sugárforrás rendszere mikrohullámokat használ és távolság meghatározás elvén működő készülékeken alapul (adó-vevő). Az adó maga a virtuális forrás, a vevő pedig a virtuális dózisteljesítmény mérő készülék. Az adó és vevő az egymáshoz képesti viszonyított távolságot folyamatosan méri és az adatokat a számítógépre továbbítja. Ennek segítségével az általunk fejlesztett program kiszámítja egy kiválasztott nuklid dózisteljesítményét a távolság függvényében az alábbi egyenlet alapján:

$$\dot{D} = k_\gamma \cdot A / r^2 \qquad (1)$$

ahol:

- Ḋ [µSv/h]: aktuális dózisteljesítmény „r” távolságban – program által kiszámított érték,
- A [TBq]: a virtuális radioaktív sugárforrás aktuális napi aktivitása – felhasználó által megadott érték,

- r [m]: a forrás és a detektor közötti távolság – mért érték,
- k_γ [µSv/h·m^2/TBq]: dózis állandó, vagy dózis konverziós tényező, izotóp függő - felhasználó által megadott érték [6].

Tehát az operátor adja meg az aktivitást és az izotóp típusát, így az „A" és a „k_γ" ismert, a távolság pedig a virtuális rendszer által mért adat. Az általunk fejlesztett algoritmus a fenti egyenletet használva, folyamatosan újra és újra számolja az aktuális dózisteljesítményt valós időben, a mért távolságok alapján.

Amennyiben nincs sugárforrás beprogramozva, akkor a rendszer automatikusan a természetes háttér értéket mutatja, azaz 0,1 µSv/h körüli értékeket.

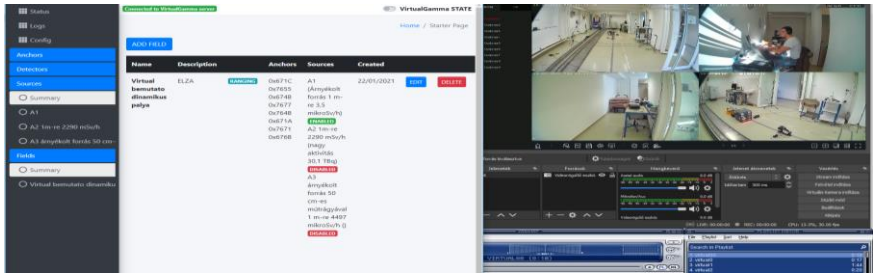
Az 1 m-ről mérhető 3,5 µSv/h dózisteljesítmény a számolások szerint 46,3 MBq aktivitású ^{137}Cs forrásnak felelne meg (ekkora valódi forrás volt elhelyezve az imitált besugárzó készülékben). Azaz az operátor a természetes háttér értéket követően a virtuális sugárforrás rendszerben beállítja a ^{137}Cs aktivitást A_1= 46,3 MBq-re, így a virtuális detektor kijelzője pont akkor dózisteljesítményt fog mutatni, mintha egy 46,3 MBq-es ^{137}Cs forrás lenne elhelyezve az imitált besugárzó készülékben. A valós detektor is pont ennyit mér, valamint a valós izotópazonosító készülék is ^{137}Cs -et jelez. Ez azért van, mint említettük, mert egy valódi 46,3 MBq napi aktivitású ^{137}Cs forrás is el volt elhelyezve az imitált besugárzó készülékben. A 46,3 MBq-es forrás imitálja az árnyékolt 30,1 TBq forrás dózisteljesítmény terét az imitált besugárzó berendezéstől 1 m távolságban.

Amikor a virtuális radioaktív sugárforrás kivezérlésre kerül, akkor az operátor átállítja az aktivitást a műbizonylaton szereplő napi aktuális aktivitás értékre, azaz A_2= 30,1 TBq-re. Ekkor a valódi dózisteljesítmény mérő nem fog többletet jelezni, de a virtuális dózisteljesítmény mérő „mért" értéke a 7. ábra alapján 2452 mSv/h.

50 cm vastag műtrágya árnyékolást használva az 1 m-ről a virtuális rendszerrel mérhető dózisteljesítmény „mért" értéke 4426 µSv/h (9. ábra). Ez megfelel A_3= 59 095 MBq ^{137}Cs forrásnak, azaz az operátor ekkor átállítja az aktivitás értékét A_3-ra.

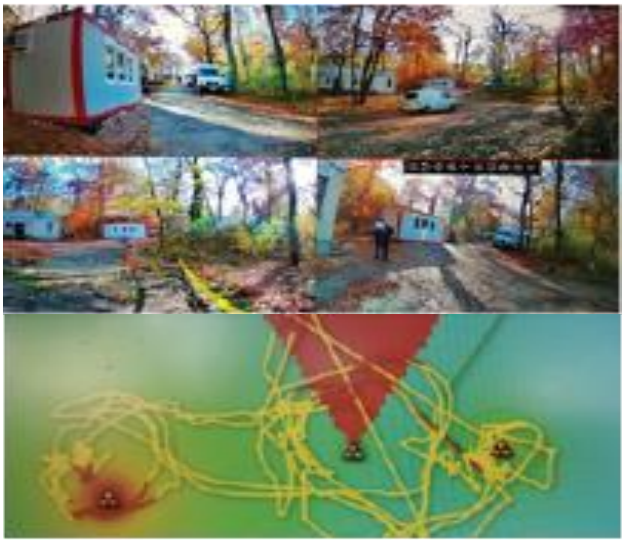
Miután a kivezérlés hibáját a felhasználó megszünteti és a virtuális radioaktív forrás visszament a helyére az operátor újra megváltoztatja az aktivitást a kezdeti állapotra, azaz A_4=A_1= 46,3 MBq. Így 1 m távolságból mind a valódi, mind a virtuális dózisteljesítmény mérő ugyanúgy 3,5 µSv/h értéket fog jelezni, ami megegyezik a használt valódi sugárforrás adataival.

Tehát a virtuális forrás rendszer operátorának annyi a dolga, hogy néhányszor a megfelelő időben megváltoztatja a virtuális sugárforrás aktivitás értékeit, valamint irányítja a készülék fényeit és hangjait. Az operátor a megfelelő időben ki, illetve visszavezérli a virtuális radioaktív forrást, mindezt teljes diszkrécióban megteheti, mivel egy másik szobában videokamerás megfigyeléssel követi nyomon a műveleti terület eseményeit (11. ábra). A megfelelő időzítéssel így elérhető, hogy a felhasználó abszolút valóságos szituációként élje meg az adott szcenáriót. A videofelvétel kiértékelésével láthatóvá válnak a felhasználó hibázási pontjai, vagyis, hogy mikor, hol vétett hibát, esetleg mely intézkedéseket hozott meg későn, vagy nem teljesen megfelelően hajtotta végre a feladatot. Ez pedig jelentősen hozzájárulhat a felhasználó tapasztalatának, gyakorlatának bővítéséhez.



11. ábra: A szcenárió megfigyelő és operátor állomása, valamint a virtuális forrás irányító konzolja, ahol a forrásokat tulajdonságait előre definiálják, [saját szerkesztés]

A HUN-REN EK SBL tanpályáinak megvalósításakor kifejlesztésre került a virtuális sugárforrás felderítő rendszer vizualizálása, mely során a virtuális sugárforrás dózistérképe megjeleníthető az operátor-felhasználó számára. Az SBL-en kifejlesztett virtuális felderítő rendszer segítségével a felderítő (személy vagy UGV robot) virtuális sugárforrást keresve ténylegesen végig tud menni a tanpályán a virtuális dózisteljesítmény mérő készülékkel. A rendszer a detektor által kijelzett értékek mellett egy személyi útvonalat jelző „térképet" is generál, amelyben látható a bejárt útvonalon kapott virtuális dózisteljesítmény értékek, (12. a., b. ábra). Ezen felül rendelkezésre áll egy virtuális dózisteljesítmény térkép mód is, ahol a teljes szcenárió terület virtuális dózisteljesítmény viszonyai is megjeleníthetőek. Ezen extra funkciók kivetíthetőek a felderítő mobil telefonjára vagy akár egy okosszemüvegre is. A tanpályán rendelkezésre áll négy db HD kamera, illetve a személyi testkamera felvételeit és a virtuális rendszer adatait is szinkronban lehet megtekinteni egy központi kijelzőn. Ennek segítségével lehet elemezni, értékelni és fejleszteni az egyes bevetéseket, beavatkozásokat a virtuális rendszerrel végzett valós felderítést követően. Ez a módszer nagyban hozzájárulhat az egyes beavatkozó egységek, sugárforrás felderítők, sugárvédelmi megbízottak, sugárvédelmi megbízott helyettesek képzéséhez.



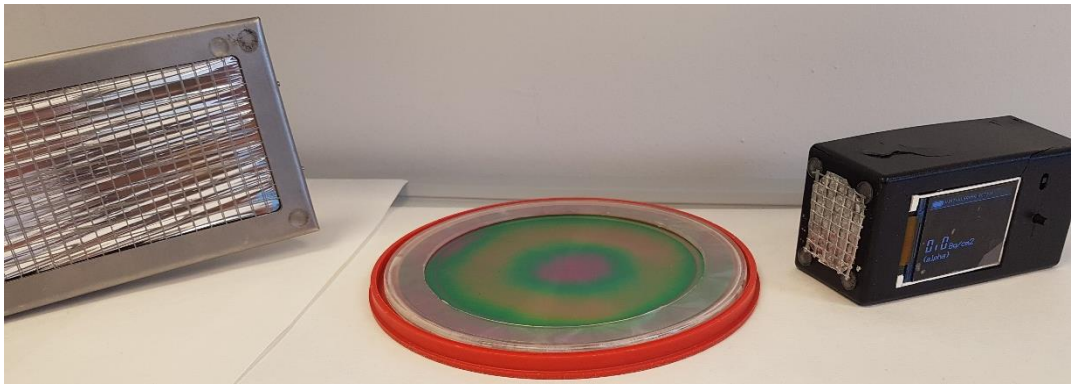
12. a, b, ábra: A tanpálya (bal ábra), a tanpálya személyi útvonal monitoring megjelenítése és vizualizálása (jobb ábra) a virtuális sugárforrás felderítő rendszerrel, [saját szerkesztés]

A VIRTUÁLIS RADIOAKTÍV FELÜLETI SZENNYEZETTSÉG ÉS VIRTUÁLIS FELÜLETI SZENNYEZETTSÉG MÉRŐ

A virtuális gamma sugárzó forrással és a virtuális dózisteljesítmény mérővel valósághűen demonstrálható egy gamma sugárzó radioaktív anyag dózisteljesítmény és felületi szennyezettség mérése. Az alfa sugárzók felületi szennyezettség mérési karakterisztikája ettől egészen eltérő. Utóbbi sugárzás csak közvetlen közelről mérhető, ugyanakkor a szennyezés szinte minden esetben kiterjedt.

A virtuális radioaktív szennyezettség mérőnek és virtuális radioaktív szennyezésnek az alábbi tulajdonságokkal kell rendelkeznie:

- A virtuális felületi szennyezettség mérőnek külső megjelenését tekintve hasonlítania kell az igazi felületi szennyezettség mérőhöz (13. ábra jobb-bal oldali készülék mérő ablaka).
- A mérési karakterisztikának valósághűnek kell lennie, azaz csak közvetlen közelről szabad a rendszernek bejeleznie.
- A virtuális szennyezés a valós szennyezéshez hasonlóan kiterjedt felületű, melynek szélén a felületi szennyezettség értéke minimális, míg a közepén maximális.
- A rendszernek mérnie kell a dekontaminálás hatását.

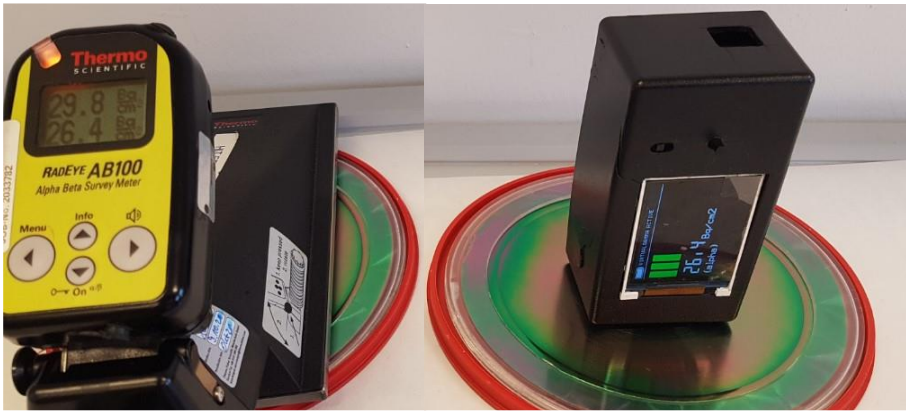


13. ábra: Thermo AB-100 valódi felületi szennyezettség mérő (bal), valamint a virtuális szennyezettség mérő mérőfeje (jobb), középen látható az etalon ^{239}Pu sugárforrás, [saját szerkesztés]

Virtuális felületi szennyezettség és szennyezettség mérő bemutatása, a virtuális szennyezés a felhasználó-gyakorlatozó szemszögéből

A gyakorlatlan felhasználó a valós és virtuális felületi szennyezettség mérő között a készülék küllemét és működését tekintve elvileg nem tud különbséget tenni. A készülék a felületi szennyezettség értékeket [Bq/cm^2]-ben jeleníti meg. A programozható felületen be lehet állítani a felületi szennyezettség maximális értékét, illetve a felületi szennyezettség kiterjedését. Továbbá a háttér értéket és a dekontaminálás utáni értékeket is definiálni lehet. Az operátor on-line figyelheti a virtuális szennyezettség mérő készülék által mért értékeket és a megfelelő pillanatban a különféle felületi szennyezettségi szintek között tud váltani. Tehát az adott folyamathoz a megfelelő érték beprogramozható pár másodperces átállási idővel. Az alábbi ábrákon (14.-15. ábra) ugyanazon etalon ^{239}Pu forrás mérése során a valódi és a virtuális felületi szennyezettség mérő látható.

14. ábra: Thermo AB-100 valódi felületi szennyezettség mérő (alsó érték a kijelzőn) és a virtuális felületi szennyezettség mérő alfa háttér mérése (valós mérőeszköznél a kijelzőn az alsó érték az alfa szennyezettség) (0,00 Bq/cm^2) a ^{239}Pu etalon sugárforrások mellett, [saját szerkesztés]



15. ábra: A valós (bal oldali ábra)) vs. virtuális felületi szennyezettség mérő (jobb oldali ábra) „mért" alfa felületi szennyezettség értéke (valós mérőeszköznél az alsó érték) a második etalon forrás esetén, mindkét esetben 26,4 Bq/cm^2, [saját szerkesztés]

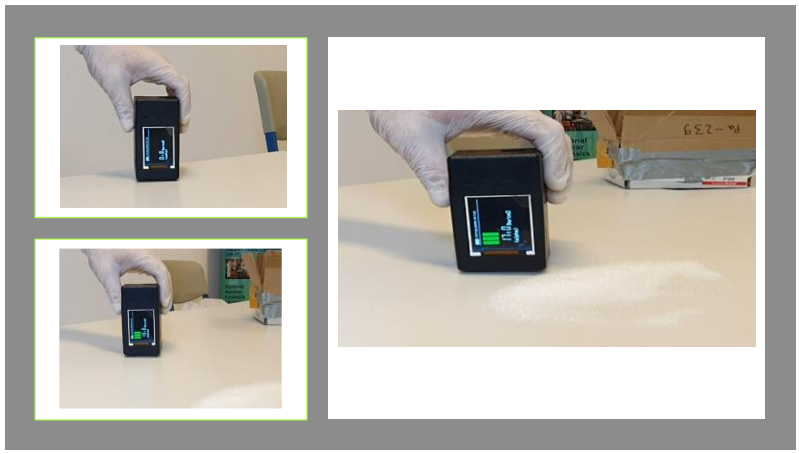
Amennyiben az alfa sugárzó ^{239}Pu etalon sugárforrást letakarjuk, a valós műszer is a háttér értéket mutatja (16. ábra):

16. ábra: A valós (bal) vs. virtuális (jobb) felületi szennyezettség mérő „mért" alfa felületi szennyezettség értéke (valós mérőeszköznél az alsó kijelzett érték az alfa szennyezettség) a letakart etalon forrás esetén, mindkét esetben 0,00 Bq/cm^2, [saját szerkesztés]

A VIRTUÁLIS FELÜLETI SZENNYEZETTSÉG MÉRŐ BEMUTATÁSA EGY SZCENÁRIÓN KERESZTÜL

A bemutatott szcenárióban egy radioaktív sugárzást mérő detektor bejelez az egyik sugárkapunál. Ezután a talált forrást a 490/2015. (XII. 30.) rendelet alapján vizsgálatra elszállítják egy laboratóriumba [7]. A gyanús csomag kicsomagolásakor egy ampulla az asztalra esik és eltörik, a benne lévő anyag kiszóródik az asztal felületére.

Első lépésként felületi szennyezettség mérővel háttér mérést kell végezni, majd az asztalt kell szisztematikusan végig mérni. Amennyiben észlelhető felületi szennyezettség, nagyságát és kiterjedését is meg kell határozni (17. ábra).



17. ábra: A virtuális felületi szennyezettség mérővel háttér „mérése" (bal oldali felső ábra), szennyezés keresése (bal oldali alsó ábra), kiterjedés meghatározása (jobb oldali ábra), [saját szerkesztés]

Amennyiben a mért értékek meghaladják a beavatkozási szintet, meg kell kezdeni a dekontaminálást. A dekontaminálás hatásfoka az alábbi egyenlet alapján számolható *[4]*:

$$E=100 \cdot (A_k/A_0) \qquad (2)$$

ahol:

- E: a dekontamináció hatásfoka [%],
- A_k: aktivitás koncentráció értéke a felület tisztítás után [Bq/cm^2],
- A_0: aktivitás koncentráció értéke a felület tisztítása előtt [Bq/cm^2].

