ISSN 2676-9042

Vol 6, No 4, 2024.

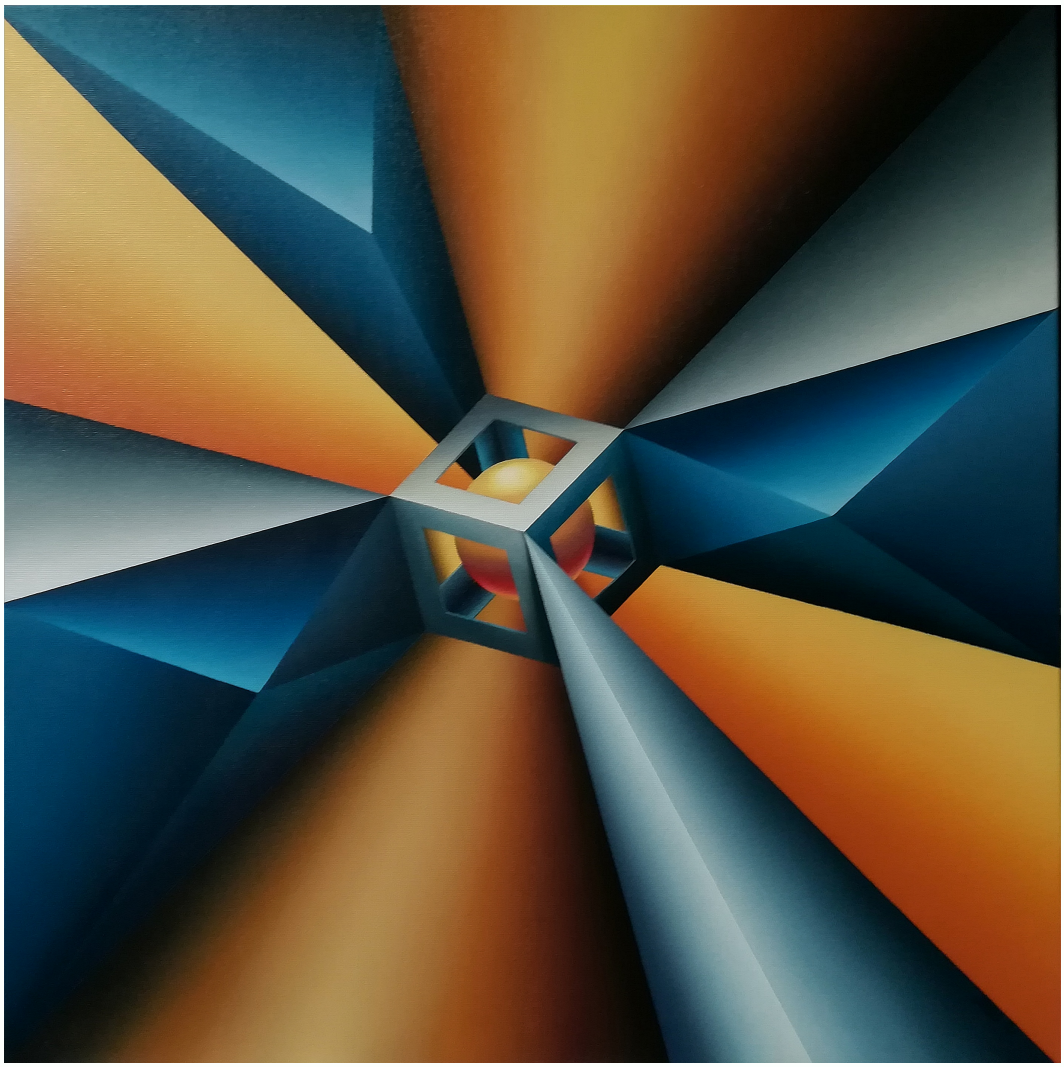
2024, VI. évf. 4. szám

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
Birth of light painting | **Fény születése** 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 4, 2024. | **2024. VI. évf. 4. szám**

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

BALOGH Attila

balogh.attila@kgk.uni-obuda.hu

Attila BALOGH holds a degree in Agricultural Economics and Engineering, is a certified English-Hungarian translator and earned an Executive MBA through a dual US-Hungarian program. He was the first Hungarian graduate of the MITx MicroMasters Program in Supply Chain Management. Works 25 years in IT and telecommunications, including 20 years in senior leadership roles at IBM, EMC, T-Systems Hungary, and private firms. He is now a professional investor and entrepreneur, a PhD student at Óbuda University's Doctoral School of Innovation Management and an assistant lecturer at the Keleti Károly Faculty of Business and Management. His research focuses on corporate innovation management and the intersection of emerging technologies and business models. Mr. Balogh is a founding member, strategic leader, and mentor of the Mind Mate Inspiration Association. As a University of Rhode Island (US) graduate, he serves as a Global Alumni Ambassador and a Member of its Alumni Engagement Council.

BALOGH Attila okleves gazdasági agrármérnök, angol-magyar szakfordító, amerikai-magyar duális képzésű Executive MBA diplomával is rendelkezik. Az MITx MicroMasters in Supply Chain Management képzés első magyar végzett hallgatója. 25 éve a magyar és nemzetközi informatikai és telekommunikációs területen dolgozik, ebből 20 évet felsővezetőként töltött, saját tulajdonú cégek és multinacionális cégek (IBM, EMC és T-Systems Magyarország) menedzsment tagjaként. Jelenleg szakmai befektető és saját cégeinek vezetője. Az Óbudai Egyetem Innováció Menedzsment Doktori Iskolájának PhD hallgatója, a Keleti Károly Gazdasági Kar tanársegédje. Főbb kutatási területei a vállalati innovációmenedzsment, az új technológiák és üzleti modellek kapcsolatai és lehetőségei. A Mind Mate Inspiration Egyesület alapító tagja, stratégiai vezetője és mentora. A University of Rhode Island (US) végzett hallgatójaként Global Alumni Ambassador és az Egyetem Alumni Engagement Council-jének tagja.

CSISZÁRIK-KOCSIR Ágnes

kocsir.agnes@kgk.uni-obuda.hu

Ágnes CSISZÁRIK-KOCSIR Ph.D., Associate Professor at the Keleti Károly Faculty of Economics, Óbuda University. Prior to her university career, she was responsible for the financial management of several EU-funded projects in addition to her general project management tasks. He has been working at the predecessor institution of Óbuda University since 2007, first as a teaching assistant, later as an assistant professor. Since 2013 he has been an associate professor at the Keleti Károly Faculty of Economics at Óbuda University. Hirsh index 23. Member of the editorial board of several professional associations, national and international journals, editor and member of the scientific and organizing committee of several national and international scientific conferences. He is a committed advocate of project thinking and building financial, digital and consumer awareness, as evidenced by his research.

Dr. habil. CSISZÁRIK-KOCSIR Ágnes az Óbudai Egyetem Keleti Károly Gazdasági Karának egyetemi docense. Egyetemi munkássága előtt számos Európai Unió által finanszírozott projekt pénzügyi menedzsmentjét látta el az általános projektvezetői feladatok mellett. Az Óbudai Egyetem jogelőd intézményében 2007 óta dolgozik először tanársegédként, később adjunktusként. 2013-tól az Óbudai Egyetem Keleti Károly Gazdasági Karának egyetemi docense. 2017-ben habilitált, 2018-tól intézetigazgatóként, 2020-tól pedig a Kar kutatási dékánhelyetteseként dolgozik. 2004-től az MTMT-ben a mai napig rögzített publikációinak száma több, mint 600. Hirsh-indexe 23. Több szakmai szervezet, hazai és nemzetközi folyóirat szerkesztőbizottságának tagja, lektora, valamint több hazai és nemzetközi tudományos konferencia tudományos és szervezőbizottságának tagja. Elkötelezett híve a projektszemélet és a pénzügyi, digitális és fogyasztói tudatosság építésének, amit kutatási is igazolnak.

DÉR Attila

der.attila@uni-obuda.hu

Attila DÉR is a student at the Doctoral School of Safety 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 Faculty of Electrical of engineer. His research interests include cybersecurity, protection of critical infrastructures in particular energy supply.

DÉR Attila az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán lévő Biztonságtudományi Doktori Iskola hallgatója. Okleveles vil-lamosmérnöki végzettségét a Kandó Kálmán Villamosmérnöki Karán szerezte Ipari felügyeleti és kommunikációs rend-szerek specializációján. Kutatási területei a kiberbiztonság, kibervédelem, kritikus infrastruktúrák védelme különös tekintet-tel az energiaellátásra.

ELEK Barbara

elek.barbara@bgk.uni-obuda.hu

Barbara ELEK is a geophysical environmental engineer, fire protection engineer. She is an associate professor at the Institute of Safety Science and Cybersecurity of the Donát Bánki Faculty of Mechanical and Safety Engineering of Óbuda University. She is the head of training of the faculty's EHS engineer and specialist training. Lecturer and supervisor of the university's Doctoral Scholl on Safety and Security Sciences. Her research areas are: fire and explosion protection, safety issues of vital energy systems and facilities, environmental safety.

ELEK Barbara okl. környezet-geofizikusmérnök, tűzvédelmi szakmérnök. Jelenleg az Óbudai Egyetem Bánki Donát Gépész- és Biztonságtechnikai Mérnöki Kar Biztonságtudományi és Kibervédelmi Intézetében egyetemi docens, valamint a kari EHS szakmérnök és szakember képzés képzésvezetője. Az egyetemi Biztonságtudományi Doktori Iskola oktatója, témavezetője. Kutatási területei: tűz – és robbanás elleni védelem, energetikai létfontosságú rendszerek és létesítmények biztonsági kérdései, környezetbiztonság.

KERTAI-KISS Ildikó

kertai.kiss.ildiko@gmail.com

She has been working in organization and management science since 2008, including in the consulting industry (organizational development, organizational diagnostics, leadership development, mentoring) and in higher education for more than 10 years as an applied psychologist, university lecturer and supervisor. As a PhD student at the PhD School of Safety and Security Science, University of Óbuda, since 2014, he has been working on functional issues of safety in socio-technical systems (management and organization science), safety culture, organizational behaviour, risk analysis of organizational processes and the organizational background of human error. In addition to teaching and research, he is a member of the research group of the Society of Informatics Economy at Óbuda University and a member of the board of the Culture-Economy Section of the Hungarian Economic Society. In her free time he sings in the Budapest Academic Choir and performs in orchestral productions.

Szervezés-és vezetés tudománnyal 2008. óta foglalkozik, ezen belül a tanácsadó iparban (szervezetfejlesztés, szervezeti diagnosztika, vezető fejlesztés, mentoring) és a felsőoktatásban több, mint 10 éve dolgozik, mint alkalmazott pszichológus, egyetemi oktató és szakfelelős. Mint az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD-hallgatója, 2014-től, a szocio-technikai rendszerek biztonságának funkcionális kérdéseivel (vezetés- és szervezés tudomány), biztonsági kultúrával, szervezeti magatartással, a szervezeti folyamatok kockázatainak elemzésével és az emberi hibázás szervezeti hátterével foglalkozik. Az oktató és kutató munka mellett, tagja az Óbudai Egyetem Társadalom Informatika Gazdaság, kutató csoportjának, valamint a Magyar Közgazdasági Társaság Kultúra-gazdaság szakosztályának elnökségi tagjaként végez társadalmi munkát. Szabadidejében a Budapesti Akadémiai Kórusban énekel, zenekari produkciókban lép fel.

KOLEJANISZ Márk

mark@kolejanisz.hu

Dr. Márk KOLEJANISZ is a lawyer, founded Kolejanisz Legal Office in 2016. He gratuated at Eötvös Loránd University Faculty of Law with summa cum laude. He speaks English, German and Greek. At the university, he led an active academic life, winning the National Science Student Competition in 2004. He worked in the public administration, in the Parliament and in various ministries, as well as in the corporate world as a public law consultant. He was the legal advisor of the Hungarian Tire Association for several years after its foundation. His areas of expertise are data protection and digital law, along with the law of civil organizations, in which field the book 'Guide to Civil Law' had been published, which he co-authored. The Kolejanisz Legal Office has been a gold level supporter of the Magyar Élelmiszerbank since 2014.

Dr. KOLEJANISZ Márk ügyvéd, a Kolejanisz Ügyvédi Irodát 2016-ban alapította. Az Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Karán jogász végzettséget szerzett summa cum laude minősítéssel. Angolul, németül és görögül beszél. Az egyetemen aktív közösségi tudományos életet élt, Országos Tudományos Diákköri versenyt nyert 2004-ben. Dolgozott a közigazgatásban, az Országgyűlésben és különböző minisztériumokban, illetve a vállalati világban közjogi tanácsadóként. A Magyar Gumiabroncs Szövetség jogi tanácsadója volt a megalapításától éveken keresztül. Szakterületei az adatvédelmi és digitális jog, valamint a civil szervezetek joga, utóbbi témában jelent meg az Útmutató a Civil törvényhez című munka, melynek társszerzője. A Kolejanisz Ügyvédi Iroda a Magyar Élelmiszerbank arany fokozatú támogatója 2014 óta.