A dekontamináció hatásfoka a felület érdességétől, nedvszívó képességétől, a szennyező anyag fizikai-kémiai formájától, valamint a dekontamináló szertől és a dekontaminálás technikájától függ. A hatásfok a felület többszöri tisztítása esetén egyre csökken. A dekontaminálási fázisokat követően két állapot állhat fenn:

- A szennyezést sikerült zéró szintre csökkenteni.
- A felületről a maradék szennyezés az adott dekontamináló technológiával nem eltávolítható.

A 18. ábrán az egyes tisztítási folyamatokat követően a virtuális felületi szennyezettség érték csökkenését mutatjuk be. A felület dekontaminálásakor a nem fixált felületi szennyezettség jellemzően exponenciális jellegűen csökkeni kezd. A virtuális rendszert exponenciális felületi szennyezettség csökkenésre állítottuk be.

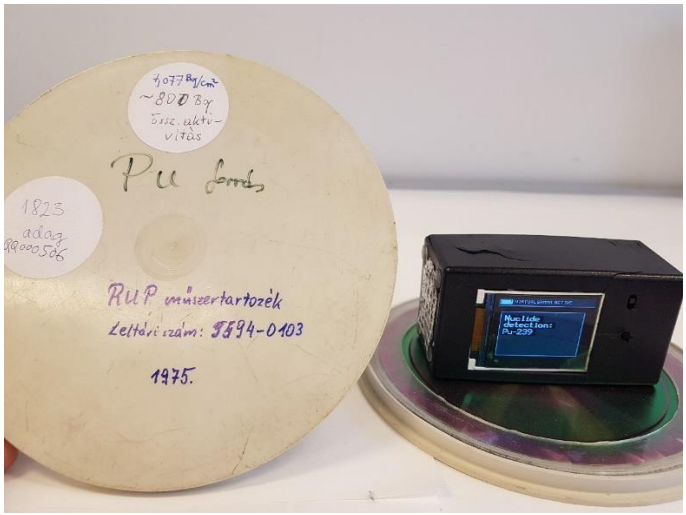
18. ábra: A „mért” virtuális felületi szennyezettség értékek csökkenése a dekontaminálási fázisokat követően, [saját szerkesztés]

A sorozatos dekontaminálást követően a szennyezettség értékre egyre lassabban kezd csökkenni, majd megáll. Ennél a pontnál az összes nem fixált szennyeződést sikerült eltávolítani. A fixált szennyezés az adott dekontaminálási technikával nem jön le a felületről, így annak értéke állandó. Ugyanakkor az alfa sugárzó anyag letakarásával elérhető a mért felületi szennyezettség zéró értéke, mivel az alfa sugárzás áthatólóképessége minimális (1. ábra). A 19. ábrán látható a fixált „alfa szennyezés” letakarásának a hatása a virtuális rendszerrel „mérhető” felületi szennyezettség értékekre.

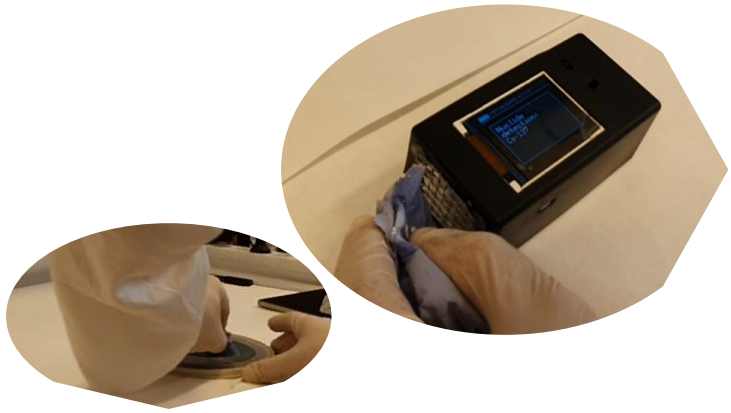
19. ábra: A virtuális fixált felületi alfa szennyezettség letakarása, [saját szerkesztés]

A VIRTUÁLIS RENDSZER IZOTÓP AZONOSÍTÓ ÜZEMMÓDJA

Az elveszett radioaktív sugárforrás keresési gyakorlatoknál a felderítők a forrás lokalizálása után izotóp azonosító készüléket használnak, mely segítségével a megtalált forrás izotóp összetételét határozzák meg. Amennyiben a virtuális rendszerrel izotóp azonosító készüléket imitálunk, akkor a készülék kijelzőjén a szcenárióban szereplő nuklid neve megjeleníthető, és a zártságvizsgálat alkalmával vett dörzsmintavételezésnél a dörzsminta „nuklid azonosítása" is elvégezhető (20.-21. ábra).



20. ábra: A virtuális izotóp azonosító üzemmódban a készülék a forráson lévő felirattal megegyezően ^{239}Pu-et „érzékel", [saját szerkesztés]



21. ábra: A virtuális izotóp azonosító üzemmódban a készülék a zártságvizsgálatkor vett dörzsminta nuklid „azonosítására” is alkalmas, [saját szerkesztés]

A szcenárióban a ^{239}Pu forrásról vett dörzsminta „nuklid azonosítása” alapján megállapítható, hogy a ^{239}Pu forrás felülete ^{137}Cs-el szennyezett. Ez alapján a ^{239}Pu forrás zártnak tekinthető, mivel a dörzsminta nem mutatott ki ^{239}Pu-et. Ugyanakkor a ^{137}Cs jelenléte szerint valószínűsíthető, hogy a ^{239}Pu forrás felülete ^{137}Cs-el szennyeződött, mivel tárolóban a ^{239}Pu forrás melletti ^{137}Cs forrás valószínűleg nyílttá vált.

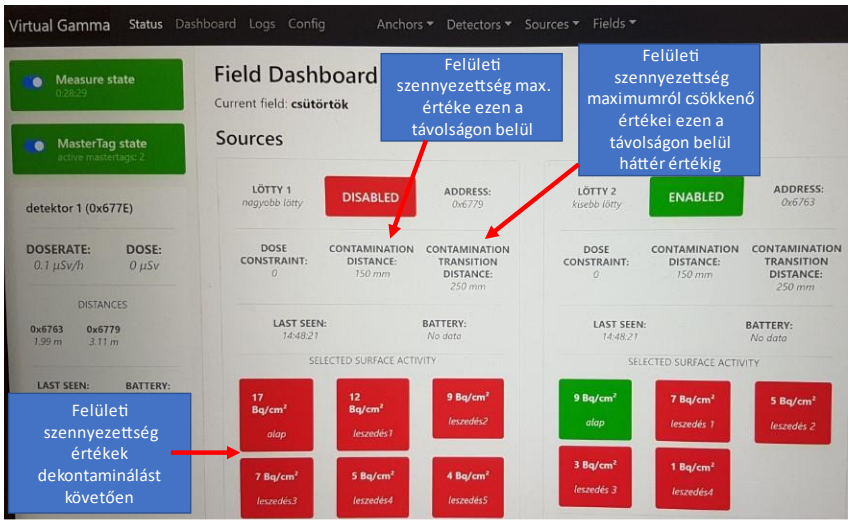
A VIRTUÁLIS FELÜLETI SZENNYEZETTSÉG MÉRŐ FELÉPÍTÉSE, PROGRAMOZÁSA

A virtuális felületi szennyezettség egy elektronikus adó, míg a virtuális felületi szennyezettség mérő egy elektronikus vevő egység. Az adó-vevő valós időben érzékeli az egymástól való távolságot és ezen értékeket másodpercenként folyamatosan frissíti és elküldi a rendszerhez tartozó számítógép részére. A bejövő mért adatokat a számítógépen futó program fogadja és a felprogramozott rendszer által számított értékeket jeleníti meg a vevő (virtuális felületi szennyezettség mérő) kijelző egységén. Jelen esetben a mértékegységet [Bq/cm^2]-ben adja meg. A program platformja interneten elérhető, így a rendszert akár mobiltelefonnal és egyéb okos eszközökkel is lehet programozni és irányítani. A virtuális felületi szennyezettség mérő üzemmódban három fő érték adható meg:

- (I.) Távolság, melyen belül a virtuális felületi szennyezettség mérő bejelez és maximum értéket mutat (pl. egy elcseppenő szennyezés centruma).
- (II.) A teljes szennyezés kiterjedését megadó kiterjedés paramétere.
- (III.) A harmadik érték maga a felületi szennyezettség értéke, melyet szeretnénk mérni, amennyiben a felületi szennyezettség mérő bizonyos távolságon belül kerül az adóhoz képest. Itt több értéket is meg lehet határozni: például kezdeti szennyezettség értéket, majd több csökkenő értéket is.

Egy valós szennyezés felületi szennyezettség koncentrációja általában nem egyenletes, a centrumtól távolodva csökken. Ezen funkció ezt is képes imitálni. Ha ezen a távolságon túl mérünk, akkor a készülék 0-t jelez, azaz itt már nincs szennyezettség. Így a virtuális felületi szennyezettség mérővel többszöri méréssel ki lehet mérni a felületi szennyezettség határát.

Az operátornak az egyes dekontaminálási fázisokat követően ezen előzetesen beprogramozott értékeket kell beállítania. Az átállás időigénye általában pár másodperc. Az operátor videokamera rendszeren keresztül követheti a beavatkozók aktuális munkáját és ezen információk alapján beállíthatja a szcenárió adott idejéhez köthető felületi szennyezettség értékeket. Ha szükséges, a helyszínen is tartózkodhat, és a mérendő felületi szenynyezettség értékeket az okos telefonon keresztül is valós időben állítgathatja. A rendszer a pillanatnyi távolság alapján automatikusan kiszámítja a 0-maximum közötti felületi szennyezettség értékeket (22. ábra).



22. ábra: A virtuális felületi szennyezés és szennyezettség mérő programozása, [saját szerkesztés]

ÖSSZEFOGLALÓ

Az SBL által kialakított tanpályákon maximum 4.-5. kategóriájú radioaktív sugárforrások alkalmazása engedélyezett. Árnyékolatlan, nagy aktivitású forrással és emiatt igen nagy dózisteljesítményű terekben nem szabad sugárforrás felderítési gyakorlatokat tartani. Ugyanakkor speciális esetekben (pl. baleset, szabotázs, működési hiba, talált forrás) előfordulhat, hogy egy nagy aktivitású sugárforrás kikerül az árnyékolás mögül és igen nagy dózisteret hoz létre. A beavatkozókat biztonságos környezetben ezen ritka, de veszélyes esetekre kell felkészíteni.

A kifejlesztett virtuális radioaktív forrás, virtuális dózisteljesítmény mérő rendszer segítségével igen nagy aktivitású és dózisterű radioaktív sugárforrásokat tudunk imitálni valósághűen. A virtuális rendszerrel a viszonylag ritkán előforduló, ugyanakkor igen veszélyes helyzeteket lehet begyakorolni, mely hozzájárul az ionizáló sugárzás elleni védelem magasabb szintű eléréshez ezen speciális esetekben is. Ilyen rendkívüli eseményeknél nagyon rövid idő alatt lehet jelentős dózisterhelést elszenvedni, ezért fontos begyakorolni a megfelelő lépéseket és a gyors reagálást.

A felületi szennyezettség meghatározása számos szituációban szükséges lehet. Az alfa sugárzó izotópok felderítésének bonyolultságát a magyarázaton és bemutatáson kívül a valós tapasztalat megszerzésével lehet a legjobban érzékeltetni. A valós felületi szennyezettséggel történő gyakorlat végzése sugárszennyezés és inkorporáció (lenyelés, belégzés)

jelentős kockázatával járhat. A kezdő gyakorlatozók még nem rendelkeznek megfelelő rutinnal, ezért számukra a felületi szennyezettség mentesítése, vagyis a dekontamináció különösen kockázatos.

A virtuális rendszer abszolút biztonságos, bárhol alkalmazható és a felületi szennyezettség mérésének lehetőségével egy teljes sugárforrás felderítési szcenárió méréstechnikai imitálása megvalósítható teljesen valósághűen, sugárvédelmi következmények nélkül. A virtuális rendszer az elsődleges reagáló, vagy elhárító szervek munkájában segítséget nyújthat a biztonságos felkészülésben. A virtuális rendszer segítségével kiképzett felderítők, a megszerzett rutin által, a későbbiekben nagyobb biztonsággal képesek kezelni egy valós esetet, ahol adott helyszínen radioaktív szennyezettség észlelhető.

FELHASZNÁLT IRODALOM

[1] 190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről *https://net.jogtar.hu/jogszabaly?docid=a1100190.kor* (2022.06.07.)

[2] https://rhk.hu/sugarvedelem (2022.06.07.)

[3] Prof. Dr. Rajnai Zoltán: Kritikus (Információs) Infrastruktúrák Összetétele, Biztonsági kérdései, előadás 2020.

[4] 2/2022. (IV. 29.) OAH rendelet az ionizáló sugárzás elleni védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről, https://net.jogtar.hu/jogszabaly?docid=A2200002.OAH&txtreferer=00000001.txt (2022.07.11.)

[5] http://www.radprocalculator.com/Gamma.aspx (2022.07.11.)

[6] Bodor Károly, Dr. Völgyesi Péter, Dr. Kovács András: Segédlet készítése az Országos Nukleáris Védettségi Intézkedési Terv mellékleteihez, OAH-MMT pályázat, 2020.11.10.

[7] 490/2015. (XII. 30.) Korm. rendelet a hiányzó, a talált, valamint a lefoglalt nukleáris és más radioaktív anyagokkal kapcsolatos bejelentésekről és intézkedésekről, továbbá a nukleáris és más radioaktív anyagokkal kapcsolatos egyéb bejelentést követő intézkedésekről, https://net.jogtar.hu/jogszabaly?docid=a1500490.kor (2022.06.07.)

OCCUPATIONAL HEALTH AND SAFETY REGULATIONS OF THE NATIONAL TAX AND CUSTOMS ADMINISTRATION

A NEMZETI ADÓ ÉS VÁMHIVATAL MUNKAVÉDELMI JOGI SZABÁLYOZÁSA[1]

OPOR Csaba Barnabás[2]

Abstract

The current occupational safety law in our country has been in effect since January 1, 1994. However, the customs guards belonging to the state tax and customs authority have been present in various service relationships and organizational forms over the past 150 years. Since the establishment of the National Tax and Customs Administration in 2011 and the creation of tax and customs service relationships in 2021, the legal provisions contain several different regulations, references, and authorizations compared to the Occupational Safety Law. However, there has not been adequate legislative background established for these. Currently, there are no distinct provisions regarding customs guards in the occupational safety law. It would be necessary to conduct a legal overview regarding the National Tax and Customs Administration, highlighting the differences and making specific legislative proposals for the missing legal regulations to ensure that the occupational safety requirements for customs guards are clear and fully enforceable.

Keywords

National Tax and Customs Administration, customs guard, service obligations, presentation of the current regulatory situation, legislative proposals

Absztrakt

Hazánk jelenleg érvényben lévő munkavédelmi törvénye[1] 1994. január 1. óta hatályos, ugyanakkor az állami adó- és vámhatósági testület állományába tartozó pénzügyőrök a szervezet elmúlt 150 éves történetében több szolgálati jogviszonyban és több szervezeti formában voltak jelen. A Nemzeti Adó- és Vámhivatal 2011-es megalakulása és az adó és vámhatósági szolgálati viszony 2021-es létrehozása óta a jogszabályi rendelkezések a Munkavédelmi törvényhez képest több eltérő szabályozást, utalást, felhatalmazást tartalmaznak, amikhez nem született meg a megfelelő jogszabályi háttér. Jelenleg a munkavédelmi törvényben nincsenek eltérő rendelkezések a pénzügyőrök tekintetében. Szükségszerű lenne egy jogi áttekintés a Nemzeti Adó- és Vámhivatal tekintetében, rávilágítva az eltérésekre, valamint konkrét jogszabályi javaslatokat tenni a hiányzó jogi szabályozásokra, hogy a pénzügyőrökre vonatkozó munkavédelmi előírások egyértelműek és teljes mértékben alkalmazhatóak is legyenek.

Kulcsszavak

NAV, pénzügyőrség, szolgálati kötelmek, jelenlegi szabályozási helyzet bemutatása, jogalkotási javaslatok

[1] Jelen tanulmány a szerző „A Nemzeti Adó- és Vámhivatal munkavédelmi jogi szabályozása” című szakdolgozata (Óbudai Egyetem BGK Munkavédelmi szakmérnök szak; védés: 2024. 01. 31.; konzulens: Dr. Lesfalvi Tibor PhD) alapján készült.

[2] csabaopor@gmail.com | ORCID: 0009-0009-9967-2598 | Occupational Health and Safety (OHS) and Fire Safety Manager, ANY Security Printing Company | munka- és tűzvédelmi vezető, ANY Biztonsági Nyomda

BEVEZETÉS

Magyarországon az állami adóhatósági és vámhatósági feladatokat jelenleg a 2010. évi CXXII. törvény[2] által létrehozott Nemzeti Adó- és Vámhivatal (továbbiakban: NAV) látja el. A 2011. január 1-én hatályba lépő törvény a köztisztviselők jogállásáról szóló 1992. évi XXIII. törvény[3] hatálya alá tartozó Adó- és Pénzügyi Ellenőrzési Hivatalt (továbbiakban: APEH), akik az addigi adóhatósági feladatokat látták el, és a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló 1996. évi XLIII. törvény[4] hatálya alá tartozó, túlnyomó részt pénzügyőrökből álló Vám- és Pénzügyőrséget (VPOP) olvasztotta össze. A Vám- és Pénzügyőrség fő tevékenysége a vámhatósági feladatokon túl a bűnmegelőzés, bűnüldözés és rendészeti feladatok ellátása volt.

A munkavédelemről szóló 1993. évi XCIII. törvény egyes rendelkezéseinek végrehajtásáról szóló 5/1993. (XII. 26.) MüM rendelet[5] (továbbiakban Vhr.) 2. számú melléklete szerint III. veszélyességi osztály és a több mint 1000 fő munkavállaló alapján egy fő felsőfokú munkavédelmi szakképesítésű alkalmazott szükséges teljes munkaidővel a feladatok ellátására . A NAV létszáma 18000 fő körül mozog.

A 2022. augusztus 6-án megjelent 2023. július 15-től hatályos NAV Szervezeti és Működési Szabályzatról szóló 5/2022 (VIII.5.) PM utasítás[6] (továbbiakban SZMSZ) alapján a NAV Központi Irányítása (továbbiakban KI) az SZMSZ 24. § bekezdés h) pontja szerint a központi szerv, ahol az erőforrás-gazdálkodási elnökhelyettes közvetlenül irányítja a munka- és tűzvédelmi feladatok ellátását. Ugyanakkor a NAV Gazdasági Ellátó Igazgatóság (továbbiakban GEI), szervezeti ábrája tartalmaz Humánpolitikai és Munkavédelmi Főosztályt, de az SZMSZ feladatot nem határoz meg ezzel kapcsolatban.

Érdemes ennek okán visszanyúlni és a kezdetektől röviden áttekinteni az SZMSZ-ek alakulását és időrendben megvizsgálni a változásokat. A NAV honlapján[7] az első hatályos SZMSZ 2011. június 30-tól érhető el. A kezdetektől az erőforrás-gazdálkodási elnökhelyettes irányítja közvetlenül a szaktevékenységet. 2013-ban a NAV Bűnügyi Főigazgatóság külön álló referenst kap, a szervezeti ábra alapján, ami később el is tűnik. 2016-ban több változás is történt, a szaktevékenység közvetlen irányítása a KI főigazgatóhoz kerül és megalakul a GEI, aminek feladata többek között a központi és területi szervek működésével összefüggő feladatok ellátása. 2019-től már csak operatív irányítást gyakorol újra az elnökhelyettes, az elvi irányítási feladatot a gazdasági és humánigazgatási ügyekért felelős szakfőigazgató kapja, valamint megjelenik a GEI-n belül a Humánpolitikai és Munkavédelmi Főosztály, azon belül a Munkavédelmi Osztály. 2020 nyarán a KI főigazgatójához visszakerül ismét a közvetlen irányítás.

2021. augusztus 20-ai hatállyal módosul a Nemzeti Adó- és Vámhivatal szerveinek hatásköréről és illetékességéről szóló 485/2015. (XII. 29.) Kormány rendelet[8], mely meghatározza a GEI vonatkozásában, hogy a NAV operatív gazdálkodási feladatainak megvalósítása keretében, üzemeltetési és ellátási feladatainak végrehajtásával támogassa a központi és területi szervek működését, így ezen feladatokat a 2021. szeptember 19-ei SZMSZ már nem tartalmazza.

2022. augusztus 6-tól a NAV vezetője az elnök lesz és ismét a már említett erőforrás-gazdálkodási elnökhelyetteshez kerül vissza az irányítás.

Érdekesség, hogy a Közbeszerzési és Ellátási Főigazgatóságról szóló 250/2014. (X. 2.) Kormány rendelet[9] már a 2021. december 24-i módosításával előírja a Közbeszerzési és Ellátási Főigazgatóság (továbbiakban: KEF) részére, hogy a NAV csak akkor láthatja el

az üzemeltetési (munkavédelmi feladatokat is) és ellátási feladatait, ha a KEF azt nem tudja vállalni. Így a 485/2015. (XII. 29.) Kormány rendelet és a 250/2014. (X. 2.) Kormány rendelet két különböző rendelkezést hoz.

2015. december 1-én az egyes törvényeknek a Nemzeti Adó- és Vámhivatal átalakításával, valamint a költségvetési tervezéssel és gazdálkodással kapcsolatos módosításáról szóló 2015. évi CXCI. törvény[10] elfogadásával a NAV Bűnügyi Főigazgatóság (továbbiakban BF) gazdálkodási önállóságát megszüntette, beolvadt a NAV-ba, mint központi szerv.

A NAV a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény[11] alapján központi államigazgatási szerv, de szintén ezen jogszabály alapján nem rendvédelmi szerv.

A Nemzeti Adó- és Vámhivatalról szóló 2010. évi CXXII. törvény (továbbiakban NAV TV) első bekezdése szerint „a NAV államigazgatási és fegyveres rendvédelmi feladatokat ellátó, …, központi hivatalként működő központi költségvetési szerv.”.

A közigazgatási átalakítások és a bérrendezéseket célzó jogszabályi változások következtében, minden szakág külön szolgálati jogviszonyformát kapott, az addigi általános közalkalmazotti és köztisztviselői besorolások helyett. Így a 2021. január 1-én hatályba lépő a Nemzeti Adó- és Vámhivatal személyi állományának jogállásáról szóló 2020. évi CXXX. törvény[12] (továbbiakban: NAV SZJTV), az addig a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló 2015. évi XLII. törvény[13] (továbbiakban: HSZT) alapján, a pénzügyőrök hivatásos szolgálati jogviszonyban voltak, most külön pénzügyőri státuszba kerültek, valamint a közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény[14] hatálya alá tartozó köztisztviselők, az adó- és vámhatósági szolgálati jogviszonyon belül, tisztviselői státuszba kerültek.

A JELENLEGI JOGI HELYZET ÉS HIÁNYOSSÁGOK BEMUTÁSA

Munkavédelmi törvény vonatkozó előírásai

A Munkavédelemi törvény 87. § 9. pontja alapján az adó- és vámhatósági szolgálati jogviszony szervezett munkavégzésnek minősül.

A Munkavédelmi törvény 9. § (3) bekezdése szerint rendkívüli munkavégzési körülmények (pl. mentési, katasztrófaelhárítási tevékenységek) esetére, illetve a Nemzeti Adó- és Vámhivatalnál pénzügyőri munkakörben kifejtett munkatevékenységre, a miniszter által kiadott külön jogszabály kivételesen indokolt esetben eltérő követelményeket állapíthat meg az egészséget nem veszélyeztető és biztonságos munkavégzésre vonatkozóan.

A rendkívüli munkavégzéssel kapcsolatban a NAV TV semmit, a NAV SZJTV 105. §-a kizárólag a munkaidővel és túlmunkával kapcsolatos eljárásokat határozza meg.

A pénzügyőri intézkedések és a kényszerítő eszközök alkalmazásáról, valamint az elfogott, előállított, őrizetbe vett és fogva tartott személyek őrzésének és kísérésének eljárási szabályairól szóló 20/2018. (XII. 21.) PM rendelet[15] 2. §. h) pontja leírja a rendkívüli eseményeket, miszerint:

„az intézkedés során bekövetkező minden olyan esemény, tevékenység vagy mulasztás, amely az intézkedés alá vont, az intézkedést végrehajtó vagy más személy életét,

testi épségét, egészségét, anyagi javait, a személyi szabadság korlátozása helyének rendjét vagy az őrzésbiztonságot sérti vagy veszélyezteti;"

Összehasonlításként figyelemre méltó, hogy az igazságügyi alkalmazottak szolgálati jogviszonyáról szóló 1997. évi LXVIII. törvény[16] részletesen kitér a rendkívüli munkavégzés feltételeire:

„45. § (1) Az igazságügyi alkalmazott rendkívüli esetben a munkaidejét meghaladóan is munkára kötelezhető, illetve köteles ügyeletet vagy készenlétet ellátni. A munkaidőbeosztástól eltérő, a munkaidőkereten felüli, illetve a készenlét, ügyelet alatt elrendelt munkavégzés rendkívüli munkavégzésnek minősül.

(2) Az (1) bekezdéstől eltérően rendkívüli munkavégzés munkaszüneti napon csak baleset, elemi csapás vagy súlyos kár megelőzése, illetőleg elhárítása, továbbá külön törvényben előírt feladat megvalósítása érdekében rendelhető el.

(3) A rendkívüli munkavégzés elrendelése nem veszélyeztetheti az igazságügyi alkalmazott testi épségét, egészségét, illetőleg nem jelenthet személyi, családi és egyéb körülményeire tekintettel aránytalan terhet.

(4) A rendkívüli munkavégzést az igazságügyi alkalmazott kérésére írásban kell elrendelni."

A Munkavédelmi törvény záró rendelkezéseiben 88. § (3) a) pontja alapján felhatalmazást kap a feladatkörében érintett miniszter, hogy:

„a rendkívüli munkavégzési körülmények esetére, illetőleg a rendvédelmi szervek, az önkormányzati tűzoltóságok tekintetében a munkavégzésre irányuló jogviszonyban, szolgálati viszonyban kifejtett munkatevékenységre vonatkozóan – az egyes szervek specifikumait figyelembe véve – ezen törvényben meghatározottaktól eltérő munkavédelmi követelményeket, eljárási szabályokat, tevékenységek veszélyességi osztályba sorolását, továbbá a balesetek, a foglalkozási megbetegedések és fokozott expozíciós esetek bejelentésére, kivizsgálására és minősítésére vonatkozó szabályokat ágazati rendeletben határozza meg;" .

Csakhogy a NAV nem rendvédelmi szerv, így amire a Munkavédelmi törvény 9. § lehetőséget ad, esetében a 88. § nem hatalmazza fel.

Véleményem szerint az, hogy a NAV részére nincs meghatározva külön, hogy mik a rendkívüli munkavégzésre vonatkozó szabályok, egyfelől lehet azért, mert a Munkavédelmi törvény erre nem ad felhatalmazást, de alapvetően a szervezet rendvédelmi mivoltából adódhat, mivel egy katasztrófahelyzetnél vagy veszélyhelyzetnél, a kormány amúgy is elrendeli a foglalkoztatottak munkavégzését.

A Munkavédelmi törvény 86. § alapján a munkavédelmi hatóság jogköre nem terjed ki többek között a rendvédelmi szervekre. A törvény előírja, hogy ezekre a szervek tekintetében külön jogszabályban rendelkezni kell, hogy ki látja el a hatósági feladatokat.

A munkavédelmi hatósági feladatokat ellátó egyes szervek kijelöléséről szóló 373/2011. (XII. 31.) Korm. rendelet[17] (továbbiakban: hatósági kormányrendelet) meg is állapítja a Belügyminisztérium irányítása alá tartozó szervek munkavédelmi hatóságait. Ezekre a szervek saját munkavédelmi szabályzata is hivatkozik, mint például a Büntetés-végrehajtási szervezet (továbbiakban BV) esetében a BV Munkavédelmi Szabályzatáról szóló 10/2020. (III. 31.) BVOP utasítás[18] 14. pontja alapján, súlyos munkabaleset esetén a Büntetés-végrehajtás Országos Parancsnoksága vonatkozásában az Országos Rendőrfőkapitány jár el.

Ez a NAV esetében szintén szükséges lenne, mivel sok olyan bűnügyi feladatokat ellátó munkakör van (MERKUR bevetési egység, fedett nyomozók), amelyek esetén nyomozást befolyásoló adatok vagy fedett munkakörben dolgozó személyes adatai kerülhetnek át, egyéb nem rendvédelmi hatósághoz.

Szolgálati kötelmekkel összefüggő balesetek és megbetegedések

A pénzügyőrök esetén a NAV SZJTV a Munkavédelmi törvénytől eltérően a 235. §-ban a munkabalesetek és foglalkozási megbetegedések helyett a szolgálati kötelmekkel összefüggő baleset és betegség fogalmat vezeti be, hasonlóan, mint más rendvédelmi szerveknél a belügyminiszter irányítása alá tartozó rendvédelmi szervek munkavédelmi feladatai, valamint foglalkozás-egészségügyi tevékenysége ellátásának szabályairól szóló 70/2011. (XII. 30.) BM rendelet[19] alapján (továbbiakban BM rendelet). Bár a NAV SZJTV rendelkezései között, mint fogalommeghatározás nem szerepel, hogy mi az a szolgálati kötelmek, de a BM rendelet meghatározása szerint: „a munkavédelemről szóló törvényben meghatározott munkabaleseten, illetve a 27/1996. (VIII. 28.) NM rendeletben[20] meghatározott foglalkozási megbetegedéseken túl az a baleset, illetve betegség, amely a hivatásos állomány tagját

a) azonnali szolgálatba, munkába rendelés esetén a rendelkező szóbeli vagy írásbeli parancs vagy utasítás vételétől számított időtől a szolgálatteljesítés, munkavégzés helyére történő megérkezéséig, valamint onnan lakóhelyére menet közben,

b) kiképzési terv, napirend szerint előírt gyakorlati foglalkozásokon, a fizikai állóképesség fenntartásával kapcsolatos szervezett sportfoglalkozásokon,

c) a rendvédelmi szervek tömegkapcsolatainak erősítése céljából a rendvédelmi szerv által szervezett sportversenyeken, speciális rendezvényeken, bemutatókon

érte, illetve azzal összefüggésben keletkezett vagy jelentősen súlyosbodott."

A NAV SZJTV úgy rendelkezik, hogy a külön jogszabályban leírt eljárás rend szerint szükséges az ilyen fajta balesetek és megbetegedések kivizsgálása.

Mivel ez speciális jogszabály, így a Vhr. munkabalesetekre vonatkozó részei (5. § (1) és 7. § (1)) helyett ezt kell alkalmazni baleset esetén és a NAV saját hatáskörben készíti a minősítő határozatot a munkavédelmi hatóságot ezáltal kihagyva, mivel a hatóság részére csak a munkabalesettel kapcsolatos dokumentumokat kell megküldeni, a szolgálati kötelmekkel kapcsolatos események nem tartoznak a munkavédelmi törvény alá.

Így viszont felmerül egy szabályozási probléma, hogy ha nem a munkavédelmi hatóság a hatóság, akkor nincs kinek megküldeni a baleseteket, illetve nincs, aki vizsgálja a súlyos vagy halálos baleseteket. Felmerül a kérdés, hogy ha egy pénzügyőr intézkedés közben súlyosan megsérül (például hivatalos személy elleni erőszak), akkor azt a büntetőeljárásól szóló 2017. évi XC. törvény[21] 30. § c) alapján a nyomozó ügyészség fogja a helyszínen vizsgálni, ott meg nem tudom, milyen jogkörrel lép fel egy „civil" hatóság.

Továbbá a NAV SZJTV felhatalmazza a jelen esetben a Pénzügyminisztert, hogy a szolgálati kötelmekkel összefüggő balesetek és betegségekkel kapcsolatos eljárásokat, szabályokat megállapítsa.

Érdekesség, hogy a NAV SZJTV felhatalmazásainál, az egészséget érintő pontokat javarészt tartalmazza a Nemzeti Adó- és Vámhivatalnál adó- és vámhatósági szolgálati jog-

viszonyban állók és tisztjelöltek alkalmassági vizsgálatáról, a gyógyító-megelőző egészségügyi ellátásról, valamint a pénzügyőrök szolgálatképtelenségének megállapításáról szóló 15/2020. (XII. 29.) PM rendelet[22] (továbbiakban 15/2020 PM rendelet), de a fertőző betegségek és oltások, munkaképes állapot vizsgálata, és a szolgálati kötelmekkel kapcsolatos előírásokat nem.

Ez is egy szabályozási anomália, miszerint a törvényi felhatalmazásnak a miniszter nem tett eleget, illetve a korábbi NGM rendeletek nem kerültek felülvizsgálatra.

Jelenleg a NAV a Pénzügyminisztérium alá tartozik, korábban 2010-2018 között a jogelőd Nemzetgazdasági Minisztérium volt a felettes szerv. A 2021-es jogviszony váltást, viszont a Nemzeti Adó- és Vámhivatal hivatásos állományú tagjai esetében alkalmazható egészségkárosodási ellátásról, valamint a baleset, betegség szolgálati kötelmekkel való összefüggésének megállapításával kapcsolatos eljárásról szóló 64/2016 (XII.29.) NGM rendelet[23] (továbbiakban NGM rendelet) nem követte le. A pénzügyőr státusz helyett hivatásos állományra hivatkozik, ami a szervezetben egyedül egy esetben áll meg, akik a Nemzeti Közszolgálati Egyetemre vannak vezényelve, mint hivatásos, de pénzügyőr státuszban.

Mivel az NGM rendelet folyamatosan hivatásosokat emleget, és a HSZT-re hivatkozik, így nem gondolnám helyénvalónak, a pénzügyőrökre használni ezt a jogszabályt.

Kötelesség és veszély

A Munkavédelmi törvény 63. §-ától a NAV SZJTV eltérő rendelkezéseket állapít meg bizonyos esetekben. Az adó- és vámhatósági tisztviselő - ahogy egy civil munkavállaló is - köteles megtagadni felettese utasításának a végrehajtását, ha bűncselekményt vagy szabálysértést valósítana meg vagy más személy életét, testi épségét vagy egészségét, illetve a környezetét közvetlenül és súlyosan veszélyeztetné.

A tisztviselő az utasítás végrehajtását megtagadhatja, ha annak teljesítése az életét, egészségét vagy testi épségét, közvetlenül és súlyosan veszélyeztetné, vagy jogszabályba vagy a feladatellátásra irányadó normatív utasításba ütközne.

Ezzel ellentétben a pénzügyőr részére az utasítás parancs, és a pénzügyőr szükség esetén a veszély vállalásával is végre kell hajtania az utasításokat a NAV SZJTV 80. § (1) bekezdés a) pont alapján.

Ugyanakkor a pénzügyőr köteles felettese utasításának végrehajtását megtagadni, ha annak teljesítésével bűncselekményt követne el, de ezen kivételen túl „a pénzügyőr a jogszabálysértő utasítás végrehajtását nem tagadhatja meg. Ha azonban annak jogellenessége felismerhető számára, arra haladéktalanul köteles az utasítást adó figyelmét felhívni. Ha a felettes a rendelkezését ennek ellenére fenntartja, azt kérelemre írásba kell foglalnia. A jogszabálysértő utasítás végrehajtásáért kizárólag az azt kiadó felel”[12].

Tehát, ha a Munkavédelmi törvény szerint egy pénzügyőr munkája során valakit veszélyeztet, attól még a feladatát végre kell hajtania, legfeljebb kérheti az írásbeli utasítást. Ezt nem tartom életszerűnek, egy családi házas övezetnél, papírfalakkal elválasztott irodaépületnél vagy egy közlekedési szituációnál, ahol a NAV MERKUR bevetési egység fegyveres rajtaütést hajt végre, ahol a hatókörben sok civil tartózkodik.