KOLLÁR Csaba

kollar.csaba@uni-obuda.hu

Csaba KOLLÁR is a communications engineer, certified communications specialist, electronic information security manager, doctor of economics (PhD), and doctor (PhD) and habilitated doctor (Dr. habil.) in military engineering. He is also a cybernetics consultant, coach, and mediator. His research interests include the social aspects and economic impacts of the digital age, with a particular focus on the human aspects of information security, information security awareness, human-robot interaction, smart cities, artificial intelligence, social credit systems, and domotics. He is a senior research fellow at Óbuda University, where he leads the specialized courses for Domotics Engineer/Consultant and Facility and Property Professional Engineer/Manager. He is also the head of the Artificial Intelligence Workshop and serves as the 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. Csaba KOLLÁR is an expert with the Hungarian Society of Military Science and the National Association of Human Professionals, and has been a 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 doktora (PhD) és 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/szaktanácsadó és a létesítménygazdálkodó és -üzemeltető szakmérnök/szakmenedzser 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. A Magyar Hadtudományi Társaság és a Humán Szakemberek Országos Szövetsége szakértője. 2018. negyedik negyedévétől a Mesterséges Intelligencia Konzorcium tagja.

MÁRTON Zoltán

marton.zoltan@uni-obuda.hu

Zoltán MÁRTON is the head of the STEAM Office at Obuda University and serves as the Platform Coordinator of the Hungarian STEM Platform. He holds degrees in safety technology engineering and engineering education, and he is currently pursuing his PhD in Security and Safety Sciences at Obuda University. His professional and research focus centers on STEAM-based curriculum development, skill-building for cyberspace-based protection strategies, and innovative, digitally supported teaching methods. He has been actively involved in coordinating and leading several international projects, including Erasmus+ initiatives and projects focused on digital skills, STEAM education, and gamified learning experiences. Through these roles, he contributes to advancing interactive and safety-focused educational content in Hungary and beyond.

MÁRTON Zoltán az Óbudai Egyetem STEAM Irodájának vezetője és a Magyarországi STEM Platform koordinátora. Biztonságtechnikai mérnöki és mérnökpedagógiai diplomával rendelkezik, jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában hallgató. Szakmai és kutatási fókuszában a STEAM-alapú tananyagfejlesztés, a kibertér-alapú védelmi stratégiák készségfejlesztése és az innovatív, digitálisan támogatott oktatási módszerek állnak. Aktívan részt vett több nemzetközi projekt koordinálásában és vezetésében, többek között Erasmus+ kezdeményezésekben és a digitális készségekre, a STEAM-oktatásra és a játékosított tanulási tapasztalatokra összpontosító projektekben. E szerepkörök révén hozzájárul az interaktív és biztonságközpontú oktatási tartalmak fejlesztéséhez Magyarországon és azon túl is.

MÉSZÁROS Ádám

meszaros.adam@uni-obuda.hu

Ádám MÉSZÁROS is a certified economist majoring in business development, a technical manager, holds an Executive MBA degree and a sign language interpreter qualification. He has been working in the IT field for 8 years, in the roles of project manager, scrum master and product owner. He is currently the managing director and head of product development of a Hungarian IT company developing medical software. He has several years of experience and international certificates in the field of Agile and Scrum. He is a PhD student at the Doctoral School of Security Studies of Óbuda University and a teaching assistant at the Károly Keleti Faculty of Economics. His main research area is the relationship between psychological safety and teamwork based on the agile project approach.

MÉSZÁROS Ádám okleveles közgazdász vállalkozásfejlesztés szakon, műszaki menedzser, Executive MBA diplomával és jelnyelvi tolmács végzettséggel rendelkezik. 8 éve informatikai területen dolgozik, projektmenedzser, scrum master és product owner szerepkörökben, jelenleg egy orvosi szoftvereket fejlesztő magyar informatikai vállalkozás ügyvezetője és termékfejlesztési vezetője. Az Agile és a Scrum területén több éves tapasztalattal, nemzetközi tanúsítványokkal rendelkezik. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD hallgatója, a Keleti Károly Gazdasági Kar tanársegédje. Főbb kutatási területe a pszichológiai biztonság és az agilis projektszemlélet alapú csapatmunka kapcsolatai.

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.

MORVAY László (1967) villamos-üzemmérnök orvostechnikai ágazaton (KKVMF, 1989) és 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

Contract tender assessor 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).

Kutatási, Fejlesztési és Innovációs Hivatal szerződéses pályázati bírálója. 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 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 Országos 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.

RAJNAI Zoltán

rajnai.zoltan@bgk.uni-obuda.hu

Dr. Zoltán RAJNAI is currently the National Cyber Coordinator of Hungary and professor at the Obuda University. Previously Dr. Rajnai served as Colonel in Hungarian Defense Forces (1981-2013) and was professor at the National Defense University in the field of Information, info-communication, and telecommunication systems (1993-2013). Since 2013, Dr. Rajnai also is the Dean of faculty of Mechanical and Safety Engineering, Head of Doctoral School on Safety and Security Sciences with main responsibilities in the field of Cyber Security, Information Security, info-communication, and telecommunication systems. Dr. RAJNAI received education from the High School at the Hungarian Defense Forces (1981-1985), the Military Academy (1990-1993), the Doctoral School on Military Sciences (1997-2000), and the Joint Security College- Paris, France (2003-2004).

Prof. Dr. RAJNAI Zoltán Magyarország nemzeti kiberkoordinátora, az Óbudai Egyetem professzora, 2015-tól az Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karának dékánja. A Biztonságtudományi Doktori Iskola alapítója, vezetője, kutatási területe a kiberbiztonság, az információbiztonság, az infokommunikáció és a távközlési rendszerek fejlesztése. Korábban (1981–2013) ezredesként szolgált a Magyar Honvédségben, 1993–2013 között a Zrínyi Miklós Nemzetvédelmi Egyetem tanáraként fő szakterülete az információs, kommunikációs és távközlési rendszerek szervezése és azok biztonsága volt. RAJNAI professzor a katonai főiskolai és egyetemi tanulmányait követően a Hadtudományi Doktori Iskolában (1997–2000) és a párizsi Összhaderőnemi Védelmi Kollégiumban (CollègeInterarmées de Défense – CID) tanult.

RÉTI Zsófia

retizsofia@kolejanisz.hu

Zsófia RÉTI is working in Expert position at the Kolejanisz Law Firm. She finished her studies on Judicial Administration Bsc in Győr at Deák Ferenc Faculty of Law and Political Sciences of Széchenyi István University, where she is currently studying undivided Master of Law. She has awarded the 3rd place in the Infocommunication Law Section of the 36th National Scientific Student Conference with her scientific essay on the question of the censorship of public figures on social media platforms. She has also been awarded the Ministry of Justice of Hungary's National Excellence in Law Scholarship on several occasions.

A Kolejanisz Ügyvédi Iroda szakértő munkatársa. 2020-ban végzett a győri Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Karán igazságügyi igazgatási alapszakon, majd tanulmányait ugyanezen egyetemen folytatta és folytatja jelenleg is jogász osztatlan mesterszakon. A XXXVI. Országos Tudományos Diákköri Konferencia Infokommunikációs Jogi Tagozatában III. helyezést ért el a közszereplők közösségi média oldalakon történő bírálhatóságának kérdésével foglalkozó tudományos dolgozatával. Emellett több alkalommal elnyerte az Igazságügyi Minisztérium Nemzeti Kiválósági Jogászösztöndíját.

SZŰCS Endre

szendre63@gmail.com

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.

VARGA János

varga.janos@kgk.uni-obuda.hu

János VARGA is an associate professor of economics at the Óbuda University, in Budapest, Hungary. Since 2009 he is lecturing in different fields of management. He finished his PhD studies in 2012 and got PhD 2 years later. During his research activities he deals with the competitiveness of the economic participants (research areas: competitiveness of firms and nations, change management, quality of leadership). He was a visiting lecturer in Romania and Poland. He participates in national and international scientific organisations. He is a member of the Hungarian Academy of Sciences and Hungarian Economic Association. Since 2011 he took part in ten research projects as a team member or research leader. Mr. Varga has more than 300 publications in scientific journals or in conference

VARGA János egyetemi docens az Óbudai Egyetemen. Különböző menedzsment területeken oktat. 2012-ben abszolválta doktori tanulmányait, majd szerzett fokozatot 2014-ben. Kutatási témája a versenyképesség. Vendégtanár volt több alkalommal is Romániában és Lengyelországban. Hazai és nemzetközi szervezetek tagja vagy tisztségviselője. A Magyar Tudományos Akadémia köztestületi tagja, emellett olyan szervezetekben is tagsággal rendelkezik, mint például a Magyar Közgazdasági Társaság. 2011 óta 10 nagyobb kutatási projektben vett részt, amelyekben tagként vagy vezető kutatóként segítette a munkát. Tudományos teljesítményére aktivitás jellemző. 300-nál is több publikációja van, amelyek között Q1-es, Q2-es, Q3-as és Q4-es cikkek, kiadványok, egyetemi jegyzetek is találhatók. Nemcsak

proceedings. The professor has 15 years' experience of teaching and also participated in several training programme in the last few years. He is a special advisor of the European Parliament since 2018.

az oktatásban, hanem a szakmai képzésekben, tréningekben is jelentős tapasztalatokat szerzett az elmúlt 15 évben. 2018-tól az Európai Parlament munkájába is betekinthetett független tanácsadóként.

ZSARNOVSZKI Attila

zsarnovszki.attila@stud.uni-obuda.hu

Attila ZSARNOVSZKI was specialized on engineering, revising and auditing activities related to industrial technologies with explosion hazard. He is highly qualified in the engineering solutions related to the field´s electric engineering erections and process control. He has an MSc in Elelctrical Engineering, he is a member of the Hungarian Chamber of Engineers, licensed expert and designer in explosion protection, oil- and gas engineering, pharmaceutical manufacturing, petrolchemical and more. He is the founder of EX-ON Engineering LLC., that has been for over 18 years the only independent domestic engineering company concentrating solely on industrial technologies with potential explosion hazard. EX-ON Engineering LLC. is an accredited certification organization in several areas (e.g. ATEX), offering professional engineering and inspection services (e.g. field inspections, design and expert works). Attila ZSARNOVSZKI is currently a PhD student at the Doctoral School of Safety and Security Sciences at the University of Óbuda.

ZSARNOVSZKI Attila a robbanásveszélyes ipari technológiákkal kapcsolatos mérnöki, felülvizsgálati és ellenőrzési tevékenységekre szakosodott. Magasan képzett az elektrotechnikai szerelésekkel és a folyamatirányítással kapcsolatos mérnöki megoldások terén. MSc villamosmérnöki diplomával rendelkezik, a Magyar Mérnöki Kamara tagja, robbanásvédelmi, olaj- és gázipari, gyógyszergyártási, petrolkémiai és további szakterületek szakértője és tervezője. Az EX-ON Mérnökiroda Kft. alapítója, amely több mint 18 éve az egyetlen független hazai mérnöki cég, amely kizárólag a potenciális robbanásveszélyes ipari technológiákra koncentrál. Az EX-ON Mérnökiroda Kft. több területen (pl. ATEX) akkreditált tanúsító szervezet, amely professzionális mérnöki és ellenőrzési szolgáltatásokat (pl. helyszíni vizsgálatok, tervezési és szakértői munkák) nyújt. ZSARNOVSZKI Attila jelenleg munkája mellett az Óbudai Egyetem Biztonságtudományi Doktori Iskola PhD hallgatója.

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 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

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 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 tapasztala-

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.

tokat, 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 4, 2024. | **2024. VI. évf. 4. szám**

CONTENT | TARTALOM

APPEARANCE OF SAFETY AND SECURITY IN THE HUMANITIES (PART 3)

A BIZTONSÁG MEGJELENÉSE A HUMÁN TUDOMÁNYOKBAN (3. RÉSZ)

KOLLÁR Csaba[1]

Abstract

This paper explores the concept of safety and security within the humanities, focusing on its psychological aspects. The study delves into the individual characteristics and group dynamics that influence human behavior and security perceptions. Key psychological theories, such as the safety triad in safety psychology, evolutionary psychology, developmental psychology, and organizational psychology, are examined to understand their impact on safety and security. The paper highlights how individual traits, societal interactions, and environmental factors contribute to the development of security awareness and behavior. It also discusses the role of motivation, personal development, and mental health in shaping security consciousness, emphasizing the dynamic interplay between individual actions and broader cultural contexts.

Keywords

safety and security, humanities, psychology, safety psychology, evolutionary psychology, developmental psychology, organisational psychology

Absztrakt

A tanulmány a biztonság és biztonságérzet fogalmát vizsgálja a humán tudományokban, különös tekintettel annak pszichológiai aspektusaira. A kutatás az egyéni jellemzők és a csoportdinamika hatását elemzi az emberi viselkedésre és a biztonságérzetre. A biztonságpszichológia, az evolúciós pszichológia, a fejlődéslélektan és a szervezetpszichológia kulcsfontosságú elméleteit vizsgálja, hogy megértse ezek hatását a biztonságra. A tanulmány kiemeli, hogyan járulnak hozzá az egyéni jellemzők, a társadalmi interakciók és a környezeti tényezők a biztonságtudatosság és viselkedés fejlődéséhez. Tárgyalja a motiváció, a személyes fejlődés és a mentális egészség szerepét a biztonságtudat alakításában, hangsúlyozva az egyéni cselekvések és a tágabb kulturális kontextusok közötti dinamikus kölcsönhatást.