Ruházatra vonatkozó jogszabályok

A Munkavédelmi törvény 42. § és 44. § pontja előírja, hogy a veszélyes munkafolyamatoknál, a veszélyforrás ellen védelmet nyújtó egyéni védőeszközöket kell meghatározni és biztosítani, valamint gondoskodni kell a munkahelyek munkavédelmi követelményeinek minimális szintjéről szóló 3/2002. (II. 8.) SzCsM-EüM rendelet[24] 18. § bekezdés által előírt öltözőhelyiségekről is. A pénzügyőrök egyenruha viselésre kötelezettek, a Nemzeti Adó- és Vámhivatal pénzügyőri státuszú foglalkoztatottainak Öltözködési Szabályzatáról és a szolgálati igazolványokról, valamint a szolgálati jelvény rendszeresítéséről szóló 1/2021. (I.5.) PM rendelet[25] (továbbiakban: öltözködési szabályzat) alapján, amiben a 8. § előírja, hogy a szolgálati feladat ellátása során, csak a rendszeresített egyenruházati és felszerelési tárgyak viselhetőek. A rendvédelmi szerveknek és a központi államigazgatási szervek részére a büntetés-végrehajtási szervezet részérről a központi államigazgatási szervek és a rendvédelmi szervek irányában fennálló egyes ellátási kötelezettségekről, a termékek és szolgáltatások átadás-átvételének és azok ellentételezésének rendjéről szóló 44/2011. (III.23.) Kormány rendelet[26], valamint a büntetés-végrehajtási szervezet részéről a büntetés-végrehajtásért felelős miniszter vezetése, irányítása vagy felügyelete alá tartozó szervek irányában fennálló ellátási kötelezettségről, a fogvatartottak kötelező foglalkoztatása keretében előállított termékekről és szolgáltatásokról, azok átadás-átvételéről és az ellentételezés rendjéről szóló 9/2011. (III.23.) BM rendelet[27] alapján, a fogvatartottak által gyártott egyenruházati termékek használhatóak.

A pénzügyőrök munkája során a zöldhatár ellenőrzésnél, építkezéseknél, hajó átvizsgálásnál beszállásos munkavégzésnél, lehetnek olyan veszélyek, ahol szükséges lenne például egy légzésvédőre, munkavédelmi sisakra vagy egy talpátszúrás elleni védőcipőre. A rendelet szerint csak rendszeresített felszerelés lehet, így például sajnálatos, hogy a Bv. Holding Kft.-nél kapható szolgálati cipő és gyakorló cipő, amit a PM rendelet meghatároz, nem rendelkezik MSZ EN ISO 20345:2022 egyéni védőeszközökre vonatkozó szabvány[28] általi minősítéssel. A NAV honlapján[29] kizárólag a kényszerítőeszközök rendszeresítéséről szóló dokumentumok találhatóak.

Képesítésre vonatkozó szabályok

A Nemzeti Adó- és Vámhivatalnál rendszeresített pénzügyőri munkakörökről, a képesítési előírásokról, valamint a munkaköri pótlékról szóló 21/2020. (XII. 30.) PM rendelet[30] a szervezetre vonatkozóan meghatározza az adott tevékenységhez a szükséges végzettségeket.

A munkavédelemmel a kapcsolatos tevékenységhez is meghatározza a rendelet a végzettségeket a 2. számú melléklet, 10. Biztonsági munkacsoport 10.1. pontjában előírt felsőoktatásban szerzett végzettségek, azaz:

„10. Biztonsági munkakörcsoport

10.1. Az I. besorolási osztályban:

10.1.1. felsőoktatásban szerzett jogi, gazdaságtudományi, rendészeti (büntetés-végrehajtási szakirány is), nemzetbiztonsági, honvédelmi/nemzetvédelmi és katonai, informatikai, híradástechnikai, távközlési, mechanikai, had- és biztonságtechnikai mérnöki, biztonság- és védelempolitikai, villamosmérnöki, építőmérnöki, agrármérnöki (bármely szakirányon), gazdasági mérnöki, üzemgazdászi felsőfokú iskolai végzettséget adó szakképzettség;

szakirányú továbbképzésben szerzett adó- és pénzügyi ellenőrzési szakértő, mérnök-közgazdász, pénzügyi vállalkozási szakértő szakképzettség;

10.1.2. felsőoktatásban szerzett felsőfokú iskolai végzettséget adó szakképzettség, valamint munkavédelmi technikusi vagy tűzvédelmi előadói, tűzvédelmi főelőadói szakképesítés vagy szakosító továbbképzésben szerzett általános informatikus;"

A NAV GEI Humánpolitikai és Munkavédelmi Főosztálya által korábbi 33/2023 és 30/2022 számú kiírt pályázat a fenti jogszabályban előírt végzettségeket tekinti feltételnek, ugyanakkor a pályázatban előírt feladatok között szerepel a Munkavédelmi törvényben meghatározott munkavédelmi szaktevékenység, ami ez esetben egy tanári diplomával és egy informatikai OKJ végzettséggel el lehet végezni a NAV tekintetében. Ugyanakkor a jogszabály nem veszi figyelembe, hogy 2021-től kezdve már nem munkavédelmi technikus, hanem munkavédelmi előadó néven lehet szaktevékenységre feljogosító végzettséget szerezni. De ha valaki nem a 10.1.1. pontban felsoroltak közül szerzett végzettséget, de egy munkavédelmi szakember/szakmérnök oklevelet szerzett, akkor sem végezhet elvben tevékenységet a NAV-nál.

JAVASLATOK MEGFOGALMAZÁSA A JELENLEGI JOGSZABÁLYOK MÓDOSÍTÁSÁRA

Munkavédelmi törvény

Véleményem szerint, az első és legfontosabb módosítási javaslat a munkavédelemmel kapcsolatos jogszabályokkal kapcsolatban, hogy a NAV felhatalmazást kapjon az eltérésre a Munkavédelmi törvény bizonyos rendelkezéseitől, tehát a 88. § (2) bekezdésében ne csak a rendvédelmi szervek, hanem a NAV is szerepeljen a felsorolásban.

A már említett hatósági jogkör kérdésében a 86. §-ba szintén be kell venni a NAV-ot a pénzügyőrök tekintetében, hogy ne a munkavédelmi hatóság alá tartozzon, hanem egy másik rendvédelmi szervhez vagy a PM alá tartozó önálló hatósághoz.

Szolgálati kötelmek

A NAV SZJTV 247. § bekezdése előírja, hogy külön miniszteri rendeletben meg kell határozni a pénzügyőrök tekintetében a betegségek és balesetek esetén az eljárás rendet, amit félig a Nemzeti Adó- és Vámhivatal hivatásos állományú tagjai esetében alkalmazható egészségkárosodási ellátásról, valamint a baleset, betegség szolgálati kötelmekkel való összefüggésének megállapításával kapcsolatos eljárásról szóló 64/2016. (XII. 29.) NGM rendeletet tartalmaz, de mivel folyamatosan a HSZT-re hivatkozik, így véleményem szerint kompletten hatályon kívül kell helyezni, mivel a benne lévő törvényi felhatalmazás is hatályon kívül helyezésre került, amire a rendelet hivatkozik. Mivel alapvetően a rendelet a HSZT-re illetve olyan korábbi jogszabályokra hivatkozik, amik szintén hatályon kívül vannak helyezve, valamint az egészségügyi ellátásokról a 15/2020 PM rendelet már rendelkezik, így véleményem szerint csak a szolgálati kötelmekkel összefüggő eseményekkel kapcsolatos eljárásokat és definíciókat kell megtartani.

Javaslom a Nemzeti Adó- és Vámhivatal hivatásos állományú tagjai esetében alkalmazható egészségkárosodási ellátásról, valamint a baleset, betegség szolgálati kötelmekkel

való összefüggésének megállapításával kapcsolatos eljárásról szóló 64/2016. (XII. 29.) NGM rendelet hatályon kívül helyezését.

EVE követelmények

A NAV munkavédelmi szabályzata az egyéni védőeszközök tekintetében hivatkozik az egyéni védőeszközök követelményeiről és megfelelőségének tanúsításáról 18/2008. (XII. 3.) SZMM rendeletre[31] (továbbiakban SZMM rendelet), ezért indokolt abban a NAV nevesített szerepeltetése.

Ruházat és védőeszköz

Ahhoz, hogy egy pénzügyőr jogszerűen tudjon egyéni védőeszközt viselni, úgy az öltözködési szabályzaton szükséges módosítani. Mivel a pénzügyőri tevékenység eléggé szerteágazó, így nagyon sok veszélyes munkakör tartozik a szervezethez. A MERKUR bevetési egység, mint kommandó által használt sisak, kesztyű vagy fülvédő tekintetében a vonatkozó jogszabályok alapján nem tisztázott, hogy azok most egyéni védőeszközök vagy sem. De a hajósok is hordanak mentőmellényt, illetve végeznek átvizsgálások alkalmával beszállásos munkavégzést, amikor egy uszály ballaszt tereit vizsgálják át. De elég egy építkezésen történő ellenőrzés, ahol a kivitelező által meghatározott egyéni védőeszközök között szerepel a munkavédelmi sisak. Ha szigorúan vesszük a jogszabályokat, akkor egyéni védőeszközt a pénzügyőr nem viselhet.

SZMSZ

A már korábban említett a Nemzeti Adó- és Vámhivatal Szervezeti és Működési Szabályzatáról szóló 5/2022. (VIII.5.) PM utasítás határozza meg a szervezet felépítését. Véleményem szerint egy szervezet működése akkor tud jól működni, ha a feladatok megvannak határozva, illetve az az adott szinten van kezelve. A NAV esetében, míg a munkavédelemmel kapcsolatos feladatok a 24. § alapján az erőforrás-gazdálkodási elnökhelyettesnél van, úgy az organogramból az látszik, illetve a NAV munkavédelmi szabályzatából[32] az derül ki, hogy ezt a GEI látja el. Szerintem a munkavédelemi feladatok ellátásnak és felügyeletének a gyakorlása fajsúlyosabb téma annál, ahogy egy SZMSZ fél mondatban letudja úgy, hogy közel 40 szerv és 18000 ember vonatkozásában nincs meghatározva semmi konkrétum. Így egy területi szervnek egy osztálya a szervezet „aljáról" kétséges, hogy ezt teljeskörűen el fogja tudni látni, úgy, hogy a munkavédelem megvalósítása mindenhol költség és ez közvetlenül a költségeket irányító gazdasági igazgató alá tartozik.

Munkaképes állapot vizsgálata

A NAV SZJTV a pénzügyőröket a, 80. § (2) b) pontjában műtétnek nem minősülő invazív vizsgálatokra kötelezi, így mind a kábítószer mind az alkohol vizsgálatnál vérvételre kötelezett a pénzügyőr.

Olyan miniszteri rendelet jelenleg nincs, amely ezeket az eljárásokat tartalmazza, illetve a jelenlegi munkavédelmi szabályzatban nincs szétválasztva a jogviszonyok szerint,

illetve nem is tartalmazhatná a vizsgálatok rendjét a hiányzó rendelet miatt. Ez abból szempontból lehet aggályos, ha egy foglalkoztatott pozitív eredményt fúj és nem fogadja el az eredményt, illetve emiatt fegyelmi eljárást kap, úgy jogilag nem járt el megfelelően a munkáltató.

Védőoltások

A NAV SZJTV 80. § (2) bekezdés c) pontja alapján a pénzügyőr köteles magát az előírt védőoltásoknak alávetni, kivéve, ha az egészségügyről szóló 1997. évi CLIV. törvény[33] alapján a kezelőorvos ennek elhalasztásáról dönt, vagy a beteg egészségügyi állapota ezt nem teszi lehetővé.

A NAV SZJTV 80. § (4) és (5) bekezdése egy még ki nem adott miniszteri rendeletre hivatkozik, aminek meg kellene határoznia azokat fertőző betegségeket, melyre szükséges lenne a kötelező védőoltás, a biológiai kóroki tényezők kockázata elkerülése érdekében. A törvény a NAV Képzési, Egészségügyi és Kultúrális Intézetét hatalmazza fel, hogy javasolja a kötelezni kívánt védőoltásokat, melyeket a NAV Elnöke rendel el.

Ha egy pénzügyőr nem kívánja beadatni ezeket az oltásokat, úgy a hiányzó miniszteri rendelet alapján nincs tisztázva az eljárásrend, így jogszerűen nem tud kifogást tenni.

A Pénzügyminisztérium által jogszabály a védőoltásokkal kapcsolatban a NAV tekintetében nem került kiadásra. A 15/2020 PM rendelet csak „A végrehajtott foglalkozás-egészségügyi alapfeladatokra vonatkozó kimutatás adattartalma" című 2. számú mellékletben „a munkakörhöz kötött védőoltásokkal kapcsolatos feladatok esetszáma" miatt került említésre.

Részemről fontosnak tartanám, hogy kötelező védőoltások legyenek előírva.

Hatósági feladatok

A pénzügyőrök és a szolgálati kötelmekkel összefüggő incidensek, valamint a jogszabályi előírásoknak megfelelően a NAV pénzügyőrei tekintetében is szükséges egy külön munkavédelmi hatóságot létrehozni, így azt javasolnám, hogy a már létező hatósági kormányrendeletet módosítani kéne és abba a NAV-val kapcsolatos előírásokat is fel kéne venni.

VESZÉLYES MUNKAFOLYAMATOK ÉS TECHNOLÓGIÁK JOGI ÉS MUNKAVÉDELMI SZABÁLYOZÁSA

Szükségesnek tartom a veszélyes technológiáknak és folyamatoknak az elemzését, mivel a pénzügyőrök feladatuk során sok olyan tevékenységet végeznek, amik munkájukból adódóan számukra természetes és veszélytelennek tartják, de a munkavédelemmel kapcsolatos jogszabályok azokat kifejezetten veszélyesnek minősíti. Ilyen munkák lehetnek a beszállásos munkavégzések[34], melyeket a hajókon, vasúton történő vámellenőrzéseknél végeznek, amikor csempészárut keresnek az egyenruhások. De ugyancsak nagy expozíció éri a fegyveres állományt az éves lövészeteken, a kéz-kar rezgés a lőfegyverek használatánál bőven meghaladja a határértékeket, illetve az olyan munkaköröknél, ahol kifejezetten sok lövészeten kell részt venni így a zaj expozíció is magas. A vámvizsgálatok során előkerülő

ismeretlen anyagok bevizsgálása is felvet kérdéseket, hogy a Szakértői Intézet olyan anyagokat vizsgál be, aminek nem ismerik az eredetét, összetételét, így nem tudják milyen fajta kémiai vagy biológiai expozíció ellen kellene védekezniük vagy mi éri őket. Nem utolsó sorban ott vannak a rendvédelmi feladatok is az egyszerű járőrtől a bevetési egységekre váró veszélyekkel.

Zaj és rezgés

A NAV pénzügyőrei fegyveres rendvédelmi feladatokat ellátó szerv. Ebből adódik, hogy legalább negyedévente lőgyakorlaton vegyenek részt, de vannak olyan szervek melyek heti szinten járnak lőtérre. A maroklőfegyver működéséből adódóan a benne felrobbanó lőpor miatt a lövedék és fegyverre ható erő-ellenerő hatása következtében, a lövő kezére is erő hat, ami egy rezgés. Ez a rezgésgyorsulás a rezgésexpozíciónak kitett munkavállalókra vonatkozó minimális egészségi és munkabiztonsági követelményekről szóló 22/2005. (VI, 24.) EüM rendelet[35] által megengedett 50 m/s2 értéket túl lépheti.

A közben keletkező lő dörej a munkavállalókat érő zajexpozícióra vonatkozó minimális egészségi és biztonsági követelményekről szóló 66/2005. (XII. 22.) EüM rendelet[36] által meghatározott zajexpozíciós határértékek felett van.

A járőr autókon elhelyezett megkülönböztető jelzés is hordoz magában kockázatot, mivel a megkülönböztető jelzések esetén szükséges hangnyomásról az MSZ 07-4009:1982 szabvány rendelkezik mely szerint a gépjárműtől 7 méterre legalább 98 dB(A) hangnyomást kell mérni oldal irányban .

A járőrhajókon lévő infrahangot is szükségesnek tartom vizsgálni, mivel a motor működéséből és az abból adódó rezonanciából keletkező hanghullámok károsak az egészségre főleg, ha folyamatos a szolgálat és a hajón töltik a pihenőidőt is.

A fentiekből adódik, hogy ezekkel kapcsolatban is szükséges a szervezet számára a jogszabályok alóli felmentés, speciális egyedi jogszabály megalkotása, melynek keretében lehetne szabályozni a gyakorlatokat és intézkedéseket nem befolyásoló megfelelő egyéni védőeszközök és szolgálatszervezések biztosítását.

Kémiai kockázatok

A jövedéki termékek vizsgálata, lefoglalása, csempészáru felkutatása, vámvizsgálat stb. mind a NAV feladata. Ebből adódóan a NAV pénzügyőreinek és a Szakértő Intézetének a feladata az üzemanyagok mintavétele és laborvizsgálata, hogy ténylegesen azt tartalmazza, amit a vásárló kifizet. Így rendszeresek a NAV részéről az üzemanyagtöltő állomásokon a mintavételek. A határátkelőhelyeknél a csomagokat átnézése során találhatnak kábítószernek minősülő anyagokat, hamis dohánytermékeket, ismeretlen helyről származó és ismeretlen anyagokat tartalmazó termékeket. Ezek mind kémiai és biológiai kockázatot jelentenek, amire szükséges intézkedni, főleg, mert sok olyan anyaggal találkozhatnak, ami nem szerepel a kémiai kóroki tényezők hatásának kitett munkavállalók egészségének és biztonságának védelméről szóló 5/2020. (II. 6.) ITM rendeletben[37].

Pszichoszociális stressz

Merkúr, fedett nyomozók, rendőrségi közös akciók, ellenőrzések (építkezés, kocsma), vámvizsgálat, csomagbontás, fegyver és kényszerítőeszköz használat, nyomozás, stb., mind olyan tevékenység, ami stresszel jár.

A stresszt nehéz mérni. A pénzügyőröknek van pszichológiai vizsgálata, de úgy gondolom, hogy ez nem a lelki érzelmi terhek leadására van, hanem hogy képes-e szabály követően és stabilan szolgálatot teljesíteni, illetve nincs-e mentális problémája. Szerintem nagyon sok figyelmet kéne fordítani a mentális kondícióra, hogy ne égjenek ki az emberek, illetve tudjanak beszélni a problémájukról. Fontos, mivel sok olyan beosztás van, ahol teljes titoktartás mellett kell élniük. Ezekből a problémákból adódhat később egyéb függőségek kialakulása is, ami természetesen egy életpálya összeomlásához vezethet. A vezetőknek külön kellene erre figyelniük, hogy beosztottjaik, mit hogyan élnek meg, milyen segítség szükséges a számukra.

Szükségesnek tartanám a 15/2020 PM rendeletnek az ez irányú kiegészítését vagy egy belső eljárásrendet kialakítani, hogy a pszichoszociális kockázatok értékelésre kerüljenek, valamint a szükséges intézkedések elérhetőek legyenek az állomány részére.

ÖSSZEFOGLALÓ

A NAV pénzügyőreire vonatkozó hatályos munkavédelmi jogszabályi előírások ismertetését követően az azokkal kapcsolatos szerintem megállapítható jogszabályi hiányosságokra szerettem volna rámutatni, valamint ezek kiküszöbölésére szövegszerű jogszabályalkotási, jogszabálymódosítási javaslatokat tenni.

Összefoglalva látszik, hogy a NAV tekintetében több esetben a speciális feladatellátásból is adódóan nincs meg a jogharmónia, nagyon sok módosításra és új jogszabály kiadására lenne szükség, hogy a pénzügyőrök munkavédelmi szempontból – a rájuk vonatkozó speciális szabályok előírásainak a mentén is – az egészséget nem veszélyeztető és biztonságos feltételek minél teljesebb körű biztosítása mellett jogszerűen tudják ellátni a feladataikat.

A jogszabályok helyretétele, a szükséges jogszabályok megalkotása, módosítása állami feladat. Ezek után a NAV-nak szervezeti szinten kell megoldani, hogy a munkavédelem központi helyre kerüljön és egységesen, a részletszabályokat jól megfogalmazva, – azokat alkalmazhatóan meghatározva – kellő mennyiségű referenssel leoktatva és visszaellenőrizve bevezesse az új szabályokat. Fontosnak tartanám, ha a Pénzügyminisztériumnak is lenne egy munkavédelmi főreferense, aki figyelemmel kíséri e folyamatokat és jogszabályváltozásokat.

A NAV elvárja a pénzügyőröktől, hogy életük kockáztatásával hajtsák végre a tevékenységüket, de munkavédelmi szempontból nincsenek jogilag védve a foglalkoztatottak, illetve a különleges szolgálatokat ellátók adatai is kikerülhetnek, ami a személyazonosságuk védelme miatt aggályos, így a NAV részére külön munkavédelmi hatóság kijelölése mindenképpen szükséges.

Az egyenruha és védőeszközök összhangba hozása is átgondolandó vagy olyan egyenruha rendszeresítése szükséges, amely megfelel a szabványoknak.

Elengedhetetlen foglalkozni a pszichoszociális stresszel, valamint egy alkoholpolitikát kialakítani a szervezet részére.

Úgy gondolom, hogy a jogalkotók nagy feladat előtt állnak, hogy minden jogszabály összhangba kerüljön, és így a pénzügyőrök is megkapják a biztonságos és egészséges munkafeltételeket.

FELHASZNÁLT IRODALOM

[1] *1993. évi XCIII. törvény a munkavédelemről*.
[2] *2010. évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról*.
[3] *1992. évi XXIII. törvény a köztisztviselők jogállásáról*.
[4] *1996. évi XLIII. törvény a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról*.
[5] *5/1993. (XII. 26.) MüM rendelet a munkavédelemről szóló 1993. évi XCIII. törvény egyes rendelkezéseinek végrehajtásáról*.
[6] *5/2022. (VIII. 5.) PM utasítás a Nemzeti Adó- és Vámhivatal Szervezeti és Működési Szabályzatáról*.
[7] „A Nemzeti Adó- és Vámhivatal Szervezeti és Működési Szabályzata". Nemzeti Adó- és Vámhivatal. [Online]. Elérhető: https://nav.gov.hu/kozadat/altalanos_kozzeteteli_lista/nav_feladat_es_hataskore_1366633265651/szmsz/nav_szmsz
[8] *485/2015. (XII. 29.) Korm. rendelet a Nemzeti Adó- és Vámhivatal szerveinek hatásköréről és illetékességéről*.
[9] *250/2014. (X. 2.) Korm. rendelet a Közbeszerzési és Ellátási Főigazgatóságról*.
[10] *2015. évi CXCI. törvény egyes törvényeknek a Nemzeti Adó- és Vámhivatal átalakításával, valamint a költségvetési tervezéssel és gazdálkodással kapcsolatos módosításáról*.
[11] *2010. évi XLIII. törvény a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról*.
[12] *2020. évi CXXX. törvény a Nemzeti Adó- és Vámhivatal személyi állományának jogállásáról*.
[13] *2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról*.
[14] *2011. évi CXCIX. törvény a közszolgálati tisztviselőkről*.
[15] *20/2018. (XII. 21.) PM rendelet a pénzügyőri intézkedések és a kényszerítő eszközök alkalmazásáról, valamint az elfogott, előállított, őrizetbe vett és fogva tartott személyek őrzésének és kísérésének eljárási szabályairól*.
[16] *1997. évi LXVIII. törvény az igazságügyi alkalmazottak szolgálati jogviszonyáról*.
[17] *373/2011. (XII. 31.) Korm. rendelet a munkavédelmi hatósági feladatokat ellátó egyes szervek kijelöléséről*.
[18] *10/2020. (III. 31.) BVOP utasítás a büntetés-végrehajtási szervezet Munkavédelmi Szabályzatáról*.
[19] *70/2011. (XII. 30.) BM rendelet a belügyminiszter irányítása alá tartozó rendvédelmi szervek munkavédelmi feladatai, valamint foglalkozás-egészségügyi tevékenysége ellátásának szabályairól*.
[20] *27/1996. (VIII. 28.) NM rendelet a foglalkozási betegségek és fokozott expozíciós esetek bejelentéséről és kivizsgálásáról*.

[21] *2017. évi XC. törvény a büntetőeljárásról*.
[22] *15/2020. (XII. 29.) PM rendelet a Nemzeti Adó- és Vámhivatalnál adó- és vámhatósági szolgálati jogviszonyban állók és tisztjelöltek alkalmassági vizsgálatáról, a gyógyító-megelőző egészségügyi ellátásról, valamint a pénzügyőrök szolgálatképtelenségének megállapításáról*.
[23] *64/2016. (XII. 29.) NGM rendelet a Nemzeti Adó- és Vámhivatal hivatásos állományú tagjai esetében alkalmazható egészségkárosodási ellátásról, valamint a baleset, betegség szolgálati kötelmekkel való összefüggésének megállapításával kapcsolatos eljárásról*.
[24] *3/2002. (II. 8.) SzCsM–EüM együttes rendelet a munkahelyek munkavédelmi követelményeinek minimális szintjéről*.
[25] *1/2021. (I. 5.) PM rendelet a Nemzeti Adó- és Vámhivatal pénzügyőri státuszú foglalkoztatottainak Öltözködési Szabályzatáról és a szolgálati igazolványokról, valamint a szolgálati jelvény rendszeresítéséről*.
[26] *44/2011. (III. 23.) Korm. rendelet a büntetés-végrehajtási szervezet részéről a központi államigazgatási szervek és a rendvédelmi szervek irányában fennálló egyes ellátási kötelezettségekről, a termékek és szolgáltatások átadás-átvételének és azok ellentételezésének rendjéről*.
[27] *9/2011. (III. 23.) BM rendelet a büntetés-végrehajtási szervezet részéről a büntetés-végrehajtásért felelős miniszter vezetése, irányítása vagy felügyelete alá tartozó szervek irányában fennálló ellátási kötelezettségről, a fogvatartottak kötelező foglalkoztatása keretében előállított termékekről és szolgáltatásokról, azok átadás-átvételéről és az ellentételezés rendjéről*.
[28] *MSZ EN ISO 20345:2022 Egyéni védőeszközök. Biztonsági lábbeli (ISO 20345:2021)*.
[29] „A Nemzeti Adó- és Vámhivatal rendszeresített kényszerítő eszközei". [Online]. Elérhető: https://nav.gov.hu/kozadat/altalanos_kozzeteteli_lista/nav_feladat_es_hatskore_1366633265651/nav_kenyszerito_eszkozei
[30] *21/2020. (XII. 30.) PM rendelet a Nemzeti Adó- és Vámhivatalnál rendszeresített pénzügyőri munkakörökről, a képesítési előírásokról, valamint a munkaköri pótlékról*.
[31] *18/2008. (XII. 3.) SZMM rendelet az egyéni védőeszközök követelményeiről és megfelelőségének tanúsításáról*.
[32] „A Nemzeti Adó- és Vámhivatal vezetője által kiadott 2134/2016/VEZ szabályzat a munkavédelemről". [Online]. Elérhető: https://abpe.nav.gov.hu/abpe_joomla/images/stories/komponens/2016/2134-2016_munkavedelemrol.doc
[33] *1997. évi CLIV. törvény az egészségügyről*.
[34] *MSZ-09-57.0033-1990 szabvány Munkavédelem. Veszélyes berendezésekben beszállással végzett munkák biztonságtechnikai követelményei*.
[35] *22/2005. (VI. 24.) EüM rendelet a rezgésexpozíciónak kitett munkavállalókra vonatkozó minimális egészségi és munkabiztonsági követelményekről*.
[36] *66/2005. (XII. 22.) EüM rendelet a munkavállalókat érő zajexpozícióra vonatkozó minimális egészségi és biztonsági követelményekről*.
[37] *5/2020. (II. 6.) ITM rendelet a kémiai kóroki tényezők hatásának kitett munkavállalók egészségének és biztonságának védelméről*.

SOME ASPECTS OF STRUCTURAL STABILITY IN THE FIELD OF FIRE SAFETY AT WORK

A SZERKEZETI STABILITÁS EGYES VONATKOZÁSAI A MUNKAHELYI TŰZBIZTONSÁG TERÉN

NAGY Rudolf [1]

Abstract

Fire safety in the workplace requires a comprehensive understanding of the basics of fire safety that goes well beyond lay fire safety knowledge. The subjects covered here, which deal with the issues of strength and stability, take a somewhat different approach to the occupational safety components of fire protection, inspired by the general fire safety professional approach. The reason for this is the rather different way in which the EU-wide sectoral regulatory framework for fire safety at work is structured within the Community hierarchy. The basic document from which the issue of fire safety in the workplace will be derived is Council Directive 89/391/EEC, which underpins this and is the starting point for this paper. In other words, the approach to fire safety adopted here is based on the principles of occupational safety and health. It is also clear from what has been described that, in the context of the knowledge reviewed here, the occupational safety aspects of preventive measures to reduce the risk of fire in the workplace can only be understood in their basic context. It is therefore not possible to provide an overview of the entire professional knowledge of fire safety design for architects in this form.

Keywords

fire, workplace, fire safety, strength, building structure

Absztrakt

A munkahelyi tűzbiztonság a laikus tűzvédelmi ismereteken jelentősen túl mutató átfogó alapokat kíván az abban érintettektől. Az itt felvonultatott szilárdság és stabilitás kérdésével érintett tárgykörök az általános tűzvédelmi szakmai felfogás inspirálta megközelítéstől némileg eltérően tárgyalja a tűz elleni védekezés munkabiztonsági összetevőit. Ennek oka a munkahelyi tűzbiztonság megteremtését célzó uniós szintű ágazati szabályrendszer közösségi hierarchiájába tagozódásának meglehetősen eltérő volta. Az ezt alátámasztó, és egyben ezen írás kiindulópontját is kitűző alapdokumentum, amelyből a munkahelyi tűzbiztonság kérdését az elkövetkezendőkben származtatjuk, a (89/391/EGK) Tanács Irányelv. Vagyis a tűzvédelem itt alkalmazott megközelítéséhez a munkavédelmi elvek képezik a fő szempontot. A leírtakból az is kitűnik, hogy az itt áttekintett ismeretek birtokában a munkahelyeken jelentkezhető tűzkockázatok csökkentését szolgáló preventív intézkedések munkabiztonsági kapcsolódási pontjai az alapösszefüggések szintjén válnak csak értelmezhetőkké. Tehát a teljes építész tűzvédelmi tervezői szakmai ismeretek áttekintésére ilyen formán ezen kereteken belül nem vállalkozhatunk.

Kulcsszavak

tűz, munkahely, tűzbiztonság, szilárdság, épületszerkezet

[1] nagy.rudolf@uni-obuda.hu | ORCID: 0000-0001-5108-9728| habil. senior lecturer, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary| habil. adjunktus, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

Az Irányelvben foglaltak szerint a munkáltató felelősségi körében intézkedni köteles a munkavállalók biztonságának és egészségének védelmére, beleértve a tűzek megelőzését is. Ennek megfelelően a munkavédelem tekintetében az Irányelv 1. melléklete a már a munkahelyek létesítéséhez kötődően is taglalja tűzvédelem kérdéskörét. Vagyis a munkahelyi élet- és vagyonvédelem tűzbiztonság oldaláról jelentkező feladataiban prioritásként kezelendő a megelőzés eszközrendszere. A tűzveszély jelentette kockázatok kezelését és az ezek eredményességét biztosító ismeretek átadását is ideértve. Szükségszerű tehát, hogy a munkavédelmi képzés keretében tematikusan tárgyaljuk a tűzbiztonság lényeges kérdéseit. Az ehhez kapcsolódó kérdéskörök általánosságban véve az alábbi három terület köré csoportosíthatók:

- Épületek szerkezeti kialakítása (Stabilitás és Szilárdság),
- Veszélyeztetetteknek a veszély hatóköréből való kivonása (Menekülés),
- Veszélyeztetettek időbeni figyelmeztetése és a tűz megfékezése (Tűzjelzés és tűzoltás). [1]

Alapvetően a munkahelyeken keletkező tűzek kialakulásának kockázata elsősorban az ott zajló munkafolyamatokban felhasznált anyagok, valamint az alkalmazott technológia tűzveszélyességétől függ. A tűz kockázatának további meghatározó fontosságú eleme a tűzterjedés jellege, hisz a nagyobb kiterjedésű tűz növeli a tűz súlyosságát, vagyis nagyobb kockázatot jelent. A tűzterjedés pedig sok egyéb mellett lényeges mértékben függ az adott környezetben fellelhető éghető anyagok mennyiségétől. Ilyen formán mind a szabadban tárolt vagy épületen kívül telepített technológiákban jelenlévő tűzveszélyes anyagok, illetőleg az épített létesítmények által befogadott helyiségek kialakításánál a térelhatároláshoz felhasznált építőanyagok tűzvédelmi tulajdonságaitól. [2]

SZABADBA TELEPÍTETT TECHNOLÓGIÁK TŰZBIZTONSÁGA

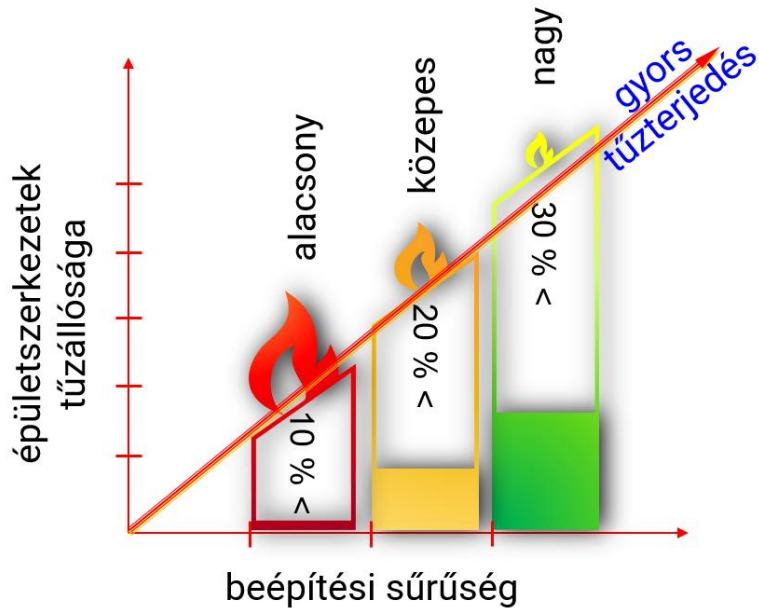
Egyes gyártási, létesítményüzemeltetési eljárásokra jellemző, hogy némely termelési fázisok technológiai elemeit szabadban létesülő állvány jellegű építményeken helyezik el. A tűz terhelés szempontjából bizonyos értelemben kedvezőnek is nevezhetjük az ilyen létesítmények tűzbiztonságát, hiszen mind a gyártó berendezések, mind pedig a technológiai kapcsolatokat biztosító épületszerkezetek a legtöbb esetben nem éghető anyagból készülnek. Ezért a tűzterjedésbe való bekapcsolódásukkal szerkezeti anyagaikat tekintve nem kell számolnunk. Túl ezen a szabad téri tűzfejlődés során a termikus állapotokra jellemzően többszáz fokkal is alacsonyabb lehet a szerkezeteket érő tűzhatás, és szerkezeteik szilárdságvesztésének állapota is jóval később következhet be. Másfelöl azonban a tűzeseti hatásokat nézve a térelhatároló falszerkezetek hiánya miatt azok tűzterjedést korlátozó tűzvédelmi szerepe nem használható ki. Ráadásul az így kialakított technológiai terek nemegyszer szorosan egymás mellett, sőt akár közvetlenül egymás fölötti technológiai helyiségekként kerülnek beépítésre az állványszerkezetbe. [3]