Kulcsszavak

biztonság, humán tudományok, pszichológia, biztonságpszichológia, evolúciós pszichológia, fejlődéslélektan, szervezetpszichológia

[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

PSZICHOLÓGIA

A pszichológia, mint tudomány rendszerint az egyént helyezi vizsgálódásai középpontjába [1]. Az egyén egyedi tulajdonságokkal rendelkezik, melyek összességében csak rá jellemzőek, ugyanakkor számos olyan tulajdonsága is van, ami alapján egy/több csoport tagja is lehet. Az egyedi tulajdonságok az egyén jellemében, viselkedésében, gondolkodásában, kommunikációjában jutnak kifejezésre, de ezek az egyedi tulajdonságok és jellemvonások – melyek rendszerint kialakultak a felnőttkorra – nem tekinthetőt statikus képződményeknek, hiszen a társas interakciók, a környezeti hatások, valamint az idő folyamatosan alakítják azokat. Az interakcióknak és egyéb hatásoknak köszönhetően jobb esetben az egyén jelleme fejlődik, formálódik (ami alatt társadalmi megközelítés szerint a „jó ember" fogalmát értjük), rosszabb esetben azonban torzul, sérül, ami devianciához, kirekesztettséghez és kirekesztődéshez, elmagányosodáshoz, agresszióhoz, s megannyi pszichikus betegséghez vezethet. Az egyén egyedisége mellett Deming [2] [3] és Covey [4] a következő humanista elveket fogalmazz meg:

1. Mindenki számos szempontból egyedi. Az egyének speciális tulajdonságait nem lehet megérteni vagy értékelni általános elvek vagy fogalmak alkalmazásával, mint például a teljesítménymenedzsment viselkedésalapú elvei vagy a pszichoanalízis állandó személyiségjegy-perspektívája.
2. Az egyénekben sokkal több lehetőség rejlik, mint amit általában megvalósítanak, és nem szabad úgy érezniük, hogy a múltbeli tapasztalatok vagy a jelenlegi kötelezettségek akadályozzák őket aktivitásukban.
3. Az egyén jelenlegi állapota az érzések, a gondolkodás és a hiedelmek tekintetében a személyes siker kritikus meghatározója.
4. Az ember énképzete befolyásolja a mentális és fizikai egészséget, valamint a személyes hatékonyságot és teljesítményt.
5. Az eredménytelenség és az abnormális gondolkodás és viselkedés a valódi én („aki vagyok") és az ideális én („aki szeretnék lenni") közötti nagy eltérésekből fakad.
6. Az egyéni motívumok nagyon változatosak, és az ember belsejéből származnak.

A pszichológia és biztonság kapcsolatáról szóló részben elsőként a biztonságpszichológiában alkalmazott biztonsági triád [5] [6] alapján írok a fontosabb pszichológiai jellemzőkről, majd külön alrészekben az evolúciós pszichológia, a fejlődéslélektan, illetve a munka- és szervezetpszichológia biztonsággal összefüggő megállapításairól.

A biztonsági triád a pszichológiai fogalmakat a biztonsági kultúra vonatkozásában egy háromszögbe rendezi (1. ábra), a háromszög egyes oldalainál a környezeti tényezők, a személyi tényezők és a viselkedési tényezők vannak, melyek közül írásomban részletezve csak a személyi tényezőkről írok.

A biztonsági triád dinamikus és interaktív. Az egyik tényező változása végül hatással van a másik kettőre is. Például az olyan viselkedések, amelyek csökkentik a sérülés valószínűségét, gyakran környezeti változással járnak, és a biztonságos viselkedéssel összhangban lévő attitűdökhöz vezetnek. Ez különösen igaz, ha a viselkedést önkéntesnek tekintik. Más szóval, amikor az emberek úgy döntenek, hogy biztonságosan cselekszenek, akkor a biztonságos gondolkodásmód szerint viselkednek. Ezek a viselkedések gyakran valamilyen környezeti változást eredményeznek. [7]

1. ábra: A biztonsági kultúra a biztonsági triád értelmezésében

A személyi tényezők

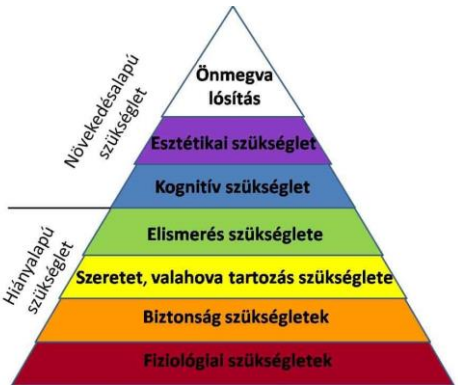
A tudás alapjának az adatokból feldolgozott információt tekintjük, s a tudás járul hozzá az egyén (vagy akár a szervezet) tapasztalatain keresztül annak bölcsességéhez. Az adatok és az információk sokféle forrásból származhatnak, úgymint evolúciós hagyaték, egyedfejlődés (ezekkel később foglalkozom), társas interakciók, írott források, elektronikus/online források, saját tapasztalások. Sloman és Fernbach [8] azt vizsgálja, hogy hogyan hat egymásra az emberek tudása és tudatlansága. A tudásmegosztás révén az egyén fejlődik, időt nyer (mivel nem kell minden tapasztalást magának átélnie, elég, ha tud/hall róla), s maga is hozzájárul egy másik ember fejlődéséhez és hatékony időgazdálkodásához. A tudásmegosztás elősegítheti, hogy az egyén sikeresen birkózzon meg a kihívásokkal és a veszélyekkel, ugyanakkor a szándékos, vagy tudatlanságból eredő hamis tudások megosztása, a tévhitek és a félreértések ugyan lehet, hogy növelik az egyén biztonságtudatát, de alapvetően biztonsága ellenében hatnak. Glassner [9] nem a tudásmegosztás, hanem a társadalmi-, politikai- gazdasági- és kommunikációs (média) rendszerek biztonság- illetve félelemérzetre gyakorolt hatását vizsgálja, s megállapítja, hogy ezek a rendszerek képesek markánsabban érzékeltetni és bemutatni a veszélyeket tényleges súlyukhoz képest. E megközelítés alapján az egyén az elvárható mértékhez képest sokkal több figyelmet fordít arra, hogy biztonságban érezze magát, saját maga és családja egészsége, fizikai biztonsága érdekében komolyabb anyagi áldozatokra is hajlandó, nem egy esetben túlbiztosítva magát.

Míg a *képesség* „az összes veleszületett és szerzett pszichés adottság, amely egy teljesítmény eléréséhez szükségesek" [10 p. 221], addig a készség azt jelenti, hogy az egyén a képességeit ténylegesen kívánja-e, akarja-e felhasználni, alkalmazni egy adott tevékenység, vagy feladat elvégzése során. E megközelítés alapján az egyén rendelkezik, rendelkezhet a biztonságra vonatkozó képességével, tehát logikusan átgondolva az adott szituációt, felmérheti a reális veszélyeket és fenyegetéseket és ezek ellen felléphet. Ugyanakkor többek között lustasága, nemtörődömsége, pillanatnyi lelki állapota, fáradtsága, kiégettsége, vagy az adott helyzetben levő többi egyénnek való megfelelés, vagy a szituáció téves felmérése és értékelése miatt mégsem teszi meg. Az egyén biztonságtudatossági fejlesztésének tehát két szintje van: (1) a biztonsággal kapcsolatos képességek fejlesztése, (2) és ezek átültetése a gyakorlatba, vagyis az ismeretek készség szintű elsajátítása.

Az *intelligencia* a „tapasztalatokból való tanulás, az elvont fogalmakban gondolkodás és a környezet hatékony kezelésének a képessége". [1 p. 595] Az intelligencia „mértéke

egyénileg különbözik, és függ az örökletes képességektől, valamint a tanult tapasztalatoktól." [10 p. 202] Annak ellenére, hogy mivel az intelligens emberek több információval rendelkeznek, így elvileg mélyrehatóbban képesek megérteni a kockázatokat, a veszélyeket és általánosságban a világ működést, nem állíthatjuk azt, hogy az intelligencia és a biztonságérzet között pozitív korreláció lenne. Az intelligens ember biztonságérzetét a sok információ negatívan is befolyásolhatja, mivel a kevésbé intelligens emberekhez képest reálisabban értékelheti és mérheti fel a környezeti veszélyeket, s különösen azok a tényezők erodálják biztonságérzetét, melyekre nincs ráhatása.

A pszichológiában számos *motivációs elmélet* született, úgymint: büntetés-jutalom, szükséglethierarchia, motiváció-elfojtás, erőforrás, szociál-kognitív, AMP. Skinner [11] szerint az egyén viselkedése a környezeti ingerekre adott válaszaiból alakul ki, s ezt a viselkedést a büntetéssel és a jutalmazással lehet alakítani, formálni, irányítani. A biztonsági szabályzatokban és a munkaszerződésben leírt normatívák rendszerint kitérnek az egyéni felelősségre, illetve arra, hogy szabályszegés esetén milyen büntetésre lehet számítani. Maslow [12] sokszor és számos tudományterületen idézett, a szükségletek hierarchiájával foglalkozó művében a szükségleteket egy piramisban ábrázolja (2. ábra), s azt állítja, hogy „a hierarchiában alacsonyabban elhelyezkedő szükségleteket legalább részben ki kell elégíteni, hogy a magasabban elhelyezkedő szükségletek a motiváció fontos forrásaivá válhassanak". [1 p. 402]



2. ábra: Maslow szükséglethierarchiája, melyet [13] egészített ki saját megjegyzéseivel

Bár azt állíthatjuk a Maslow-piramis alapján, hogy a fiziológiai szükségletek után a biztonsági szükségletek (biztonságban lenni, veszélymentesen lenni, elkerülni a veszélyeket) következnek, a biztonságtudománynak jobban megfelel az az elképzelés, hogy a biztonság a szükséglethierarchia minden szintjén megjelenik, csak interpretatív tartalma változik. Egyébként, még a modell megjelenése előtt maga Maslow [14] is hasonlóan vélekedik, amikor a piramis csúcsán levő önmegvalósítással kapcsolatban ír. Az önmegvalósítók jellemzői között ugyanis leírja, hogy „a valóságot gyakorlatiasan érzékelik", „jól tűrik a bizonytalanságot", „inkább a problémákra" (és azok megoldására), semmint „önmagukra összpontosítanak", „objektív nézőpontból képesek az életre tekinteni" [1 p. 403]. Ezek a jellemzők a biztonságtudatos emberre is jellemzők. A motiváció-elfojtás elméletet Herzberg [15] alkotta meg, s a munkahelyi motivációkat két csoportba sorolta: higiéniás tényezők, motivációs tényezők. Az előbbiben található a jó munkakörülmények, a biztonságos mun-

kahely, a megfelelő jövedelem, az utóbbiban az értékes munka (érzése) és a személyes fejlődés. Ha a higiéniás tényezők nem, vagy nem megfelelő mennyiségben, mértékben, szinten állnak rendelkezésre, akkor az komoly negatív hatást gyakorol a munkavállalók hozzáállására, felelősségérzetére, teljesítményére, aminek ráhatása van a vállalat egészének működésére is. Az erőforrás-elméletet Ryan és Deci [16] dolgozta ki, s arról szól, hogy a motivációjuk mértéke 3 tényezőtől függ (1) önrendelkezés (szabadnak érezhetik magukat, szabadon hozhatnak döntéseket, nem kell megtenniük azt, amit nem akarnak), (2) emberi kapcsolatok (az embereknek szükségük van arra, hogy szeretteikkel, barátaikkal, ismerőseikkel kapcsolatokat ápoljanak) és (3) értelem (az ember akkor motivált, ha tevékenységének értelme, s így célja is van, képes megérteni, hogy mit, miért tesz). E három komponens meglétének hiánya alulmotiváltsághoz vezet, amit az egyén a stressz növekedésében, mentális, pszichoszomatikus és fizikai betegségekben él meg, viselkedése megváltozik, ami szélsőséges esetben kiégéshez vezethet. A Bandura [17] által megalkotott szociál-kognitív tanuláselmélet azt állítja, hogy a motiváció a környezetből, más személyek példájából, a belső gondolatok és az érzelmek kölcsönhatásából származik. Bandura nagy jelnetőséget tulajdonít más személyek példájának, hiszen az egyén számára szimpatikus személyek magatartása és véleménye (pl.: egy tiniceleb álláspontja az interneten történő információk megosztásáról) nagymértékben befolyásolja a rajongó magatartását és véleményét is. A szerző amellett érvel, hogy olyan motiváló környezetet kell létrehozni és fenntartani, mely kielégíti az egyén pszichológiai igényeit, teljesítményre sarkallja, sikerre buzdítja, s egyben biztosítja az ezek eléréséhez szükséges erőforrásokat. Pink [18] AMP (autonomy - függetlenség, mastery - kiválóság, purpose – cél) modelljében azt állítja, hogy a magas teljesítmény és elégedettség titka – a munkahelyen, az iskolában és otthon – az a mélyen emberi igény, hogy saját életünket irányítsuk, új dolgokat tanuljunk és hozzunk létre, és tegyünk. E tevékenységünket motiválja a függetlenség, a kiválóság(ra törekvés) és a cél.

A bemutatott motivációs modellek többségénél felfedezhető, hogy a függetlenség, önállóság és a motiváltság között kapcsolat van. Ez alapján úgy gondolom, hogy a munkaszervezetben komoly figyelmet kell fordítani arra, hogy a dolgozó motiváltságát úgy tartsák fenn, hogy közben az ne veszélyeztesse az egyén, illetve a szervezet biztonságát, vagyis a szabadság és önállóság (érzése) ne a biztonsági szabályok hiányában, vagy be nem tartásában realizálódjon.

A *személyiség* a „viselkedésnek, gondolkodásnak és az érzelmeknek az a jellegzetes mintázata, amely meghatározza, hogy a személy hogyan alkalmazkodik környezetéhez.” [1 p. 610] Geller [7] úgy véli, hogy bizonyos személyiségjellemzők bizonyos embereket ellenállóbbá tesznek a szorongással szemben. Azok az egyének, akik azt hiszik, hogy irányítják saját sorsukat, és általában a legjobbat várják az élettől, nagyobb valószínűséggel veszik át az uralmat a stresszorok felett. Fontos felismerni, hogy ezek a személyi tényezők – az önuralom és az optimizmus – nem az emberek állandó veleszületett tulajdonságai. Ezek olyan lelkiállapotok vagy elvárások, amelyek személyes tapasztalatból származnak, és táplálhatók. Lehetséges olyan élményeket adni az embereknek, amelyek növelik a „kontroll” érzését, és elhitetik az emberekkel, hogy valami jó fog származni abból, hogy megpróbálják a stresszt konstruktív cselekvéssé változtatni.

Az egyén biztonságának sikere pszichológiai értelemben belső és külső tényezőktől függ [7]. A belső tényezők a következők: attitűdök, hiedelmek, érzések, gondolatok, sze-

mélyiségjegyek, értelmezések, értékek, szándékok – ezeket összességében a komplex személyiségkép egy-egy dimenziójában is értelmezhetjük. Kollár [19] Oroszi [20] alapján összefoglalta, hogy melyek azok a fontosabb személyiséggel (is) kapcsolatos jellemzők, amelyek hatással lehetnek az egyén (információ)biztonságára (3. táblázat).

1. Személyes	2. Munkahelyi	3. Pillanatnyi	4. Stresszhelyzet
Segítőkész	Új munkatárs	Fáradtság	Konfliktuskerülés
Naiv	Napi rutin	Sietség, kapkodás	Meggondolatlanság
Nyitott, barátságos	Problémamegoldás	Figyelmetlenség	Reflex
Kíváncsi, érdeklődő	Ismeretlenekkel való együttműködés	Túlterheltség	Leblokkolás
Befolyásolható	Elégedetlenség	Szabadság	Hárítás
Lusta	Lefizethetőség	Betegség	Kompromisszum
Hanyag, nemtörődöm	Megzsarolhatóság	Ünnepek	Együttműködés
Rajongó	Bosszú	Düh	Irányíthatóság

1. táblázat: Az egyén biztonságára ható fontosabb, személyiséggel (is) kapcsolatos tényezők [19]

Az 1. táblázat alapján a személyiségjegyeket két csoportba sorolom: pozitív és negatív. A Pozitívak közé sorolom a segítőkészséget, a nyitott, barátságos viselkedést, az együttműködőkészséget, a negatívakhoz pedig a naivitást, a befolyásolhatóságot, a lustaságot, a hanyagságot és a nemtörődömséget, az elégedetlenséget, a lefizethetőséget, a bosszúállást. Látható, hogy még a társas együttélést, a kooperatív attitűdöt feltételező személyiségjegyek is magukban hordozhatják a biztonsági kockázatot, amelyet a social engineerek ki is használnak.

Ha az egyén képes felismerni és belátni, hogy jellemének és személyiségének formálódása rossz irányba halad, akkor akár önállóan, akár segítséggel, de a negatív folyamatok megállíthatók és visszafordíthatók [21]. A saját és környezete biztonságával nem törődő személy (pl.: tiltott gyorsulási verseny résztvevője) életében történhet olyan esemény (pl.: balesetet okoz/szenved), aminek köszönhetően újraértékeli életét és felhagy addigi káros magatartásával. Az egyénnek van egy beállítottsága/beállítódása (attitűdje), mely alapján az embereket, tárgyakat, szervezeteket, helyeket, helyzeteket, eseményeket az egyén rokonszenvesnek, vagy ellenszenvesnek tartja [22]. Ebben többek között saját korábbi tapasztalataira, neveltetésére, emlékeire hagyatkozik. Az attitűdök fontos szerepet játszanak a döntéshozatalban, az emberi kapcsolatok építésében és fenntartásában, valamint a viselkedésben. Az egyén biztonsági attitűdjére is igazak a fogalomról általánosságban írt gondolatok. A biztonsági attitűd [23] az egyén saját, személyes véleménye, meggyőződése arról, hogy a helyzetek, események, személyek, csoportok a számára milyen biztonsági kockázatot, vagy veszélyt/fenyegetést jelenthet. Geller [7] szerint az attitűd a hiedelmekhez, értékekhez, szándékokhoz és felfogásokhoz hasonlóan befolyásolható az oktatáson keresztül, míg a tréningek a viselkedést közvetlenül is befolyásolni képesek. A biztonsági oktatás és tréningek közötti kapcsolat a következő: az oktatás közvetetten befolyásolhatja a viselkedést, ha az

oktatási folyamat megváltoztat egy attitűdöt, szándékot, meggyőződést vagy értéket, amelyet egy bizonyos viselkedéshez kapcsolódónak tekintenek. A tréning közvetetten is befolyásolhatja az attitűdöket, szándékokat, hiedelmeket vagy értékeket, ha a viselkedésváltozást a résztvevő elfogadja, és egy adott attitűdhöz, szándékhoz, meggyőződéshez vagy értékhez kapcsolódónak tekinti. A lényeg az, hogy az oktatás és a képzés stratégiai kombinációjára van szükség a viselkedés és a hozzáállás javításához, vagyis a biztonsági attitűd és a biztonságtudatosság fejlesztéséhez.

Evolúciós pszichológia

Az etológiával és az evolúciós biológiával komolyabb rokonságot mutat az evolúciós pszichológia [24]. E tudományterület művelői úgy gondolják, hogy a biztonság iránti igény az élet szükségleteinek megfelelően alakult ki, s formálódott az emberi evolúció során. A biztonság iránti igény tehát végig kiséri az emberi faj fejlődését, viselkedésének mozgatórugója, hiszen az embernek meg kellett teremtenie majd a soron következő generációknak át kellett adnia azokat az ismereteit, melyek révén meg tudta különböztetni az ehető és nem ehető gombákat, növényeket, el tudta készíteni biztonságos lakhelyét, eredményesen tudta felvenni a harcot a rá támadó ellenséggel szemben, el tudta ejteni az elfogyasztani kívánt állatot, képes volt az üss vagy fuss szellemében eldönteni a helyes magatartást. Az evolúciós folyamat tette lehetővé az utódok számára, hogy elődeikhez képest az átadott tudások és a szerzett tapasztalatok révén biztonsági stratégiák és konkrét cselekvési tervek alakuljanak ki a vadállatokkal, a ragadozókkal, a betegségekkel, egy támadólag fellépő másik csoport (törzs, horda), vagy a természeti viszontagságokkal szemben. Amelyik faj – vagy szűkebben értelmezve amelyik emberi csoportosulás – nyerő biztonsági stratégiát képes volt megvalósítani, s kellően adaptívan viszonyult a változásokhoz, az túlélte a támadásokat, szerencsétlenségeket, amelyik nem, az gyakorlatilag halálra volt ítélve. Ez a stratégia leegyszerűsítve a gének továbbvitelét jelenti a szaporodás révén, s a biztonságot az utódnemzéssel és -felneveléssel rokonítja. Az adott generáció ugyanis hozhat olyan döntést, mely veszélyes (pl.: ismeretlen helyre vándorlás), a csoport egy részének sebesülését/halálát okozhatja (pl.: csoportos mamutvadászat), lemondással jár (pl.: éhínség idején nem a bőség idején megszokott módon kerülnek kiosztásra az ételek), de összességében a jövő generációjának túlélését alapozza meg. A modern társadalmakban a biztonságot számos intézmény tartja fenn, többek között a jogalkotás és a törvények, a rendvédelmi szervek, az egészségügyi és szociális intézmények. Ezek az intézmények nem mások, mint az évmilliók során folyó evolúciós folyamat utóbbi néhány ezer évre visszatekintő, vagy jelenkorunkra „tökéletesített" biztonság(érzet) fenntartására hivatott képződményei. Az evolúciós pszichológia egyik kiemelt vizsgálódási területe a béke és az agresszió mibenléte és megjelenése az emberi viselkedésben [25]. Az (erősebb) fél agressziójától való félelem is fenntarthat egy (látszat) békét, de ebben a békében nem a biztonság, hanem a félelem érzete uralkodik. Bár a modern társadalmakban is jelen van a fizikai agresszió, annak aránya a törvényeknek és a társadalom fejlődésének köszönhetően alapvetően csökkenő tendenciát mutat, miközben a rejtett, illetve a verbális agresszió növekszik. Daly és Wilson [26] is azon a véleményen van, hogy az emberi viselkedés és döntés alapját sokszor a biztonságra való törekvés adja, hiszen úgy viselkedünk, hogy az túlélésünket és a jövő nemzedékének túlélését jelentse. A biztonság-fókuszú viselkedésünk alapján értelmezhetjük a biztonsági döntéshozatal és a biztonsági kultúra fogalmait is, melyekről a fogalmi részeknél már említést tettem.

Fejlődéslélektan

Az evolúciós pszichológia az evolúciós fejlődést, a fejlődéslélektan pedig az egyedfejlődést helyezi a középpontba a fogantatástól a halálig. E fejlődés fontosabb stációi Cole és Cole felosztása szerint [27] a következők: méhen belüli fejlődés és születés, csecsemőkor, kisgyermekkor, iskoláskor, serdülőkör, felnőttkor és időskor. Az alábbiakban az egyes fejlődési korszakok biztonsággal összefüggő vonatkozásaival foglalkozom. Többször és többféle aspektusból utaltam már arra írásművemben, hogy akár a közösség/csoport, akár a család egyik alapvető feladata az, hogy a géneket tovább örökítse. Ennek feltétele az, hogy a nő olyan biztonságos környezetben legyen, mely lehetővé teszi a számára, hogy a születendő gyermekének a fogantatástól a születésig saját testének és mentális állapotának védelmén keresztül békét és biztonságot biztosít. Ebben a feladatban jobb esetben a (szűkebb) család, a férj, a barátnők is részt vesznek, s az anyával közös tevékenységük révén segítik elő a születendő gyermek és anya biztonságát. David [28] átfogó életút kutatása rámutatott arra, hogy azok a gyermekek, akiknél az anya abortuszért folyamodott, de a hatóságok ezt megtagadták, így a gyermekek megszülettek, az egész életükben a kontrollcsoport tagjaihoz képest hátrányt szenvedtek. Az ilyen „nem kívánt gyermekek veszélyeztetettebbek számos felnőttkori társadalmi és pszichológiai problémával szemben… Valószínűbb, … hogy saját társas kapcsolataikat nem kielégítően élik." [27 p. 111] Ez azt jelenti, hogy nehezebben tudnak beilleszkedni a különböző társadalmi csoportokba, nehezebben alakítanak ki tartós társadalmi kapcsolatokat, az átlaghoz képest bizalmatlanabbak a külvilággal szemben, vélt, vagy valós aggodalmaik miatt nem érzik magukat biztonságban. A csecsemőkort (2 és fél éves korig) a szülővel (elsősorban az anyával) kialakuló kapcsolat jellemzi. A szülői gondoskodás már a megszületéstől kezdve biztonságot jelent a gyermek számára, aki az alapvető érzékelési folyamatokon (hallás, látás, szaglás és ízlelés, tapintás) keresztül megannyi ingert vesz fel a környezetéből. Ezek az ingerek jobb esetben kellemesek, s ilyenkor a csecsemő biztonságban érzi magát. Rosszabb esetben kellemetlenek, amelyek nyugtalansággal, sírással válaszol. Az újszülöttek aktivitásszintje azt jelzi, hogy hogyan, s milyen könnyen kezd el sírni, amikor valamilyen szokatlan dolog történik [29]. A csecsemők viszonylag hamar megtanulják, hogy a sírás révén a környezetük (elsősorban az anyjuk) felfigyel rájuk, de a sírás, mint figyelemfelkeltő eszköz sokaknál felnőtt korban is megmarad. A sírás egy olyan mechanizmus, ami révén az egyén a biztonság, vagy legalábbis a védettség állapotába kerülhet. A csecsemőkor az egyén számára környezetének kiterjesztett felfedezését teszi lehetővé azáltal, hogy elkezd járni. A kudarcok (pl. elesik) és az újrapróbálás révén nem csak koordinációs készsége fejlődik, de a szülői pozitív visszajelzések alapján azt is megtanulja, hogy a nehézséget le lehet győzni. A bizalom/bizalmatlanság kialakulása is ehhez a fejlődési korszakhoz köthető. 7 hónapos koruk előtt a csecsemők képesek arra, hogy „az embereket két csoportra osszák, azokra, akikben lehet bízni, hogy segítenek, és a kiismerhetetlen idegenekre." [27 p. 218] Ez a képesség aztán egész életük során elkíséri őket, s a többi emberrel való interakció révén lehetőséget ad arra, hogy az egyén eredményesen alakítsa ki biztonságos társas szféráját, vagy legalábbis jobban be tudja azonosítani azokat, akik idegenek, s nem számíthat a segítségükre. A játék a csecsemőkben megannyi kellemes emléket hagy [30], melyek aztán felnőttkorban is előidézhetők. Az (információ)biztonsági tudatosság fejlesztés módszerei között a játékosítás (gamification) azért is népszerű, mert ez egy olyan oldott, feszültségmentes (de izgalommal teli) módszer, amelyik a felnőtt embereket visszavezeti a gyermeki korban átélt kellemes élménykörnyezetbe. A csecsemőkor