A szabadban telepített technológiai rendszerek tűzbiztonságát illetően nem elhanyagolható körülmény az időjárási viszonyok befolyásoló hatása. A technológiai berendezések szerkezeti beépítését jellemzően acélvázas épületszerkezetekkel oldják meg. Így az ezek időjárás szerkezeti korrózióvédelmén túl érdemleges tényező a megfelelő villámvéde-

lem biztosítása, amelynek hiányában komoly tűz- és robbanásveszélyt jelentene. Ugyanakkor az időjárási hatások sorában említenünk kell a közvetlen napsugárzást, amely különösen a tartályok felmelegedését, és megfelelő körülmények esetében azok kigyulladását, felhasadását is okozhatják. Nem véletlen, hogy a nagymértékű hőelnyelés elkerülése végett az éghető folyadékok tárolását szolgáló tartályok külső palástya a napfény visszaverést elősegítő fehér színűek. A másik lehetőségként gyakran alkalmazott megoldás a veszélyes környezeti következmények kivédésére a tartályok földbe süllyesztése. [4]

Kevéssé gondolnánk, a kritikus felmelegedés mellett az alacsony hőmérsékletek ugyancsak veszélyt hordozhatnak magukban üzembiztonsági és akár még tűzvédelmi szempontból is. Ezek a zárt tartályokban lévő gázok, gőzök térfogatcsökkenését kiváltva még masszív tartályok rideg törését is képesek okozni. Másfelöl a tűzeset során fellépő esetleges szélviszonyokat nemcsak a tűzoltást megnehezítő hatásként kell számításba venni, de a lángokat az épületszerkezetek felé terelve azok gyors szilárdságvesztésüket idézheti elő. Így a tűz várható hatásának meghatározásánál ismerni kell az anyagok alapvető tűzeseti viselkedésén felül a létesítmény épített elemeinek jellemzőit is. [5]

Ezek tűz terjedés elleni védelmének szempontjait sajátos megvilágításba helyezi a technológiai terek összekapcsolásának és a tűzterjedés és az ezzel gyakran párosuló robbanás elleni védelem követelményeinek szinkronba hozását. Különösen, ha ezeket nem egy zöldmezős beruházással megvalósuló, már meglévő technológia átalakítását, bővítését kell megoldani a korlátosan rendelkezésre álló telephelyi területeken belül. Ez a nagyobb beépítettség révén jelentékenyen ronthatja a tűzkockázatok mértékét. Az ilyen üzemi telepítési környezetben a tűzterjedés miatti veszélyeztetettség a létesítmény beépítettségi sűrűségének növekedésével fokozódik, ahogyan annak viszonyrendszerét a 1. ábra is megjeleníti.



1. ábra: A telephelyi beépítési sűrűség és a szerkezetek tűzállósági teljesítményének logikai kapcsolata a várható tűzterjedés dinamikájával összefüggésben
Forrás: Szerkesztette [6] nyomán a szerző

Azonban az itt fellépő, a védelmet gyengítő körülményeket ellensúlyozhatjuk a nagyobb tűzzel szembeni ellenállást tanúsító, nagy tűzállósági teljesítménnyel rendelkező épületszerkezetek kialakításával. Bár ezek meghatározása tűzvédelmi tervezői feladatok tekintetében egy szakmailag igen összetett, sok részlet érvényesítését megkövetelő, alapos kockázatértékelést megkívánó problémakör, mégis általánosságban elmondható, hogy a megállapított tűzkockázatok mértékének egy-egy fokozattal történő emelkedése a tűzállósági teljesítmény követelmények tekintetében nem ritkán 100%-os szerkezeti állékonyságnövekedést generálnak. Nyilvánvalóan robbanásveszély tekintetében hatványozottan fokozódó teherviselési követelmények jelentkeznek a biztonsági előírások teljesítése terén, melyekkel a gépek berendezések védelménél közelebbről is megvizsgálunk.

ÉPÜLETSZERKEZETEK TŰZVÉDELMI FUNKCIÓI

A tűz elleni védekezést érintően vitathatatlanul összetettebb problémakörrel szembesülünk, amikor a munkavégzésre szolgálók terek megvalósítását zárt terekben kell biztosítani. Az ilyen munkahelyek létrehozása, kialakítása során biztosítani kell, hogy tűz esetén az azt befogadó épületek úgy létesüljenek, hogy a tűz bekövetkezése esetén az épület fő strukturális egységét képező tűzteherre méretezett tűzvédelmi funkciót betöltő kitüntetett szerkezeti elemei kellő ellenállást tanúsítsanak a tűz hatásaival szemben. Így a benne tartózkodók a tervezett menekülés ideje alatt ne legyenek tűz közvetlen, illetve az épületszerkezetek károsodásából eredő fizikai sérülések veszélyének kitéve, valamint meggátolják, lassítsák a tűz terjedését.

Ezért első lépésben az épületek szerkezeti anyagát kell gondosan megválasztani. Felvetődhet a kérdés, miért lényeges a szerkezeti kialakítás anyagául szolgáló építőanyagok tűzvédelmi felemlítése?

Tekintve, hogy egy építményben megjelenő, beépített anyagok különböző módon kerülnek kölcsönhatásba a tűzzel, illetőleg más és más módon reagálnak az őket érő tűzhatásra is, ezeknek összhangba kell leniük a létesítményre nézve kialakított tűzvédelmi koncepcióval. [7] Az épületekben felhasznált építési termékek egy része anyagi átalakuláson megy keresztül, míg mások „csupán” alakváltozásokat szenvednek el. Azonban tűzhatás időtartamának arányában egyre gyengül a szerkezeti szilárdságuk, melynek következtében a szerkezeti állékonyságuk kritikus állapotát elérve kívánt statikai állapotukat nem tudják tovább megőrizni. Másfelől pedig lesznek olyan épületszerkezeti elemei az építménynek, amelyek éghető anyagok lévén bekapcsolódhatnak, közrehatnak a tűz fejlődésében, terjedésében, a tűz veszélyének növekedésében, súlyosságának fokozásában. Természetesen ezen kedvezőtlen körülmények idő előtti kifejlődésének megfelelő tűzvédelmi megoldásokkal elejét lehet venni. [8]

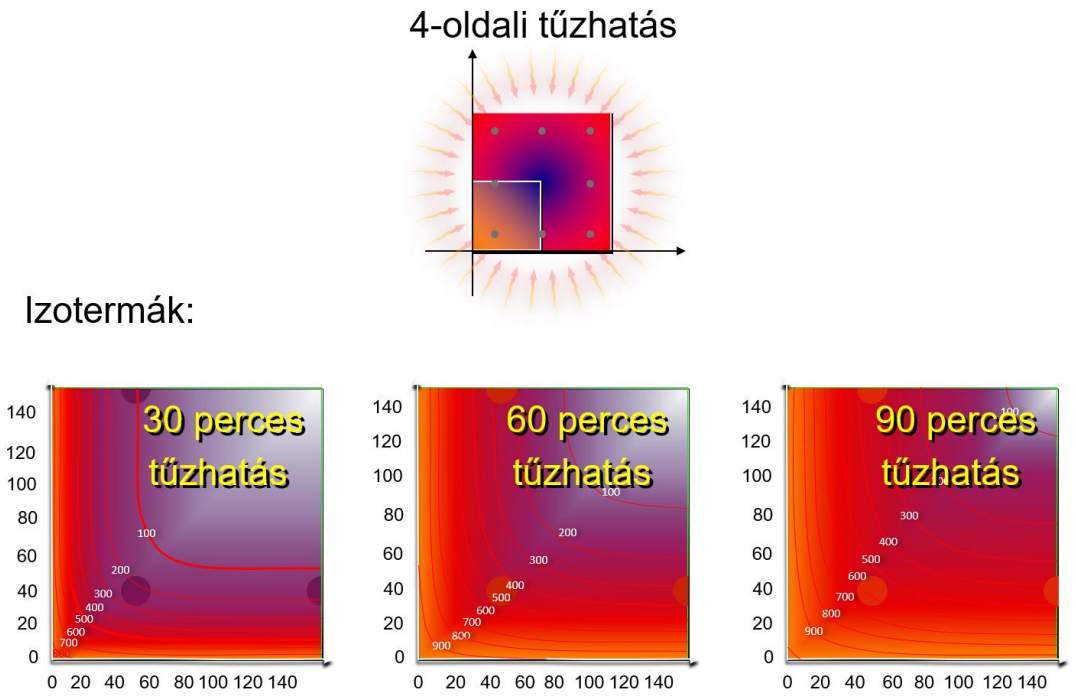
A tűz elleni védelemben alkalmazható megoldások két alapvető kategóriára oszthatók, úgymint passzív és aktív tűzvédelem. A különböző passzív védelmi megoldások a tűzvédelem területén sok helyütt megjelenhetnek. Mégis a megelőző tűzvédelem passzív elemei szempontjából elsődleges a tűz kialakulásának és terjedésének akadályozását szolgáló, elsősorban az építési termékek kiválasztásán alapuló szerkezeti kialakítás. Ugyancsak idesorolandók az épületek egymáshoz viszonyított telepítés helyének tűztávolság tartásával történő megválasztása. Ennek lényegét a tűznek a létesítménytől való távoltartása képezi. Hasonló funkciót töltenek be az egybeépítés során az épületek külső határoló felületein al-

kalmazandó tűzterjedésgátló megoldások vagy a tűz épületen belüli terjedésének akadályozásában szerepet játszó tűzgátlónyílászárók, valamint a szerkezeti áttörések, technológiai összeköttetést biztosító nyílások tűzgátló lezárásának a megoldásai is. [9]

Hogyha megnézzük a tűzvédelmi előírás rendszer által a szilárdsággal összefüggésben támasztott követelményrendszert, tapasztalhatjuk, hogy ezek igen sokrétűek, kezdve a tartószerkezetektől, egészen az úgynevezett tűzálló kábeltartó szerkezetekig bezárólag. Megállapíthatjuk, hogy attól függően, hogy milyen védelmi célokat kell teljesíteni, különböző követelményeknek kell teljesülniük. Ez azt is jelenti, hogy ha meg akarom védeni a munkavállalókat, nyilvánvalóan ehhez megfelelő feltételeket kell biztosítani, hogy tűz esetén ki tudjuk őket juttatni a tűztől érintett épületből. Ahhoz, hogy ez megtörténhessen, olyan munkakörnyezetet, olyan szilárd és stabil szerkezetek képezte munkakörnyezetet, építményeket kell kialakítani, amelyek garantálják, hogy a menekülésre szánt időtartamon belül ki tudnak menekülni az építményből. El tudják azt hagyni biztonságosan anélkül, hogy rájuk omlana a tűz következtében meggyengült épületszerkezet. Ehhez természetesen nagyon sok fizikai tényezőt is figyelembe kell venni. Már a tervező asztalon meg kell tervezi az elsődleges stabilitás nyújtó tartószerkezeteket a rendeltetésből és az ehhez illeszkedő, az épület belső térelhatárolása szerinti elrendezésből adódóan várható tűzteherre. [10]

Az épületfizikai körülmények között a legmeghatározóbbak a különböző hő transzportfolyamatok, amelyek egy építményben nagyon összetettek lehetnek. Emellett a lehetséges tűzkitét oldaláról is vizsgálandó tényezők: a szerkezet térbeli orientációja, valamint más szerkezeti elemekkel való fizikai kapcsolata. Az ezek összefüggéseinek megítéléséhez egy-egy konkrét épület esetében komoly építész tűzvédelmi szakmai ismertekre van szükség. Azonban az azt megalapozó általános ismeretek kiinduló pontjait jól megfogható módon írta le a magyar származású amerikai építész Harmathy Tibor, akinek a lefektetett alapvetései máig hivatkozási alapként szolgálnak az összetett épületszerkezetek tűzállóságának megítélésében. A róla elnevezett Harmathy-szabályok tíz fő pontba szedve rögzítik tételeit, melyeket esetenként a korszerű szerkezeti megoldásoknál egyedi kiegészítésekkel kombináltan kell értelmeznünk, amelyek mélyebb szakmai összefüggéseit Takács munkájában részletesen részletezünk ismereti. [11]

Mindezen alapvetések mellett az épületszerkezet érő tűzhatás statikai állapotokra gyakorolt befolyásának alakulását alapvetően a szilárdsági határállapotok bekövetkezése határozza meg. Az ezt definiáló paramétert a szerkezetek tűzzel szembeni ellenállását megadó tűzállósági határértékkel fejezhetjük ki. Itt értelemszerűen elsődlegesen a tűz dinamikája a mérvadó. Tehát a tűz fejlődésének várható időbeli lefolyása lényeges szempontja kell, legyen a tervezéskor megállapított tűztehernek, mivel ez döntő kihatással lesz a szerkezetekben lezajló termikus változásokra, amint azt a 2. ábrából is kiolvashatjuk.



2. ábra: Vasbeton átmelegedésének izotermái
Forrás: Szerkesztette [12] nyomán a szerző

Így fontos megfelelő pontossággal „prognosztizálni" a tűzhatás várható időbeli alakulását, amely első hallásra meghökkentően hat még a megfelelő műszaki ismeretekkel rendelkezők számára is. Logikus, hogy nem azonos a várható hőmérsékleti értékek alakulása teszem azt egy Tüzép telepen azonos tömegben tárolt fapellet és polisztirol hőszigetelő lemez égése során, köszönhetően egyebek mellett például az anyagi minőség okozta eltérő fűtőértékeknek.

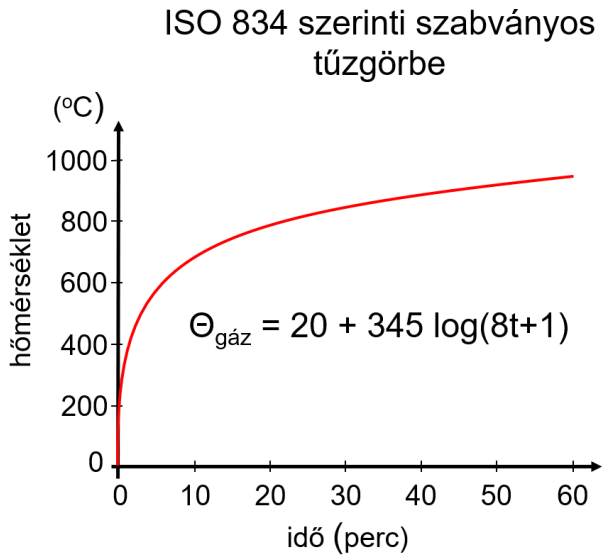
Ráadásul maradva ezen példánál a két éghető anyag égési folyamataiban az anyagi jellemzőikkel is szorosan összefüggő diffúziós égés eltérő felfutását eredményezik a termikus folyamatoknak. Nyilvánvalóan a porisztirol mint éghető műanyag intenzívebb égés fog produkálni. Nem is beszélve a tűz keletkezését kiváltó gyújtóforrások teljesítményéről, és más egyéb körülményekről.

Ha egy épület adott helyiségében bekövetkezhető tűz esetében megkívánjuk határozni milyen tűzterhelés érheti a szerkezeteket, és mindezeket hagyományos, valamennyi tényezőt egyedi matematikai számításokkal integráltan szeretnénk megoldani, látszólag rendkívül összetett és igen időigényes feladatra vállalkoznánk. Ilyenkor logikailag leegyszerűsíthető a probléma a maximálisan felszabadulható hőmennyiség kérdésére, amely matematikailag a hőmérsékleti értékek felvételével kirajzolódó függvény integrálásával áll elő és ilyenformán megegyezik görbe alatti összegzett terület nagyságával. Kémiai értelemben az ezt produkáló tűz termelte hő nem másból keletkezik, mint az adott térben jelenlévő oxigénnel való egyesülésből. Vagyis ha számszakilag nézzük, akkor kiindulhatunk az oxigén mennyiségéből eredően felszabadítható hőmennyiségekből, de persze megfordítva a kérdést

számolhatunk az éghető anyagok égéshőjével is. Bár ez utóbbi egy-egy termelő üzemcsarnokban már valóban megbonyolíthatja a számítások elvégzését.