vége felé alakul ki a gyerekekben a képesség, hogy hazudjanak, bár ebben a korban a hazugságnak még nem célja a megtévesztés, inkább csak a fantáziájában jelen levő dolgokról beszél valóságosként. A hazugság képessége aztán szintén elkíséri az egyént egész élete során, s része lesz biztonságtudatosságának, amikor saját kényelme, vagy (vélt) biztonsága, vagy saját, vagy közössége érdekének érvényesítése miatt füllent, lódít, nagyot mond, megtéveszt, átver, átejt, tévedésben tart [31] [32]. A kisgyermekkor (2 és fél év és 6 éves kor között) a nyelv elsajátításának a kora. Bár az egyén már a csecsemőkor vége felé is képes volt magát kifejezni, ez a kor hozza el a számára a nyelv használatát, s azon keresztül a többi emberrel való társalgás lehetőségét. A társalgás révén fejlődik a kisgyermek nyelvi képessége, s egyre több tudással is gazdagodik. A nyelv elsajátítása azért is fontos, mert a gyermek a szülei által mondottakat (pl.: ezt nem szabad, ez veszélyes) nem csak megérti, de meg is tudja ismételni, ami révén az instrukciók jobban bevéső dhetnek. A gyermek jogot formál arra, hogy rákérdezzen, „miért?", s a szülői válaszok markánsan formálják véleményét az adott dologban. Ha a szülő a gyerekkel folytatott verbális és nonverbális interakciók során a tiltott és szabad tevékenységekhez magyarázatot is fűz, akkor azzal fejleszti gyermeke biztonságtudatosságát is. Az iskoláskorban (6-12 év között) a testi növekedés, az agy fejlődése és a minőségileg új gondolkodás jellemző. Mivel ezen korszakban a gyerekek életük harmadát-negyedét iskolában töltik, az iskola a személyek (osztálytársak, tanárok) és a szabályok (házirend) révén komoly szocializációs hatással bír. A kortársközösségek egyaránt jelenthetnek az egyén fejlődése és jövője szempontjából előnyöket [153] és hátrányokat [34]. Az egyén a saját kortársközösségein belül biztonságban érzi magát, s gyakran a többi kortársközösség elleni agresszió (vagy legalábbis elhatárolódás tőlük) jelentheti a közösség kohéziós erejét. Az iskolás gyermek megtanulja, hogy a kortársközösségen belül milyen szabályok uralkodnak, illetve maga is részt vesz annak alakításában. Az iskoláskorú egyén rendszerint bízik kortársközössége tagjaiban, s pont e bizalom amellett, hogy biztonságérzetét növeli, veszélyforrás is lehet. A megbízhatónak gondolt osztálytársnak küldött kompromittáló fényképeken pár óra múlva már az egész közösség, vagy az egész iskola élcelődik. A törvények céljával kapcsolatban a 12-13 éves gyerekek úgy vélekednek, hogy „azért vannak … hogy ne bántsák egymást az emberek. Ha nem lennének törvényeink, akkor az emberek meggyilkolhatnák egymást. Így az emberek nem lopnak és nem gyilkolnak" [35 p. 640]. A serdülőkor (12-21 év között) végére az egyén felnőtt lesz, ami a fejlett társadalmakban rendszerint nem jelenti a szülőktől történő elköltözést, de a cselekedetekért önállóan vállalt felelősséget igen. A serdülőkorban megváltozik a törvényekkel kapcsolatos elképzelés. A törvények azért vannak, hogy „biztosítsák a biztonságot és a kormányzást. Hogy korlátozzák, hogy mit tehetnek az emberek. Lényegében irányadók az emberek számára" [35 p. 640]. Erikson [36] rámutat arra, hogy a serdülőkorban az egyén identitásának fejlődését krízisek kísérik, melyek társas kapcsolatai (család, barátok, osztálytársak) és addigi értékrendje átértékelődését is jelentik.

Nem a szociológiai, hanem a fejlődéslélektani résznél kívánok szólni az ifjúság életkori kategóriájáról. Az ifjúság, mint csoport alsó korlátját hozzávetőlegesen 11-12 éves kortól lehet számítani, abból kiindulva, hogy a fiatalok egyre korábban kezdenek önállósodni, illetve a kamaszkor időben kitolódik. Az alsó életkor meghatározásánál azonban nem a 11-12 éves kort veszi a szociológia és én sem [37] alapnak, hanem a 14. életévet – elsősorban – amiatt, hogy a nagy átlag 14 évesen kezdi el középfokú tanulmányait, (rendszerint) új környezetbe kerül, több elvárásnak, magasabb mércének kell megfelelnie. Az ifjúság felső

korlátját Gábor és Jancsák [38], alapján a 29-30 életévre teszem. A felső korhatár kitolásának több oka is van, ezek közül a három legjelentősebb (1) a tanulmányok meghosszabbodása, a (2) munkavállalás (főállású, egészidős munkaviszony), illetve a (3) saját családalapítás és gyermekvállalás időpontjának kitolódása. Az ifjúság azért érdemel különös figyelmet tanulmányom szempontjából is, mert ők azok, akik a munka világába lépve (jobb esetben) a legfrissebb tudást képviselik, az új eszközök elsajátításához kevesebb idő szükséges nekik, idősebb kollégáikhoz képest fizikailag jobban terhelhetőek. A munkahelyi korfa elemzése azért fontos akár a magánbiztonsági szektorban is, mivel jelezheti a cég/szektor fejlődési potenciálját.

A felnőttkort Cole és Cole [27] a 21 és kb. 60-65 év közötti korszakra érti, a korhatár felső határát a nyugdíjba vonulás jelenti, vagyis azt a korszakot, ami rendszerint és zömében a munkával töltött éveket jelenti. Tanulmányom későbbi megállapításai is rendszerint erre a korszakra vonatkoznak.

Az időskort általában a nyugdíjba vonulástól számítjuk. Ezt a korszakot a biológiai és a kognitív változások jellemzik. Bromley [39], illetve Staudinger és Lindenberger [40] egyaránt rámutatnak arra műveikben, hogy idős korban a biztonság felértékelődik, s egyenesen korrelál az életminőséggel. Az életminőségtől, illetve az időskori élet biztonságos megélésétől elválaszthatatlan a mentális és a fizikai egészség fenntartása, a jövőtől való félelmek és kételyek minimalizálása, a társas kapcsolatok ápolása, esetleg újraépítése. Az idős emberek többsége szenved a magánytól és az egyedülléttől, s könnyen lehetnek a kedvesnek tűnő, „öregező" szélhámos bűnözők célpontjai.

Írásművemben a fentieken kívül nem kívánok külön-külön értekezni az egyes pszichológiai irányzatokról, inkább a pszichológia és a biztonságtudomány metszéspontjában megjelenő fontosabb témákat szeretném bemutatni.

Munka- és a szervezetpszichológia

Mivel a munka- és a szervezetpszichológia megannyi területen fedi egymást, ezért e két területet együtt tárgyalom a biztonság fókuszában. A munkapszichológia „a munkaeszköz és a munkafolyamat optimális kialakításában és munkamotiváció javításában vesz részt … a balesetek okát és a megelőzés lehetőségeit" [10 p. 288], a szervezetpszichológia pedig „több személy közös munkája során kialakuló struktúrákat és folyamatokat" [10 p. 422] vizsgálja. Mivel az emberek zöme vagy munkaszervezetben dolgozik, vagy munkavégző tevékenysége (pl. egyéni vállalkozóként) a munkafolyamat része, ezért különösen fontos, hogy milyen az egyén kapcsolata saját munkaközössége tagjaival, más munkaközösségek tagjaival, hogyan viszonyul a csoport belső normarendszeréhez, esetleg hogyan alakítja azt. A munkavégző egyén szintjén kérdéses, hogy hogyan tudja/akarja betartani a munkaszervezet hivatalos (belső) szabályait, illetve a munkakörével kapcsolatos akár belső, akár külső szabályokat, rendeleteket, törvényeket, hogyan érzi magát, mi motiválja, hogyan képes megbirkózni a stresszel. Doyle [41] rámutat arra, hogy a munkavállalók motivációja, elkötelezettsége, munkahelyi jóllét-érzése, a munkahelyen megélt stressz és annak szubjektív mértéke nagymértékben attól függ, hogy a szervezet tud-e olyan intézkedéseket hozni és megvalósítani, amelyek lehetővé teszik a munkavállalók számára a biztonságos munkakörnyezetet és munkakörülményeket, megőrizve, esetleg fejlesztve az egyén fizikai és mentális egészségét. A munkavállaló egészsége és munkahelyi biztonságérzete nem csak jószolgálat a vállalat részéről, hanem komoly termelékenység- és így profitnövelő hatással is bír, így

megfelelő szervezeti kultúrát feltételezve a kiemelt szervezeti célok között kerül megemlítésre. Ugyancsak komoly hatást gyakorol a szervezeti hatékonyságra, s azon keresztül a profitra a szervezeti biztonsági kultúra, különösen az együttműködő és támogató biztonsági kultúra kialakítása és fejlesztése, mely révén a munkavállaló a biztonsággal kapcsolatos problémáit (pl.: nem biztonságos berendezés, információbiztonsági esemény) őszintén a vezetésnek, vagy az érintett kollégáknak elmondhatja. Egy ilyen légkörben a munkavállaló biztonsági attitűdje megfelelő, illetve biztonságtudatossági képzésekkel még fejleszthető is. Ellenkező esetben azonban olyan negatív folyamatok indulnak el, melyek szervezeti szinten rontják a termelékenységet, növelik a fluktuációt és a balesetek számát, az egyén szintjén pedig növelik stresszt, a frusztráltságot, ami a kiégés irányába mutat.

Markáns kapcsolat van egyén biztonságtudatossága és biztonsági attitűdje, illetve a (munkahelyi) kiégés között. Freudenberger [42] a kiégést a szakmai viselkedés leírására alkalmazta, álláspontja szerint a kiégés az egyén lelki és fizikai erőforrásainak kiapadását jelenti. Megfogalmazásában: „Ez a szindróma krónikus, emocionális megterhelések, stresszek nyomán fellépő fizikai, emocionális, mentális kimerülés állapota, amely a reménytelenség és inkompetencia érzésével, célok és ideálok elvesztésével jár, s amelyet a saját személyre, munkára, illetve másokra vonatkozó negatív attitűdök jellemeznek.” Szilágyi és Váry [43] Cherniss-re utalva a kiégéssel kapcsolatban úgy fogalmaznak, hogy a kiégés olyan folyamat, amelyben a stressz és a hajszolt munka hatására a hajdanában elkötelezett szakember eltávolodik munkájától. Kollár [44 p. 22] meglátása szerint „a kiégés fogalmának használatakor a személy érzelmi, lelki és fizikai kimerülési állapotára gondolunk, melyet a stressz és/vagy a tartós érzelmi megterhelés vált ki, s melyet az egyén a szokásos módon nem tud megoldani”. File [45], aki Maslach-ra hivatkozik, úgy gondolja, hogy „A kiégés hosszan tartó speciális foglalkozási stressz következtében kialakult tünetegyüttes, három tünetből álló szindróma:

1. érzelmi kimerülés,
2. deperszonalizáció (elszemélytelenedés) érzéketlen, vagy cinikus magatartás a betegek, vagy az ügyfelek és a munkatársak iránt, azok tárgyként kezelése,
3. csökkent teljesítmény, inkompetencia érzése.”

A fenti két definícióból is egyértelműsíthető, hogy a kiégéses munkavállaló nem csupán testi, hanem testi-lelki-szellemi (vagy más osztásban fizikai-érzelmi-tudati) téren egyaránt fokozatosan veszíti el energiáit, tartalékait. Az energiák fogyása olyan mértékű és dinamizmusú, hogy a több területről érkező, egymással szorosan együttműködő szakemberek segítsége nélkül az egyén rendszerint nem képes egymaga orvosolni problémáit még akkor sem, ha egyébként a komplex terápia néhány elemét (pl.: testmozgás, aromaterápia, fitoterápia, meditáció, zeneterápia) tudatosan, vagy ösztönösen alkalomadtán alkalmazza. A kiégés egy folyamat, melyet a szakirodalom több stációra bont, kiemelve, hogy az egyes stációk között nincsenek éles határok. Hézser [46] a kiégés folyamatának 12 lépését nevezte meg:

1. A bizonyítani akarástól a bizonyításkényszerig
2. Fokozott erőfeszítés
3. A személyes igények elhanyagolása
4. A személyes igények és a konfliktus elhanyagolása
5. Az értékrend megváltozása

6. A fellépő problémák tagadása
7. Visszahúzódás
8. Magatartás- és viselkedészavarok
9. Deperszonalizáció
10. Belső üresség
11. Depresszió
12. A teljes kiégettség (burned-out)

A felsorolásból egyértelmű, hogy ahogy az egyén előrehalad kiégés folyamatában, úgy csökken, majd a végén el is veszti biztonsági attitűdjét. Maslach (1982) – idézi Nagy [47 p. 83], munkájában kiemeli, hogy „a kiégés a pszichoszomatikus tünetek, panaszok és megbetegedések, valamint a szomatikus betegségek széles skáláját okozhatja”, melyet rendszerint öt csoportba sorolunk:

1. Pszichés tünetek
2. Fiziológiai tünetek
3. Magatartásbeli tünetek
4. Szociális magatartás
5. Problematikus viselkedésformák

A kiégés folyamatának fontosabb jelei a következők [45]: a munkához, a kollégákhoz és/vagy a vezetőkhöz való viszony megváltozása, a munkát maga végzi el, nem delegál, a munka átlátásának elvesztése, elvész a részletekben, nő a hibázás, pontatlanság, túlterheltség, nincs idő a privát életre, vagy szabadságra, a másokkal való kontaktus megterhelő, türelmetlenség, ingerlékenység, álmatlanság, dekoncentráltság, visszahúzódás és elmagányosodás, depresszió, panaszkodás (és/vagy látható jelek) szédülésre, emésztési problémákra, vérnyomás ingadozásra, légzési panaszokra, fejfájásra, alvászavarra, gyomor- és bélproblémákra. Ezek pedig szinte kivétel nélkül közvetlen hatást gyakorolnak az egyén biztonságára, növelik a balesetek kockázatát, csökkentik biztonságtudatosságát, majd a folyamat utolsó lépéseinél el is veszti azt. A folyamatban az egyén elveszti reális helyzetértékelő képességét, így nem, vagy rosszul méri fel a veszélyeket, a fenyegetettségeket.