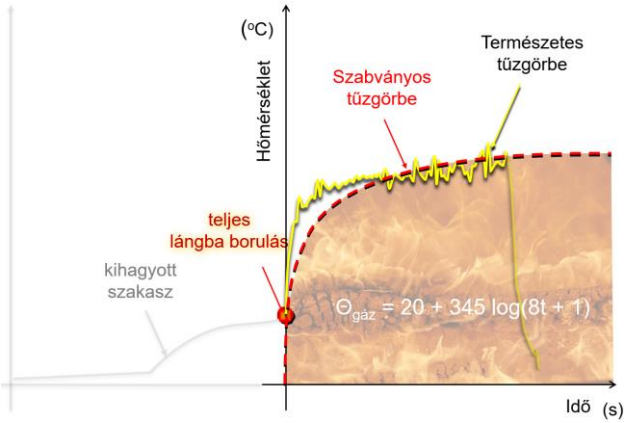
Mindezek mellett azt is számításba kell venni, hogy az előzőekben logikai megfontolással szemben lehet, hogy csak egy úgynevezett lokális tűz jelentette hő hatás éri a szerkezetet. Az ezen eltérő esetekre kidolgozott számítási módszerek megközelítésében a hőhatások alapvető különbségeként jelenítik meg, hogy a feltételezett tűz eléri-e a mennyezetet, vagy sem. Nyilván a vizsgált szerkezet szempontjából a lokális tűz esetét feltételezve a tűz szerkezethez viszonyított helyzete ugyancsak döntően befolyásolja a hőtranszport folyamatok révén a szerkezetet érő tűzhatást. [13]

Az előbbiekben elmondottak komplexitásából levezethető tűzhatások is nagyon eltérőek lehetnek. Ezért az úgynevezett zártéri tüzekben a hőtermelés ütemét az idő függvényében ábrázoló természetes tűzfejlődési görbék alapján a különböző esetek változó dinamikát rajzolnak ki. Ezt az összetett és a tervezést nehezítő viszonyrendszert kiküszöbölendő a szerkezetek tűzteherre történő tervezésében a 3. ábrán illusztrált úgynevezett szabványos tűzgörbékből kiindulva alakították ki a tűzterhelés tűzvédelmi tervezésének szemléletet. [14]



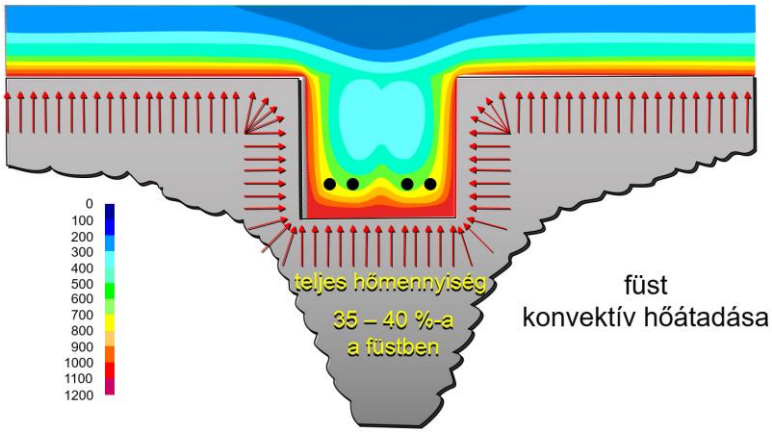
3. ábra: ISO 834 szerinti szabványos tűzgörbe
Forrás: Szerkesztette [15] nyomán a szerző

A szabványos tűzgörbék megalkotásához az a biztonság konzervatív megközelítését alkalmazó a mérnöki absztrakciót követték, hogy a természetes tűzfejlődés során az épületszerkezetekre nézve számottevő tűzhatással járó kifejlett tűz hőtermelési dinamikájának jellegét leképező szakaszát építették bele a szabványokba. *[16]* Elhagyva annak hanyatló végállapotát. Bár a szabványosított tűzgörbék változatosak, azonban legtöbbjük kezdő pontjául a természetes tűzfejlődési görbe teljes lángba boruláshoz köthető inflexiós pontjának bekövetkezése időpillanatát választották. Némely esetben a hanyatló szakaszt is ugyan így elhagyják. Ezt tükrözi vissza a 4. ábra.



4. ábra: A természetes zárttéri tűzfejlődési és a szabványos tűzgörbe kapcsolata
Forrás: Szerkesztette [17] nyomán a szerző

Egy munkahelyként szolgáló építmény szerkezete tekintetében nem egyedül a láng hősugárzásával transzportáló hő jelenthet veszélyt. A legtöbb tűzeset kapcsán a hő terjedésének mindhárom válfaja megtalálhatók a tűzhelyszínen. Így nemcsak a közvetlen tűz hatás lesz az, ami gyengítő lesz egy épület szerkezeti stabilitására. A tűztérből származó hősugárzás, illetve a füstben jelenlévő égéstermékek hősugárzása egyaránt terhelik a munkahely térelhatárolását és annak stabilitását biztosító szerkezetek állékonyságát. Emellett jelentős konvektív hőátadás is történik. Hiszen az égéstermékek, amelyek igen magas hőmérsékletre hevülhetnek, egy építményen belül elérhetik a több száz, de akár az 1000 Celsius fokos hőmérsékletet is. Miközben ezek közvetlen fizikai érintkezésbe kerülhetnek a szerkezetekkel folyamatosan gyengítik azok szerkezeti szilárdságát és integritását. Ahogyan az 5-ös ábrán, a füsttel közvetlen érintkezésbe került födém és a vele szerkezeti egységet képező vasbeton gerenda átmelegedésének példájából is kiolvasható.

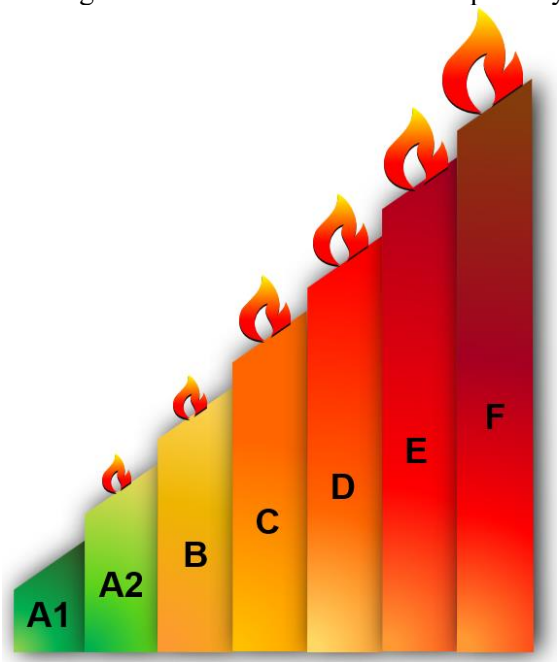


5. ábra: Födém füst konvektív hőátadása okozta átmelegedése
Forrás: Szerkesztette [18] nyomán a szerző

Illetőleg ezt követően felületen történő hőátadás, majd az azt követően az épületszerkezetekben hővezetéssel végbemenő hőtranszport a tűztől mentett oldalon elegendő idő

elteltével akár gyújtóhatást is gyakorolhat. Amely megint nagyon fontos összetevője a szilárdság megőrzésének. Azt hogy, milyen léptékű lesz ez a hővezetés az anyag szerkezetében vagy milyen ütemben és milyen nagyságú hőmérsékletek alakulnak ki, a szerkezet tűzállósága és ezzel szoros összefüggésben a már részben érintett szerkezeti kialakítás, és nem utolsó sorban az azokat alkotó építési termékek határozzák meg.

A szerkezetek kialakítására felhasznált építési termékek és elsődlegesen azok tűzvédelmi besorolását meghatározó anyaguk szabja meg. Ezért például a jelentősebb tűzkockázattal érintett épületeknél a tűzvédelmi szempontból kiemelt fontossággal bíró tűzgátló épületszerkezetek és tartószerkezetek nem éghető anyagú építési termékekből kell kialakítani. Az eltérő rendeltetés és egyéb tűzvédelmi kihatással bíró szempontoknak való megfelelés adekvát válaszainak megtalálásához meg kell határozni az építési termék tűzvédelmi sajátosságait. Ehhez szükséges a közösségi szinten szabványosított vizsgálati eljárásokkal minősített módszerekkel megállapított tűzvédelmi osztályba sorolás ad lehetőséget. Ez alapján a 6. ábrán látható fő kategóriák kerültek elkülönítésre az építő anyagok terén.

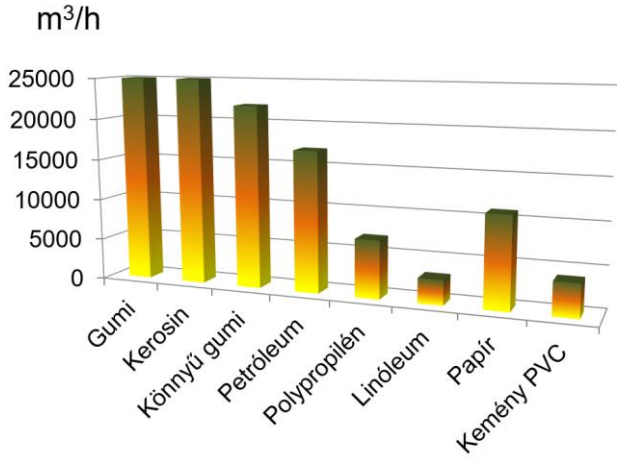


6. ábra: Építési termékek tűzvédelmi osztályba sorolásának vázlatos alapkategóriái
Forrás: Szerkesztette [19] nyomán a szerző

További kategorizálásra adnak lehetőséget az építőanyagként felhasznált anyagokból felszabadulható égéstermékek alkotta füst fejlődésének intenzitása. Ezek alapján elkülöníthetünk s1, s2, s3 rendre növekvő füstfejlesztőképességű anyagokat. Az ebből adódható veszélyhelyzetekre nézve szolgálhat adalékul egy raktárépület tűzeseti szimulációja során a füstterjedés kritikus időpillanatát kiragadó 7. ábra.

7. ábra: Raktárépületben terjedő füst láthatóságot befolyásoló hatása
Forrás: Készítette [20] alapján a szerző

Ahogyan az a 7-es ábra strukturális elrendezéséből is érzékelhető egy-egy munkahelyen a füst okozta kockázatok többnyire nem az épületszerkezetek füstfejlesztő képességéből adódnak, hanem az ott felhasznált, feldolgozott, tárolt anyagok égéséből. Az egyes technológiákban fellelhető néhány anyag füstfejlesztésének mértékét mutatja a 8-as ábra.



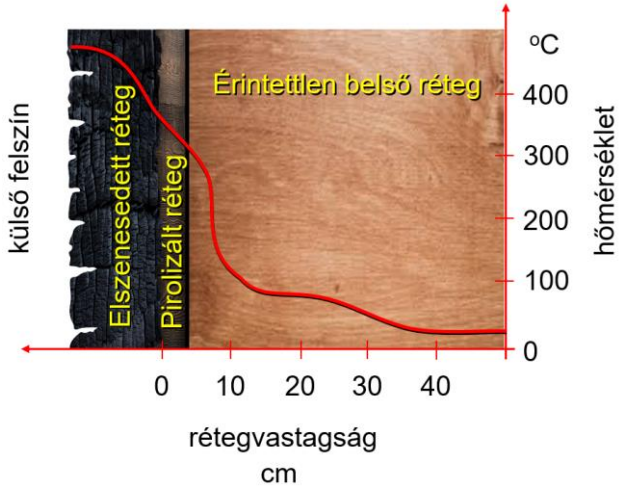
8. ábra: Néhány szilárd anyag füstfejlesztő képessége
Forrás: Szerkesztette [21] nyomán a szerző

Az éghető tűzvédelmi osztályú építési termékek szerkezeti anyagként történő alkalmazása tekintetében az egyik legelterjedtebb a fa. A lakóingatlanok és sport, illetve közösségi építmények mellett a fa a speciális építmények kivitelezésénél, illetve állványzatok összeállításánál gyakori, mint szerkezeti anyag. Munkahelyek kialakítása szempontjából kevésbe alkalmazott, azonban a paneles rendszerű könnyűszerkezettel készült, helyszínen szerelt ipari, mezőgazdasági csarnok jellegű építményeknél teherhordó faszerkezetek formájában mégis találkozhatunk velük. Emellett épületek fából készült fedélszerkezeteihez is gyakran alkalmazott szerkezeti anyag.

Tartószerkezeti célra történő alkalmazásuk éghető anyag lévén sajátos tűzvédelmi követelmények teljesítését teszik szükségessé, amelyet tűzhatásban mutatott sajátosságaiból vezethetünk le. Közelebbről a fa égésekor mutatott – éghető anyag lévén első hallásra furcsának ható - kedvező viselkedése az azt alkotó cellulóz molekulák termikus átalakulásának mechanizmusában keresendők.

A természetes formájában a fának, mint a cellulóz alapú építőanyagnak a beégésében hevítésekor kezdetben jelentős mennyiségű éghető, gáz halmazállapotú úgynevezett pirolizált bomlástermékeket szabadulnak fel. A bomlási folyamat következtében az éghető gázok felszínre törve bekapcsolódnak az ott zajló égési folyamatba. A pirolizált rétegben a termikus bomlási folyamatok lezárultával elszenesedett réteg marad vissza. A keletkezett faszén a rossz hővezetésének köszönhetően tovább fokozza a hőszigetelő hatást a mélyebben elhelyezkedő eredeti állapotú részek irányába. A farostok rossz hővezetési tényezőjének köszönhetően a belső részek irányába egyébként is igen lassan emelkedő hőmérséklet következtében a szerkezeti anyagok csak mérsékelt ütemben vesztenek szilárdságukból. Az előbbiekben jellemzett égési folyamatban létre jövő karbonizált réteg szigetelő hatását bizonyos égésgátló anyagok segítségével felgyorsítva, mesterségesen is előidézhetjük a faanyagnak a szigetelő hatás általi, tűzzel szembeni védelmet nyújtó folyamat lezajlását.

A lassú hővezetés ellenére azonban idővel ezek a még érintetlen rétegek is elérik bomlási hőmérsékletüket és megindul bennük a pirolízis. Így éri el a faanyag egyre mélyebb rétegeit az átalakulás, amint azt a 9-es ábrán is megfigyelhetjük. Az elvárt szilárdsági állapotok megtartása tehát a még tűzhatástól érintetlen belső keresztmetszetek nagyságától függenek. Vagyis a tűzállósági teljesítményt az úgynevezett beégési sebeség figyelembe vételével kell kalkulálni. Ez jellemzően a faanyag minőségétől függ. Az építési termékeknél használt nyers fenyő fűrész áruknál, mint faanyagnál ez az érték 0,6 mm/perc (tervezési értékként számolva: 1,0 mm/perc), a keményfáknál ez kisebb.



9. ábra: Fa anyagának beégési folyamata
Forrás: Szerkesztette: Mikkola [22] nyomán a Szerző

Megfelelő égéskésleltetés következtében a fa anyagát képező cellulóz bomlását kémiai úton fékező mechanizmus közbeiktatásával tovább csökkenthető a beégés folyamata.

Az ehhez szükséges vegyi anyagokkal a fa porózus szerkezetének köszönhetően igen eredményesen telíthető a felhasználni kívánt szerkezeti anyag. Az erre alkalmas technológiák közül az impregnálás folyamán az égésgátló szert valamilyen folyadékban oldatba áztatják az anyagot. Persze az oldatot más módon, például ecsettel is felhordhatják vagy rápermetezik a fa felületére.

A fa impregnálása során égéskésleltetés történhet oltógázokat fejlesztő anyagok segítségével, de egyéb fizikai módon is gátolható a faanyagok hővel szembeni ellenállósága. A már említett kedvező hőszigetelő hatás növelhető hő hatására a felületen elszenesedést kiváltó anyagokkal való impregnálás útján is, illetőleg a fa felszínén olvadékként a felszínre törő bomlástermékek útját elzáró anyagokkal is.

Ezen felül neméghető anyagokkal való mechanikus eltakarás is szóba jöhet, ott, ahol a látszó faszerkezetek esztétikai előnyeit nem kívánják érvényesíteni, például az épület gépészeti rendszereit rejtő belső terekben, vagy a fedélszékekben. A tűzállóságot fokozó elburkolás történhet tűzgátló gipszkarton vagy szilikátalapú hőszigetelő anyagok felhasználásával.

Az ipai csarnoképületeknél megszokott nagy térbeli dimenziókat magában foglaló térelhatárolással történő munkakörnyezeti kialakítás. Az ilyen technológiákban alkalmazott nagyobb termelési volumenekkel együtt jelentős felhasznált, feldolgozott és kezelt anyagmennyiségek jelenlétével jár együtt egy adott technológiai térben. Az ipari céllal felhasznált anyagok általában fokozott éghetőségi jellemzőkkel párosulva drasztikusan megnövekedtek tűzveszélyt eredményeznek a létesítmények ezen részeiben.

Ugyanakkor bármely munkakörnyezetről legyen is szó, a termelési tevékenységtől markánsan eltérő, kiszolgáló és adminisztratív, logisztikai munkafolyamatoknak helyet adó funkciók a legtöbb esetben a tűzkockázatokban is visszatükröződnek. Így a tűzbiztonság magasabb fokú garantálása érdekében valamiféle tűzvédelmi elkülönítésük indokolt. A létesítmények tűzvédelmi strukturálásánál a legegyszerűbb megoldást kínáló alapelvként alkalmazzák egyazon tűzszakaszban való létesítést. A helykihasználás és a megkerülhetetlen technológiai kapcsolódások, valamint a veszélyes technológiákban üzembiztonsági okokból alkalmazandó védőtávolságok megtartása miatt általában több tűzszakaszba integrálható kockázati egységek csoportjait fogjuk tudni azonosítani. Az ezeket egymástól elválasztó épületszerkezeteket vagy képzeletbeli határvonalakat tűzszakaszhatároknak nevezzük. Ezek jelentőségét az adja, hogy a kialakulható tűzesetek más tűzszakaszokra való átterjedését és ez által nagyobb tűzveszély bekövetkezését megakadályozandó valamennyi tűzterjedést szolgáló passzív és aktív tűzvédelmi megoldást ehhez illeszkedően alakítunk ki.

A tűzszakasz határokon az elmondottakból eredően az egyéb pusztán csak térelhatároló funkcióval rendelkező épületszerkezetektől eltérő tűzeseti viselkedést mutató tűzgátló épületszerkezeteket alkalmazunk. Az ezekkel szemben támasztott tűzállósági követelményeket kielégítő teljesítményjellemzők leírására bevezetett paraméterek a szerkezetek várható tűzhatásban történő viselkedéséhez köthetők. Az erre példaként vett A1REI 60 – ként megadott tűzgátló szerkezet teljesítménymutatójának értelmezését a 10. ábra szemlélteti.

10. ábra: Tűzgátló szerkezet egyes teljesítménymutatójának alapértelmezése
Forrás: Szerkesztette [23] nyomán a szerző

A tűzállósági teljesítmény értékét követő számérték valamennyi teljesítményjellemzőre egyaránt vonatkozó időtartamot jelöli percekben kifejezve. Vagyis az A1 nemégthető anyagból kialakított tűzgátló térelhatároló funkciót betöltő és REI 60 paraméterrel jellemzett szerkezet az őt érő tűzhatás során teherhordó képessége (R) következtében a rá nehezedő terheket, a szerkezeti integritását (E) a láng áttörését lehetővé tevő átmenő rések megjelenése nélkül, valamint a szigetelő képességét (I) a mentett oldalon gyújtó hatást kiváltani képes hőmérsékletre történő átmelegedés nélkül megtartja legalább 60 percig.