ÖSSZEFOGLALÁS

A tanulmány átfogó képet nyújt a biztonság és biztonságérzet megjelenéséről a humán tudományokban, különös tekintettel a pszichológiai tényezőkre. Az egyéni jellemzők és a csoportdinamika vizsgálata mellett a biztonságpszichológia, az evolúciós pszichológia, a fejlődéslélektan és a szervezetpszichológia fontosabb elméleteit is tárgyalja. Írásom rávilágít arra, hogy az egyéni tulajdonságok, a társas interakciók és a környezeti hatások miként befolyásolják a biztonságtudatosság és a viselkedés alakulását. A motiváció, a személyes fejlődés és a mentális egészség jelentőségét is elemeztem a biztonságtudat formálásában, kiemelve az egyéni cselekvések és a szélesebb kulturális környezet közötti dinamikus kapcsolatot. A tanulmány hozzájárul a humán tudományok és a biztonságtudomány közötti interdiszciplináris párbeszédhez, segítve a biztonságpszichológia elméleti és gyakorlati megértését.

FELHASZNÁLT IRODALOM

[1] Atkinson, R. L. – Atkinson, R. C. – Smith, E. E. – Bem, D. J. *Pszichológia.* Budapest: Osiris, 1997.

[2] Deming, W. E. *Out of the Crisis.* Cambridge: Massachusetts Institute of Technology, Center for Advanced Engineering Study, 1986.

[3] Deming, W. E. *The New Economics for Industry, Government, Education.* Cambridge: Massachusetts Institute of Technology, Center for Advanced Engineering Study, 1993.

[4] Covey, S. R. *Principle-Centered Leadership*. New York: Simon & Schuster, 1990.

[5] Geller, E. S. Managing occupational safety in the auto industry, J. *Organ. Behav. Manage.*, 10(1), 181, 1989.

[6] Geller, E. S. – Lehman, G. R. – Kalsher, M. R. *Behavior Analysis Training for Occupational Safety.* Newport: Make-A-Difference, Inc., 1989.

[7] Geller, E. S. *The psychology of safety handbook.* Florida: CRC Press LLC, 2001.

[8] Sloman, S. – Fernbach, P. *The Knowledge Illusion: Why We Never Think Alone*. New York: Riverhead Books, 2018.

[9] Glassner, B. *The Culture of Fear*. New York: Basic Books, 2018.

[10] Balázs I. (szerk.): *Pszichológiai lexikon*. Budapest: Magyar Könyvklub. 2002.

[11] Skinner, B. F. *Beyond Freedom and Dignity*. Indianapolis: Hackett Publishing Company, 2002.

[12] Maslow, A. *A Hierarchy of Needs: A Theory of Human Motivation*. New York: Prentice Hall, 1970.

[13] Papp G. *Maslow Piramis – A szükséglethierarchia*. Blog, https://pappgab.com/maslow-piramis-szukseglethierarchia (megtekintés: 2023.02.12.)

[14] Maslow, A. Self-actualization and beyond. In.: Bugenthal, J. F. T. (szerk.) *Challenges of Humanistic Psychology.* New York: McGraw-Hill. 1967.

[15] Herzberg, F. *Motivation and Hygiene*. Brighton: Harvard Business Review Press, 1959.

[16] Ryan, R. – Deci, E. *Self-Determination Theory: Basic Psychological Needs in Motivation, Development, and Wellness*. New York: Guilford Press, 2018.

[17] Bandura, A. *Social Learning Theory*. Hoboken: Prentice Hall, 1977.

[18] Pink, D. H. *Drive: The Surprising Truth About What Motivates Us*. New York: Riverhead Books, 2011.

[19] Kollár Cs. *Hackerpszichológia*. Az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Kutatók Éjszakája rendezvényen elhangzott előadás prezentációja. 2017. https://www.slideshare.net/drkollarcsaba/hackerpszichologia (megtekintés: 2023.02.12.)

[20] Oroszi E. *Social engineering – Az emberi erőforrás, mint az információbiztonság kritikus tényezője*. Budapest: Corvinus Egyetem, 2008.

[21] Oláh A. *Pszichológiai alapismeretek*. Budapest: Bölcsész Konzorcium, 2006.

[22] Lord, C. G. – Lepper, M. R. – Dean, S. R. *The Psychology of Attitudes.* Mahwah: Lawrence Erlbaum Associates, Inc., 1986.

[23] Douglas, M. – Wildavsky, A. *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers.* Berkeley: Uniersity of California Press, 1983.

[24] Bereczkei T. *Evolúciós pszichológia*. Budapest: Osiris Kiadó. 2008.

[25] Pinker, S. *The Better Angels of Our Nature: Why Violence Has Declined*. New York: Viking Press, 2011.

[26] Daly, M. – Wilson, M. *The Foundations of Evolutionary Psychology*. Mahwah: Lawrence Erlbaum Associates, 1998.
[27] Cole, M. – Cole, S. R. *Fejlődéslélektan*. Budapest: Osiris Kiadó, 1998.
[28] David, H. P. Unwantedness: Longitudinal studies of Prague children born to women twice denied abortions for the same pregnancy and matched controls. In. Ahmed, P. (szerk.) *Pregnancy, childbirth, and paranthood*. New York: Elsevier, 1981.
[29] Bates J. E. Concepts and measures of temperament. In. Kohnstamm, G. A. – Bates, J. E. – Rothbart, M. K. (szerk.) *Temperament in childhood*. New York: Wiley, 1989.
[30] Belsky J. – Most R. K. Infant exploration and play. In. Belsky, J. (szerk.) *In the beginning*. New York: Columbia University Press, 1982.
[31] Ekman, P. *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*. New York: W. W. Norton & Company, 2009.
[32] Bettelheim, B. *The Uses of Enchantment: The Meaning and Importance of Fairy Tales*. New York: Vintage Books, 2010.
[34] Bishop, J. H. Why the apathy in American high school? *Educational Researcher*, 18, 1989. pp. 6-10.
[35] Adelson, J. The political imagination of the young adolescent. In: Kagan J. – Coles R. (szerk.) *Twelve to sixteen: Early adolescence*. New York: W. W. Norton, 1972.
[36] Erikson, E. *Identity: Youth and Crisis*. New York: W. W. Norton, 1994.
[37] Kollár Cs. *A budapesti ifjúság fogyasztói csoportkultúrája az info-kommunikációs társadalomban, és ennek marketingkommunikációs aspektusai.* Budapest: PREMA Consulting, 2011.
[38] Gábor K. – Jancsák Cs. (szerk.) *Ifjúsági korszakváltás – Ifjúság az új évezredben*. Szeged: Belvedere, 2004.
[39] Bromley, D.B. *Az emberi öregedés pszichológiája*. Budapest: Gondolat Kiadó, 1972.
[40] Staudinger, U. M. – Lindenberger, U. *Understanding Human Development: Dialogues with Lifespan Psychology*. Berlin: Springer, 2012.
[41] DOYLE, C. E. *Work and Organizational Psychology: An Introduction with Attitude*. Oxfordshire: Routledge, 2004.
[42] Freudenberger, H. J. Staff Burn-out. *Journal of Social Issues*, 30, 1974. pp. 39-175.
[43] SZILÁGYI K. – VÁRY A. (szerk.) *A pszichés terhelés és a munkaközvetítés. A burnout jelenség.* Gödöllő: Gödöllői Agrártudományi Egyetem, 1997.
[44] Kollár Cs. *A munkahelyi kiégés (burnout szindróma) és annak hagyományos és alternatív terápiája.* Budapest: Prema Consulting, 2011.
[45] File B. *A vezető mint coach szerepe a munkahelyi burnout prevencióban*: http://www.hrcafe.eu/muhelymunka/a-vezeto-mint-coach-szerepe-a-munkahelyi-burnout-prevencioban (megtekintés: 2010.03.16.)
[46] Hézser G. *Miért? Rendszerszemlélet és lelkigondozói gyakorlat*. Pasztorálpszichológiai tanulmányok. Budapest: Kálvin Kiadó, 1996.
[47] NAGY E. *Egy segítő foglalkozás képviselőjének pályaképe a kiégés szempontjából.* Debrecen: Debreceni Egyetem BTK, 2007.

THE EMERGENCE OF ELEMENTS OF PSYCHOLOGICAL SAFETY IN EDUCATION DURING THE COMPLETION OF TEAM TASKS

A PSZICHOLÓGIAI BIZTONSÁG EGYES ELEMEINEK MEGJELENÉSE AZ OKTATÁSBAN A CSAPATFELADATOK ABSZOLVÁLÁSA SORÁN

MÉSZÁROS Ádám[1] – CSISZÁRIK-KOCSIR Ágnes[2]

Abstract

The concept of security can take many forms, from physical security to mental and emotional security. Today's rewritten economic system and the way organisations operate require new competences and skills that we have rarely seen before. Such new requirements include an agile approach, project orientation, but also teamwork, which has taken on a role never seen before. Agile methodologies also emphasise teamwork and responsibility, which is an integral part of a safe environment. Students also need a sense of security to perform well, which is also true for working in a team. In education, psychological safety can be affected by a number of factors. The aim of our study is to investigate the psychological safety factors that appear during a team task based on the results of a primary quantitative research.

Keywords

safety, teamwork, project approach, education, psychological safety

Absztrakt

A biztonság fogalma sokféleképpen megjelenhet a különböző fizikai biztonságoktól, a szellemi, érzelmi biztonságig. Napjaink újraírt gazdasági rendszere, a szervezetek működése olyan új kompetenciákat és készségeket igényel, melyekkel korábban csak elvétve találkoztunk. Ilyen új elvárások az agilis személetmód, a projektorientáció, de a csapatmunka is korábban nem látott szerepre tett szert. Az agilis módszertanokban is a csapatmunka és felelősség kiemelt fontosságú, mely szerves része a biztonságos közeg. A tanulmányaikat folytatónak is szükségük van a biztonságérzetre a megfelelő teljesítményért, mely a csapatban való munkavégzésre is igaz. Az oktatásban, a pszichológiai biztonságra számos tényező hathat. Tanulmányunk célja, hogy megvizsgálja azokat a pszichológiai biztonsági tényezőket, melyek megjelennek egy-egy csapatban végzett feladat során egy primer kvantitatív kutatás eredményei alapján.

Kulcsszavak

biztonság, csapatmunka, projektszemlélet, oktatás, pszichológiai biztonság

[1] meszaros.adam@uni-obuda.hu | ORCID: 0000-0002-5650-0448 | Ph.D. Student, Óbuda University, Doctoral School on Safety and Security Sciences | Ph.D. hallgató, Óbudai Egyetem, Biztonságtudományi Doktori Iskola
[2] kocsir.agnes@kgk.uni-obuda.hu | ORCID: 0000-0001-5454-7843 | Associate professor, Óbuda University, Keleti Károly Faculty of Business and Management | Egyetemi docens, Óbudai Egyetem, Keleti Károly Gazdasági Kar

BEVEZETÉS

A biztonság (angolul: safety) és a védelem (angolul: security) kifejezések a különféle tudományterületeken, valamint a különböző kontextusokban eltérően értelmezhetőek, beleérte a fizikai és nem fizikai jellegű definíciókat is. A biztonság, olyan állapotot jelent, ami az egészség vagy a jólét megőrzése érdekébenaz anyagi, fizikai vagy pszichológiai károkat okozó veszélyeket ellenőrzések ellenőrzés alatt vannak tartva, nyomatékosítva annak előmozdítását, ami különböző szinteken, különféle szereplőket jelent folyamat szinten [1]. A pszichológiai biztonságot aszerint lehet mérni, hogy a személy mennyire érzi magát magabiztosan és biztonságban abban, hogy a változásokat kezelni tudja [2].

Az olyan munkahelyek, melyek pszichológiailag biztonságosak hatalmast hatást tudnak tenni a munkahelyi csapatok eredményességére [3]. Az egyén belső motivációin és tanulási készségein túl fontos szerepe van a vezetőnek a csapatkörnyezet és -kultúra kialakításában, ahol az alkalmazottak úgy érzik, képesek tanulni kockázatvállalással és új készségek kipróbálásával, gyakorlással, gyors kudarcokkal, reflektálással és tanulással. A pszichológiailag biztonságos környezet megteremtésével a vezető megteremti a tanulási agilitás építéséhez és ápolásához szükséges feltételeket [4].