A tűzvédelmi minősítésük alapján eltérő tűzeseti viselkedéssel számolhatunk az egyes építési termékeknél. A nem éghető szerkezeti anyagokkal történő építési technológiák terén kiemelt szerepet tulajdoníthatunk a könnyűszerkezetes építési módnak, amely igen elterjedtté vált az különféle technológiai rendszerek létesítési eljárásaiban. Köszönhetően az ezeknél alkalmazott építési rendszereknek, valamint a korszerű építési anyagok felhasználásának, a modern gyártástechnológiával könnyű teherhordó és térelhatároló épületszerkezetek alakíthatók ki. Az alkalmazás leggyakoribb eseteivel az ipari, mezőgazdasági, logisztikai raktározási, és kereskedelmi jellegű létesítmények esetében találkozhatunk.

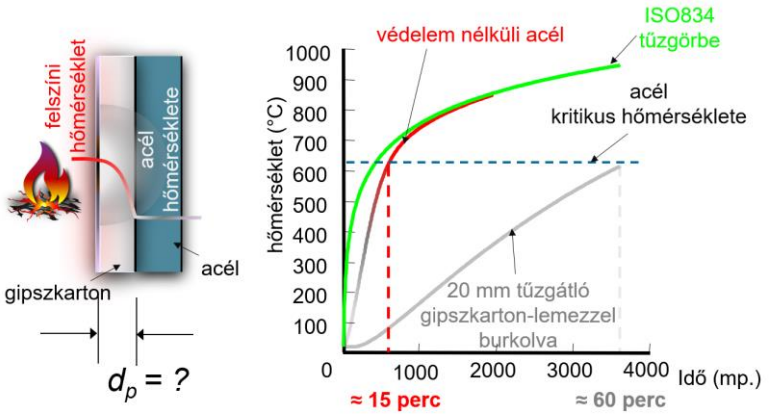
Tűzvédelmi létesítési követelmények oldaláról a könnyű acélszerkezetek alkalmazásával létesülő építmények tűzeseti szerkezeti szilárdsága jellemzőinek megfelelőségén túl ugyancsak számolni kell a szerkezeti anyagok hőtani fizikai jellemzői okozta sajátosságokkal. Ezért nem elegendő pusztán a nem éghetőség nyújtotta látszólagos biztonságra alapozni a tűzeseti hatások precíz megítélésében.

A könnyűszerkezetes építési módszerrel létesülő építmények tűzeseti szerkezeti szilárdságának további fontos aspektusát adja, hogy valamennyi épületgépészeti, stb. rendszer kiépítéséhez is ezek adják a megfelelő strukturális alapot. Azaz az azok rögzítő elemeinek installálásában is ezek képezik az eredendő szerkezeti állékonyságot. Tehát valamennyi tűzvédelmi követelményekkel rendelkező rögzítő elemmel való fizikai kapcsolatnál érvényesülnie kell a tűzállósági teljesítmények összhangjának. Sem egyik, sem másik nem gyengítheti az előírások szerint kialakított tűzállóságot. Ez értelemszerűen vonatkozik az aktív tűzvédelmi rendszerekkel alkotott szerkezeti kapcsoltokra és az azok tűzeseti vezérlésében lényeges kábelek funkcióinak megtartására is, melyek sajátosságaira a későbbiekben még kitérek.

Azonban a tűz, magától értetődően megfelelően tartós kölcsönhatás esetén, bármely épületszerkezet tönkremenetelét is előidézheti. Az ezt befolyásoló állapotok elérésének kivédését a szerkezet anyagának megválasztásán túl egyéb passzív védelmet fokozó anyagok hozzáadásával jelentősen módosíthatjuk, ami a szerkezeti tűzállóság növelését jelenti.

Annak ellenére, hogy az acélszerkezetek nem éghető anyagúak és nagy szilárdságúak, a tűz hatására már relatíve alacsony hőmérsékletek, mintegy 620 °C-on jelentős szilárdságvesztést szenvednek el és ennek nyomán eldeformálódva szerkezeti funkciójukat nem lesznek képesek betölteni. Tehát ennél nagyobb tűzállósági teljesítményt igénylő épületek kivitelezésére, csak megfelelő kiegészítő védelmet adó módszerek felhasználásával lesznek alkalmasak. Az ilyen nagyobb szerkezeti állékonyságot megkövetelő épületekben az alapesetben nagyságrendileg mintegy 15 perces tűzállóságú acélt kiegészítő védelemmel kell alkalmazni. Ezt elburkolással, hőre habosodó festéssel vagy szórással felvitt tűzgátló habarcs jelentette kiegészítő védelemmel érhetjük el. A tűzvédő festékeket olyan esetekben célszerű alkalmazni, amikor az elérni kívánt tűzállósági teljesítmény nem túl magas, valamint a szerkezet bonyolultsága például rendkívül körülményessé tenné annak elburkolással történő védelmét. Az acélszerkezetek a tűzállóságának fokozását meglehetősen kis rétegvastagságban felhordott (szórással, festéssel), de tűz esetén jelentős, jellemzően több nagyságrenddel nagyobb vastagságúra felhabosodó védőréteggel érhetjük el. Az akár a helyszínen is elkészíthető és száradása után 0,3-1 mm festékrétegben található komponensek a tűzfejlődés eredményezte hőmérsékletnövekedés hatására bomlást szenvednek el, majd a tovább emelkedő hőmérséklet következtében a megduzzadó anyagot felhabosítva elzárják a szerkezetet a közvetlen tűzhatástól és hősugárzástól.

Elvi megfontolásait illetően hasonlóan a tűzvédő festék felhabzása jelentette szigetelő hatáshoz, a szükséges tűzállósági teljesítmény elérhető megfelelő, a közvetlen tűzhatástól védő és viszonylag kis rétegvastagságú tűzgátló képességű szilikát alapú anyagokkal kialakított szórt bevonatokkal, például tűzgátló habarccsal. Ugyanakkor egyéb neméghető anyagok felhasználásával tűzvédő réteget vonhatunk az acélszerkezet köré. Az így kialakított például gipszkarton hőszigetelő rétegekkel elburkolva a szerkezeti anyagokat hatásosan növelhető a tűzállóság. Ennek egyik példáját láthatjuk a 11-es ábrán.



11. ábra: Hőszigetelő burkoló réteg tűzállósági teljesítményre gyakorolt hatása acél esetében
Forrás: Szerkesztette [24] nyomán a szerző

Az így nagyobb tűzállósági teljesítményt elérni képes szerkezetek kivitelezésénél a védelmet fokozó rétegek sérülésmentes beépítésére, illetve a tűzálló bevonatok helyszíni felhordási technológiával történő egyenszilárdságú védelem kiképzésére kiemelt figyelmet kell fordítani. A védőrétegek kialakításakor nagyfokú technológiai fegyelmet kell megkövetelni, mivel bármilyen folytonossági hiba tűzhatásban nemvárt módon és végzetesen felgyorsíthatja a tönkremenetelt súlyos veszélyeztetést előidézve a bent tartózkodókra. Különösen igaz ez a tűzálló festékrétegekre. Ezekkel a szerekkel történő kezelése a szerkezeti anyagoknak nagyobb stabilitást, hosszabb ellenállóképességet biztosít a tűzzel szemben. Szaknyelven szólva megnövekedett tűzállósági teljesítményt kölcsönöz számukra. [25]

Az ilyen jellegű ipari létesítményekben másik fontos tűzvédelmi veszélytényező a tetőszinti tűzterjedés. Viszonylag gyakori eset a kiterjedt ipari tűzeseteknél a tetőszinten történő tűzterjedés, ezzel együtt a tetőhéjalás gyors tönkremenetele. Ezek kivédése céljából fontos a csarnoképületeknél a héjszerkezeteik védelme. Ezeket jellemzően trapézlemezekből alakítják ki, amelyek tetőszinti tűzterjedés elleni védelme, olyan neméghető szigetelő anyagokkal, mint a kőzetgyapot, jelentősen fokozható. Emellett alkalmaznak sprinklerrendszereket is a szerkezet tűzeseti hűtésére.

Hasonlóan lényeges eleme ennek az építési technológiának a külső térelhatároló szerkezeteknél alkalmazott szendvicspanelek, melyek külső fém fegyverzeteiknek köszönhetően a tűztávolságok tartásával együtt meghatározó szerepet töltenek be a technológiai épületek közötti tűzterjedésben. Ezen építési technológia lapvető felhasználási területeit az ipari, mezőgazdasági, illetőleg a közösségi és kereskedelmi jellegű létesítmények, valamint a logisztikai raktárak képezik. Tűzvédelmi oldalról a viszonylag alacsony tűzeseti szerkezeti állékonyság jelentette biztonsági hátrányaik a viszonylag jelentős léptékű beépített aktív tűzvédelmi rendszerek egyidejű létesítésével kompenzálhatók. Ugyanakkor egyes tűzesetekben előállhatnak nem várt helyzetek, mint például éghető zsíros, olajos gőzök bediffundálása a fegyverzeten belülre és ott kondenzálódva, lerakódva a technológiai terekben kitört tűz során szintén meggyulladhatnak. Ezek oltása ellenben rendkívül nehéz és csak a szerkezet megbontásával kísérelhető csak meg.

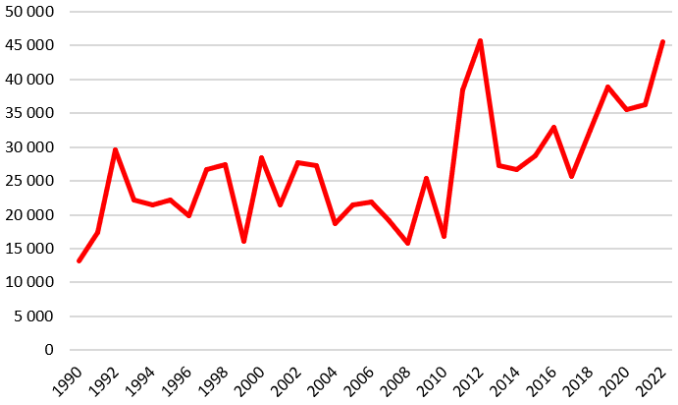
KÖVETKEZTETÉSEK

A tapasztalatok az mutatják, hogy az anyagi károk nagyságrendjének tekintetében élenjáró tényező a tűzesetek. Ráadásul amint azt a 12-es ábra is szemlélteti az 1990-es években szintet váltott. [26] Sőt ezek száma a 2012. utáni átmeneti jelentős csökkenést követően 2017-től újra drasztikusan emelkedni kezdett.

A munkahelyeken a tűzek kiváltó okai között – a vis maior eseteket nem számítva – a tűzbiztonsági előírások be nem tartása előkelő helyen szerepel. Az ezek keletkezésének kockázatait vizsgálva megállapítható, hogy a tűzveszélyesség szempontjából a tűzesetek másik fő tényezője a technológiai folyamatokhoz köthetően a munkaeszközök, berendezések szabálytalan keletkezése. [28]

Épp ezért a munkahelyi tűzmegelőzésnek továbbra is meghatározó szerepet kell kapnia a passzív tűzvédelem hatékonyságát alapvetően befolyásoló létesítési előírások épületszerkezetekre vonatkozó követelményeinek. Különösen pedig a nagy volumenű ipari és mezőgazdasági termelés és alapanyag-felhasználás feltételei között jelentkező fokozódó tűzveszélyre adandó válaszoknak. Ideértve a tűzesetek jelentette káresemények következményeinek sikeres felszámolásának esélyét megteremtő aktív tűzvédelmi berendezéseket és

ezeknek a szerkezetkre való megbízható installálását. Az ehhez a munkahelyeken alapot adó stabil épületszerkezetek nem csak a munkavállalók menekülése biztonságossá tételének igen fontos elem, de a beavatkozó tűzoltó állomány védelmét is szolgálják mentési munkák során. Az idő előtt összeomló égő épületekből a sérültek felkutatása és kimentése és a tűz oltása szilárd szerkezetek nélkül elképzelhetetlen még a legkorszerűbb tűzoltó technika segítségével is.



12. ábra: Tűzesetek számának alakulása
Forrás: Szerkesztette [27] nyomán a szerző

REFERENCES

[1] Tanács Irányelv (89/391/EGK) a munkavállalók munkahelyi biztonságának és egészségvédelmének javítását ösztönző intézkedések bevezetéséről, I. melléklet, 2. pont;
[2] Beda L.: Tűzmodellezés és tűzkockázat elemzés, Ybl Miklós egyetemi jegyzet, 1999.;
[3] SPELLMANAND F. R. & BIEBER R. M., Chemical Infrastructure Protection and Homeland Security, THE SCARECROW PRESS, INC., 2009., ISBN 978-1-59191-945-2, 149. o.;
[4] Kemencés József: Nyomástartó berendezések biztonságtechnikája, OMKT Kft, Budapes, 2010. ISBN 978-963-89258-2-0, 96. o.;
[5] Fölkl R. et al.: Munkaegészségügyi és Munkavédelmi Enciklopédia, Budapest 1987., 1. kötet, ISBN 963-592-433-X, 2653. o.;
[6] Thomson N., Fire Hazards in Industry, Butterworth-Heinemann, Woburn, 2002., ISBN 0 7506 5321 3, 21. o.;
[7] Csőke Béla: Biztosítási ismeretek - utazás a kockázatok kezelésének gyakorlatában, egyetemi jegyzet, Budapest, Óbudai Egyetem, 2012., 57. o.;
[8] Beda L., Épületek tűzbiztonságának műszaki értékelése ZMNE Doktori (PhD) értekezés, 2004.;
[9] Sárosi Gy., Veszélyes áru raktárlogisztika - korszerű követelmények. Budapest, 2006. Complex Kiadó, ISBN 963-224-869-1, 116. o.;
[10] Horváth L., Kulcsár B., Lublóy É., Sas V., Vígh L.G., Tartószerkezetek méretezése tűzhatásra. Magyar Mérnöki Kamara, 2010.;

[11] Takács L., Tűzvédelmi burkolatok helyes szemléletű kialakítása Harmathy szabályainak elemzésével, Tanulmány, Védelem online, https://www.vedelem.hu/letoltes/anyagok/448-tuzvedelmi-burkolatok-helyes-szemleletu-kialakitasa-harmathy-szabalyainak-elemzesevel.pdf, (letöltve: 2024. január 31.)
[12] EN 1992-1-2 (2004), Eurocode 2: Design of concrete structures - Part 1-2: General rules - Structural fire design [Authority: The European Union Per Regulation 305/2011, Directive 98/34/EC, Directive 2004/18/EC;
[13] Majorosné Lublóy É. et al.: Méretezés tűzteherre az Eurocode szerint – Vasbeton, acél-, fa-, falazott és öszvérszerkezetek tervezése, TERC Kereskedelmi és Szolgáltató Kft., Budapest, 2023., ISBN 9786155445941, 6. o.;
[14] Bánky Tamás et al: Építési termékek megfelelősége, Terc Kereskedelmi és Szolgáltató Kft., 2005., ISBN 963 9535 29 X, 179. o.;
[15] TvMI 11.3:2022.06.13. Építményszerkezetek tűzédelmi jellemzői, B melléklet - Tűzhatás kitéti görbéi, 65. o.;
[16] Kruppa Attila: Villamos vezetékrendszerek tűzvédelme, OBO Bettermann Kft., 2013., 24. o.;
[17] Morgan J. Hurley, et al, SFPE Handbook of Fire Protection Engineering, Greenbelt, MD, USA 2016., ISBN 978-1-4939-2565-0, 790. o.;
[18] InfoGraph GmbH, Software for Structural Design, Fire Scenario for a Composite Frame, Temperature profiles of the used sections at time t=90 min, https://www.infograph.eu/en/fire-scenario-for-a-composite-frame, (letöltve: 2024. 02. 02.)
[19] Insulation4less Ltd, Fire-resistant insulation, https://insulation4less.co.uk/collections/insulation, (letöltve: 2024. 02. 02.);
[20] Kulcsár B., Tűzmodellezés és Tűzkockázat-elemzés, félévi gyakorlati feladatkiírás, FDS és PyroSim szoftver felhasználásával, 2014.;
[21] Pál Károlyné - Macskásy H.: A műanyagok éghetősége. Műszaki Könyvkiadó, Budapest, 1980., ISBN 963-10-3179-9, 251. o.;
[22] E. Mikkola: Charring of wood based materials, Fire Safety Science, 3 (1991), pp. 547-556, 10.3801/iafss.fss.3-547, https://publications.iafss.org/publications/fss/3/547/view/fss_3-547.pdf, (letöltve: 2023. 12. 08.);
[23] Diana Helmerking: Basics Fire Safety, Birkhäuser Verlag GmbH, Basel, 2020., e-ISBN (PDF) 978-3-0356-1936-2, 21. o.;
[24] Iványi M., Acélszerkezeti tervezés az EUROCODE 3 szerint, Acélszerkezetek (klsz.) Acélszerkezetek Tűzvédelme, 2008., ISSN: 1785-4822, 23. o.;
[25] Jármai K., - Iványi M., Acélszerkezetek tűzvédelmi tervezése, Bevezetés az acélszerkezetekkel kapcsolatos európai szabványokba és alkalmazásukba, Gazdász-Elasztik Kft., Miskolc, 2008., ISBN 978-963-87738-4-5, 134. o.;
[26] Vajda Gy.: Kockázat és Biztonság, Akadémia Könyvkiadó, 1998., ISBN 963-05-7493-4, 56. o.;
[27] Központi Statisztikai Hivatal: 4.1.1.43. Munkabalesetek, otthoni balesetek és tűzesetek, https://www.ksh.hu/stadat_files/ege/hu/ege0042.html, (letöltve: 2024. 02. 03.).;
[28] Haubert Gábor: A munkahelyi kockázatértékelés és -kezelés gyakorlati kézikönyve, Munkavédelmi Kutatási Közalapítvány, Budapest, 2003, ISBN: 963-206-499-2, 118. o.;

Follow, like, post, publish! | Kövess, lájkolj, posztolj, publikálj!

https://biztonsagtudomanyi.szemle.uni-obuda.hu

https://www.linkedin.com/company/safety-and-security-sciences-review

https://www.facebook.com/biztonsagtudomanyi.szemle