SZAKIRODALMI ÁTTEKINTÉS

A pszichológiai biztonság megjelenése a munkahelyi egészségen felül egy szélesebb társadalmi jólét érzéshez is társulhat, hiszen az egészséges munkahely vagy éppen az ott keletkező negatív hatások kihatnak a munkahelyen kívüli területekre is mint a család vagy közösség és így a társadalom egészére is hatással lehet [5]. A pszichológiai biztonság olyan érzést, légkört jelent, mely lehetővé teszi, hogy az emberek őszintén és nyíltan kommunikáljanak egymással, új ötleteket mondhatnak, eltérő véleményük lehet anélkül, hogy félnének a büntetéstől, a kirekesztéstől vagy a karrierjük károsodásától [6] [7]. A pszichológiai biztonság különböző kontextusokban egyéb kiterjedéseket kaphat, mint az egészségügyben, ahol a jobb betegellátást és a szakemberek nagyobb elkötelezettségét eredményezi, míg az oktatásban a tanulók pozitív fejlődését és szocializációját támogatja [6] [8].

A projektmenedzsmentben ez egy olyan alappillér, amelyre a sikeres csapatmunka, csapatteljesítmény és csapatdinamika épül. Ebben a környezetben a csapattagok nyíltan kommunikálhatnak elképzeléseikről, kockázatokat vállalhatnak, és támogatják egymást a közös célok elérésében anélkül, hogy félnének a hibázástól vagy a kritikától [9]. Ezen felül a nyílt kommunikáció hozzájárul, a tanuláshoz és az innovációkhoz a csapatokon belül, amelyek elengedhetetlenek a sikeres projektkimenetelekhez [10]. A pszichológiai biztonság a csapatmunka alapja, de kialakulását és erősítését számos tényező befolyásolja, mint például a vezetői stílus, az érzelmi intelligencia és a használt eszközök. Az érzelmi intelligenciával rendelkező vezetők, akik hitelesek és őszinték, képesek olyan légkört teremteni, ahol a csapattagok biztonságban érzik magukat, és nyíltan kifejezhetik véleményüket így jobb elköteleződéssel bírva a munka iránt [11] [12].

A virtuális csapatokban is támogatható a pszichológiai biztonság növelése és fejlesztése a különböző megfelelő kapcsolattartó eszközök segítségével a kommunikációs akadályok leküzdéséhez [13]. Azáltal, hogy a szervezetek értékelik és fejlesztik ezt a környezetet, a döntéshozatali folyamatok hatékonyabbá válnak, a kreativitás kibontakozik, és ezáltal versenyelőnyre tehetnek szert[14]. A projekt menedzselésének gyakorlata során a pszichológiai

biztonságnak prioritást kell élveznie a csapatok sikerének és a szervezeti hatékonyság biztosítása érdekében [15] [16]. A pszichológiai biztonság az Agile metodológiában a nyílt kommunikáció és az együttműködés elősegítése révén jelenik meg, amelyek alapvető elemei ennek a megközelítésnek [17] [18].

Az agilis módszertanok, például a Kanban vagy a Scrum, elősegítik a csapatok közötti átláthatóságot és a tudásmegosztást, ami egy olyan innovatív kultúra kialakítását eredményezi, ahol a csapattagok bátran kísérletezhetnek új ötletekkel és gyorsan alkalmazkodhatnak a piaci változásokhoz [19]. A pszichológiai biztonság a csapatok önreflexióját, azaz ösztönzi a csapatokat arra, hogy rendszeresen elemezzék saját működésüket és tanuljanak a tapasztalataikból és ez közvetlenül javítja a teljesítményt [17]. Az HR-esek aktív szerepük van egy vállalkozásban, azzal, hogy támogatják az agilis munkamódszereket úgy, hogy olyan kultúrát építenek, ahol a pszichológiai biztonság és a folyamatos fejlődés áll a központban [20].

A pszichológiai biztonság az oktatásban azt jelenti, hogy olyan tanulási környezet kerül kialakításra, ahol a tanulók biztonságban érzik magukat, és ezáltal jobban teljesítenek mind tanulmányaikban, mind társas kapcsolataikban. A pszichológiai biztonságnak óriási szerepe van az oktatásban, hiszen pozitív hatással van a tanulók érzelmi állapotára, a tanárok munkájára és a teljes tanulási folyamat minőségére [21] [8] [22]. Az érzelmi biztonság kulcsfontosságú a diákok pozitív személyiségfejlődéséhez, mivel elősegíti az önbizalom növekedését és a tanulási élmények javulását. Emellett az érzelmi biztonság erősíti a diákok értékérzetét és pozitív identitásuk kialakulását [8]. A tanárok pszichológiai biztonsága kulcsfontosságú a tanári munka hatékonyságának szempontjából. A pszichológiai biztonság ugyanis pozitív hatással van a tanárok jóllétére, tanári kitartására és közvetve a tanítási környezet minőségére is [22]. Mindez más biztonsági szempontokat is felvet, főként a mesterséges intelligencia korában. A téma az AI vezérelt világban kifejezetten fontossá válik, amit több tanulmány is hangsúlyoz [23] [24] [25] [26].

A projektív technikák alkalmazásával megbízhatóbb képet kaphatunk a diákok véleményéről az oktatási környezet biztonságát illetően, mivel ezek a módszerek lehetővé teszik a tudattalan tartalmak felszínre kerülését [21]. Az oktatási intézményekben a pszichológiai biztonság megteremtése egy összetett folyamat, amely megköveteli, hogy minden szereplő – tanárok, diákok, szülők – együttműködjön a támogató kapcsolatok kialakításában, a kölcsönös tiszteletben és a világosan meghatározott határok betartásában [8]. A tanulók biztonságérzete (pszichológiai biztonsága) szoros összefüggésben áll a tanulási tevékenységgel, pozitív hatással van a tanulók akadémiai eredményeire [27] [28]. Az oktatásban elsajátított kompetenciák pozitív hatással lesznek a munkavállalás során is, melynek szervezeti hasznossága megmutatkozik a későbbiekben az egyéni és a szervezeti versenyképességben is [29] [30] [31] [32] [33].

ANYAG ÉS MÓDSZER

A kutatáshoz egy 2024-es év Q2 és Q3 időszakában végzett, online kérdőív segítségével gyűjtött kvantitatív minta került felhasználásra. A felmérés Magyarországon zajlott teljesen anonim formában, hogy megfeleljen a hatályos adatvédelmi rendeleteknek (mint a GDPR). A kérdőív célcsoportja olyan tanulók, diákok, akik jelenleg is folytatják tanulmányaikat az oktatás különböző formáiban és területein. A kérdőív lehetőséget adott a már ta-

nulmányaikat befejező személyeknek is a válaszadásra, az Ő adataik is relevánsnak tekinthetők. A felmérés számos oktatással kapcsolatos fórumon, közösségi média csoportban és levelező listán került terjesztésre, melyben az egyetemi Hallgatói Önkormányzatok is segítettek. A kérdőívet 948 fő töltötte ki, melyek közül a „Nem tudom/nem válaszolok" válaszok kerültek kiszűrésre az egyes vizsgálatok során. Egyéb adattisztításra nem volt szükség. A kérdőív elkészítésében és az adatok gyűjtésében a Google Drive rendszerben található Google Űrlapok és Google Táblázatok alkalmazások voltak használva. Az adatgyűjtés végeztével, az adatok rendszerezésére, kódolására és a vizsgálatok tervezéséhez Microsoft Excel program, a statisztikai vizsgálatokra az IBM SPSS szoftvere volt használva. A statisztikai vizsgálatok során használt tesztek és mérések közé tartoztak a leíró statisztikák, hisztogram és eloszlás görbe, korreláció- valamint regresszió vizsgálatok, az egyszerű varianciaanalízis (one-way ANOVA), a hozzá kapcsolódó Tukey HSD post-hoc teszt, illetve a független mintás t-próba, és hatásméret számítás (Cohen's d).

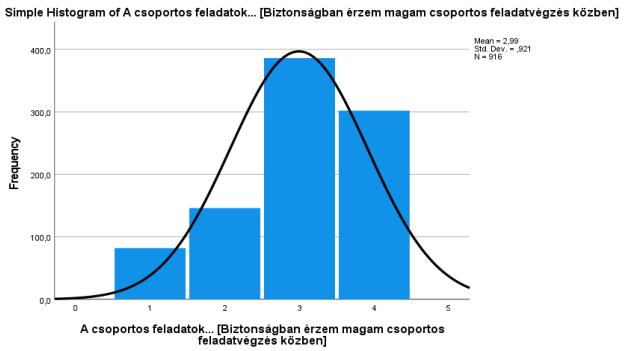
EREDMÉNYEK

A válaszadók átlagosan 2,99-es értékelést adtak a biztonságérzetükre a csoportos munkavégzés során. Ez az érték a skála felső határa felé közelít, ami azt jelzi, hogy a résztvevők többsége általánosságban biztonságban érzi magát ilyen helyzetekben. A válaszok között azonban némi szórás tapasztalható (0,921). A legalacsonyabb érték 1, a legmagasabb pedig 4 volt, ami azt jelenti, hogy voltak olyan résztvevők, akik egyáltalán nem, míg mások teljes mértékben biztonságban érezték magukat csoportos munkában.

	N	Min	Max	Átlag	Szórás	Variancia
Biztonságban érzem magam csoportos feladatvégzés közben	916	1	4	2,99	0,921	0,848

1. táblázat: Leíró statisztika: Biztonságérzet értelmezése
Forrás: Saját kutatás, 2024, N = 916

Az adatok viszonylag jól illeszkednek a normál eloszlás görbéjéhez, de van egy enyhe ferdeség, hiszen a legnagyobb sáv a 3-as értéknél található, ami azt jelenti, hogy a legtöbb válaszadó biztonságérzete közepes szintű (átlagosan biztonságban érzik magukat). A 4-es értéknél is jelentős számú válaszadó van, ami azt mutatja, hogy sokan teljes mértékben biztonságban érzik magukat



1. ábra: Hisztohram és normál eloszlás görbe: Biztonságérzet értelmezése Forrás: Saját kutatás, 2024, N = 916

A kutatás során azzal a feltételezéssel indult, hogy az egyes demográfiai jellemzők vagy a képzés alap tulajdonságai, jellemzői hatással lehetnek a bizalmi szintre. Azonban a különböző vizsgálatok során az az eredmény keletkezett, hogy sem a kitöltők neme (Férfi, Nő), a kitöltők kora (fiatalok, 22 év alatt, fiatal felnőttek – 22-30 év közöttiek és felnőttek – 30) év felettiek sem pedig a képzés szintje (gimnáziumi, diplomát nem adó, alapdiplomát adó és diplomára épülő képzések), annak tagozata (nappali vagy egyéb), sem a kitöltő jelenlegi évfolyama, de még a tanulmányai során elvégzett a csoportos feladatok száma sem hozott szignifikáns eredményt a biztonságra vonatkozóan. Az, hogy a tanulmányok során mit preferál jobban, ha maga választja a csapattársait, vagy ha beosztják (pl.: oktató által) csapatba, szintén nem mutatott szignifikáns eredményt. Így a biztonságérzet más aspektusok alapján került átvizsgálásra. A biztonságérzetnek (N=916, átlag= 2,99, szórás=0,921) és annak, hogy a válaszadók mennyire szeretek csoportokban dolgozni (N= 930, átlag=2,95 szórás=0,960) korrelációs vizsgálata a következő eredményt hozta:

		Biztonságérzet	Szeretek csoportokban dolgozni
Biztonságérzet	Pearson Correlation	1	0,662
	Sig. (2-tailed)		0,000
	N	916	914

2. táblázat: Korreláció: Biztonságérzet és Csoportos munka
Forrás: Saját kutatás, 2024, N = 916

A statisztikailag szignifikáns (Sig> 0,05) teszt alapján az eredmények erős pozitív korrelációt (Pearson féle korrelációs együttható=0,662) mutatnak a biztonságérzet és a csoportos munkavégzés kedvelése között. A kapcsolódó regressziós vizsgálat (R=0,662, R^2=0,438, F=711,645, Sig.=0,000, B=0,637) alapján a csoportos munkavégzés kedvelése a biztonságérzet varianciájának 43,8%-át magyarázza. Ez azt jelenti, hogy akik jobban kedvelik a csoportos munkát, általában magasabb biztonságérzetről számolnak be csoportos feladatvégzés közben.

Az, hogy a válaszadók önmagukra tekintve, mennyire gondolják jó csapatjátékosnak (N=948, átlag=3,30, szórás=0,738) magukat szintén összefügg a biztonsággal a korrelációs és regressziós vizsgálatok alapján.

		Biztonságérzet	Csapatjátékosság
Biztonságérzet	Pearson Correlation	1	0,324
	Sig. (2-tailed)		0,000
	N	916	916

3. táblázat: Korreláció: Biztonságérzet és Csapatjátékosság
Forrás: Saját kutatás, 2024, N = 916

Az eredmények mérsékelt pozitív korrelációt mutatnak a biztonságérzet és az önértékelés között (R=0,324, R^2=0,105, F=107,126, Sig.=0,000, B=0,410). Az csapatjátékossági önértékelés javulása mérsékelt mértékben növeli a biztonságérzetet A csapatjátékosság, a biztonságérzet varianciájának 10,5%-át magyarázza. A biztonságérzetre hathat, hogy a válaszadók, miként vélekednek a csoportos feladatok eredményeiről az egyéni feladatokéval szemben. A kérdőív erre irányuló kérdése: A csoportos feladatok eredményei általában jobbak, mint az egyéni feladatoké. (N= 930, átlag=2,95 szórás=0,960).

		Biztonságérzet	Eredményesség
Biztonságérzet	Pearson Correlation	1	0,469
	Sig. (2-tailed)		0,000
	N	916	874

4. táblázat: Korreláció: Biztonságérzet és eredményesség
Forrás: Saját kutatás, 2024, N = 916

A korrelációs együttható értéke= 0,469, közepes pozitív korrelációt mutatnak a biztonságérzet és a csoportos feladatok eredményességének megítélése között. Az eredmény szignifikáns (Sig>0,05). A kapcsolódó regressziós vizsgálat (R=0,469, R^2=0,220, F=238,768, Sig.=0,000, B=0,510) alapján elmondható, hogy a csoportos feladatok eredményességének megítélése a biztonságérzet varianciájának 22,0%-át magyarázza és az eredmény szignifikáns. Ez azt jelenti, hogy azok a válaszadók, akik úgy vélik, hogy a csoportos feladatok eredményei általában jobbak, magasabb biztonságérzetről számolnak be a csoportos feladatvégzés közben.

Az eredmények mellett érdemes a tananyag megértését is vizsgálni. Az erre vonatkozó kérdés: A csoportos feladatok segítenek jobban megérteni az anyagot (N=926, átlag= 2,74, szórás=0,965). A korreláció elemzés alapján szignifikáns, közepes és pozitív korreláció van a biztonságérzet és a csoportos feladatok anyagmegértési hatása között.

		Biztonságérzet	Jobb megértés
Biztonságérzet	Pearson Correlation	1	0,541
	Sig. (2-tailed)		0,000
	N	916	902

5. táblázat: Korreláció: Biztonságérzet és Feladatmegértés
Forrás: Saját kutatás, 2024, N = 916

A regressziós teszt alapján kimondható (R=0,541, R^2=0,292, F=371,685, Sig.=0,000, B=0,518), hogy azok a válaszadók, akik úgy vélik, hogy a csoportos feladatok segítenek jobban megérteni az anyagot, magasabb biztonságérzetről számolnak be a csoportos feladatvégzés közben. A csoportos feladatok anyagmegértési hatása a biztonságérzet varianciájának 29,2%-át magyarázza. A félévekben a csapatok összetételének alakulásakor one-way ANOVA vizsgálat készült a biztonságérzetre vonatkozóan. Ebben 4 kategóriába kerültek besorolásra a csapatösszetételek:

	N	Átlag	Szórás
Minden kurzusban / tárgyon ugyanabban a csapatban dolgozunk	90	3,00	0,821
Többnyire ugyanabban a csapatban dolgozunk	432	3,10	0,888
Kevésbé ugyanazzal a csapattal dolgozunk	94	2,89	0,886
Kurzusonként / tárgyanként eltérő csapatok vannak	236	2,87	0,981

6. táblázat: Csapatösszetételek alakulása
Forrás: Saját kutatás, 2024, N = 916

Míg a legtöbb csoport esetében nem a "Kurzusonként / tárgyanként eltérő csapatok vannak" és "Többnyire ugyanabban a csapatban dolgozunk" között szignifikáns különbség van (Sig=0,010). A Post Hoc tesztek alapján is szignifikáns különbség van a "Kurzusonként

/ tárgyanként eltérő csapatok vannak" és a "Többnyire ugyanabban a csapatban dolgozunk" csoportok között. A csapatösszetétel stabilitása pozitív hatással van a biztonságérzetre. Azok a hallgatók, akik gyakrabban dolgoznak ugyanazokkal a csapattagokkal, biztonságosabbnak érzik magukat a csoportos feladatvégzés közben.

A harmadik kutatási egység a motivációra és a biztonságérzetre vonatkozó vizsgálat. A „Motiválva vagyok csoportos feladatvégzés közben" kérdés (N=912, átlag=2,90, szórás=0,959) és a biztonságérzet korrelációs vizsgálata szignifikáns eredményt hozott.

		Biztonságérzet	Motiváltság
Biztonságérzet	Pearson Correlation	1	0,640
	Sig. (2-tailed)		0,000
	N	916	912

7. táblázat: Korreláció: Biztonságérzet és Motiváltság
Forrás: Saját kutatás, 2024, N = 916

A regresszió eredményei alapján (R=0,640, R^2=0,409, F=630,861, Sig.=0,000, B=0,615) megállapítható, hogy erős pozitív kapcsolat van a biztonságérzet és a csoportos feladatvégzés során érzett motiváció között. Ez azt jelenti, hogy azok a válaszadók, akik motiváltabbak a csoportos feladatvégzés során, magasabb biztonságérzetről számolnak be. Ez a kapcsolat statisztikailag szignifikáns ($p < 0,05$), és a csoportos feladatvégzés során érzett motiváció a biztonságérzet varianciájának jelentős részét magyarázza (40,9%). Minden egyes egységnyi növekedés a csoportos feladatvégzés során érzett motivációban 0,615 egységnyi növekedést eredményez a biztonságérzetben, ami erős hatást jelez.

A motiváció elsődleges feltételezett forrása az oktató. Így a biztonságérzet az oktatói motivációval is összefüggésbe hozható. A következő korrelációs elemzés így a biztonságérzet és a „Az oktatók motiválnak abban, hogy csoportosan végezzünk feladatokat" (N=922, átlag=2,97, szórás=0,882) kérdésekre vonatkozott.

		Biztonságérzet	Oktatói motiváció
Biztonságérzet	Pearson Correlation	1	0,218
	Sig. (2-tailed)		0,000
	N	916	896

8. táblázat: Korreláció: Biztonságérzet és Oktatói motiválás
Forrás: Saját kutatás, 2024, N = 916

Az eredmények gyenge pozitív korrelációt mutatnak a biztonságérzet és az oktatói motiváció között, hogy csoportosan végezzük el a feladatokat. A regressziós teszt (R=0,218, R^2=0,048, F=44,661, Sig.=0,000, B=0,228) alapján a következők mondhatók a mintáról: az eredmények gyenge pozitív korrelációt mutatnak a biztonságérzet és az oktatói támogatás között, hogy segíti a csapatmunkát és az önszerveződést. Ez azt jelenti, hogy akik úgy érzik, hogy az oktatók segítik a csapatmunkát és az önszerveződést, általában valamivel magasabb biztonságérzetről számolnak be.

Az oktatói oldalt tovább vizsgálva, a biztonságérzet az „Az oktató segíti a csapatmunkát, önszerveződést" (N=924, átlag=2,90, szórás=0,875) kérdés korrelációja gyenge de pozitív, szignifikanciát mutatott.

		Biztonságérzet	Oktatói segítség
Biztonságérzet	Pearson Correlation	1	0,268
	Sig. (2-tailed)		0,000
	N	916	896

9. táblázat: Korreláció: Biztonságérzet és Oktatói segítség
Forrás: Saját kutatás, 2024, N = 916

A regresszió eredményei (R=0,268, R^2=0,072, F=69,068, Sig.=0,000, B=0,283) alapján megállapítható, hogy gyenge pozitív kapcsolat van a biztonságérzet és az oktatói támogatás között, hogy segíti a csapatmunkát és önszerveződést. Ez azt jelenti, hogy azok a válaszadók, akik úgy érzik, hogy az oktatók segítik a csapatmunkát és az önszerveződést, valamivel magasabb biztonságérzetről számolnak be. Ez a kapcsolat statisztikailag szignifikáns (Sig<0,05), és az oktatói támogatás a biztonságérzet varianciájának csak egy kis részét magyarázza (7,2%).

KÖVETKEZTETÉSEK

A pszichológiai biztonság az oktatásban kulcsfontosságú tényező, amely hozzájárul a tanulók és tanárok jólétéhez, valamint az akadémiai és szociális eredményekhez. A tanulmányok alapján fontos, hogy az oktatási intézmények és a pedagógusok egyaránt törekedjenek egy támogató, biztonságos és inkluzív tanulási környezet kialakítására. A kutatás alapján a hallgatókat biztonsági érzetét nem a demográfiai jellemzők befolyásolják, hanem leginkább a csapatmunka gyakorlati része. A motiváció kiemelt fontosságú a biztonságérzet alakulásában, mert a motivált hallgatók nagyobb biztonságban érzik magukat az oktatás során és ebben az oktatóknak is fontos szerepe van. Ha a csoportmunkát az oktatói tevékenység során meglehet szerettetni a tanulókkal, akkor ez nagy hatással van a biztonságérzetükre, így a feladatok és a tananyag megértésére és a jobb eredmények elérésére is. A pszichológiai biztonság az oktatásban alapvető fontosságú, hiszen hozzájárul a tanulók és tanárok jóllétéhez, valamint az akadémiai és szociális fejlődésükhöz. A kutatások egyértelműen bizonyítják, hogy a támogató, biztonságos és befogadó tanulási környezet pozitív hatással van a tanulási eredményekre és a személyes fejlődésre. Az oktatási intézményeknek és a pedagógusoknak feladata, hogy olyan tanulási környezetet alakítsanak ki, ahol a tanulók és tanárok egyaránt biztonságban érzik magukat, és ahol a kölcsönös tisztelet és a támogatás jellemzi a kapcsolatokat.

FELHASZNÁLT IRODALOM

[1.] P. Maurice, M. Lavoie, L. Laflamme, L. Svanström, C. Romer, and R. Anderson, “Safety and safety promotion: definitions for operational developments,” International Journal of Injury Control and Safety Promotion, vol. 8, no. 4, pp. 237–240, Dec. 2001.
[2.] Newman, A., Donohue, R., & Eva, N., “Psychological safety: A systematic review of the literature,” Human Resource Management Review, vol. 27, no. 3, pp. 521-535, 2017.
[3.] Edmondson, A. C., & Bransby, D. P., “Psychological safety comes of age: Observed themes in an established literature,” Annual Review of Organizational Psychology and Organizational Behavior, vol. 10, no. 1, pp. 55–78, Nov. 14, 2022.

[4.] L. Stomski and K. Jensen, "Building Learning Agility Through Psychological Safety," in The Age of Agility: Building Learning Agile Leaders and Organizations, V. S. Harvey and K. P. De Meuse, Eds. New York: Oxford Academic, pp. 365–381, Aug. 19, 2021.
[5.] M. Shain, I. Arnold, and K. Germann, "The Road to Psychological Safety," Bulletin of Science, Technology & Society, vol. 32, no. 2, pp. 142–162, Apr. 2012.
[6.] N. Jamal, C. E. Schmalbach, J. Shapiro, M. J. Brenner, and V. N. Young, "Patient Safety/Quality Improvement Primer, Part IV: Psychological Safety-Drivers to Outcomes and Well-being," Otolaryngology--head and neck surgery: official journal of American Academy of Otolaryngology-Head and Neck Surgery, vol. 168, no. 4, pp. 881–888, Sep. 2022.
[7.] M. Kolbe et al., "Managing psychological safety in debriefings: a dynamic balancing act," BMJ simulation & technology enhanced learning, vol. 25, no. 3, pp. 164–171, Aug. 19, 2019.
[8.] M. Shean and D. Mander, "Building Emotional Safety for Students in School Environments: Challenges and Opportunities," Springer Singapore, pp. 225–248, 2020.
[9.] P. Paulus, "The Role of Psychological Safety in Team Communication: Implications for Human Resource Practices," Golden Ratio Of Mapping Idea And Literature Format, vol. 3, no. 2, pp. 156–166, Jun. 2023.
[10.] K. Swart, T. Bond-Barnard, and R. Chugh, "Challenges and critical success factors of digital communication, collaboration and knowledge sharing in project management virtual teams: a review," International Journal of Information Systems and Project Management, vol. 10, no. 4, pp. 59–75, Nov. 2022.
[11.] T. K. I. Adham and A. Sukkar, "Effective Management of Construction Project Team: Identifying Leadership Qualities and Responsibilities," Scholars Journal of Economics, Business and Management, vol. 11, no. 02, pp. 63–73, Feb. 2024.
[12.] N. Maximo, L. Coxen, and M. W. Stander, "Authentic leadership and work engagement: The indirect effects of psychological safety and trust in supervisors," SA Journal of Industrial Psychology, vol. 45, May 2019.
[13.] J. Binder, "Global Project Management: Communication, Collaboration and Management across Borders," Strategic Direction, vol. 25, no. 9, Aug. 2009.
[14.] R. Reiter-Palmon and M. Millier, "Psychological Safety and Creativity," Cambridge University, pp. 559–576, 2023.
[15.] S. R. Harper and C. D. White, "The Impact of Member Emotional Intelligence on Psychological Safety in Work Teams," Journal of Behavioral and Applied Management, vol. 15, no. 1, Sep. 2013.
[16.] M. J. Rothouse, "Establishing Trust and Authentic Communication Among Organizational Teams," Springer, pp. 69–81, 2020.
[17.] A. Tkalich and M. Buvik, "Psychological Safety in Agile Software Development Teams: Work Design Antecedents and Performance Consequences," Sep. 30, 2021.
[18.] C. Trivedi, C. M Witt, and F. Aminalroayae, "Product Innovation Using Agile Practices in Supply Chain Management Curriculum," International Journal of Business & Management Studies, vol. 5, no. 5, pp. 51–61, May 2024.
[19.] S. Chahal, "Agile Methodologies for Improved Product Management," Journal of Business and Strategic Management, vol. 8, no. 4, pp. 79–94, Sep. 2023.

[20.]F. Ajayi and C. Udeh, “Agile Work Cultures in IT: A Conceptual Analysis of HR’s Role in Fostering Innovation Supply Chain,” International Journal of Management & Entrepreneurship Research, vol. 6, no. 4, pp. 1138–1156, Apr. 2024.
[21.]I. Litvinenko and L. Bogdan, “Psychological diagnosis of the safety of the educational environment of the educational institution,” Scientific Visnyk V.O. Sukhomlynskyi Mykolaiv National University. Psychological Sciences, no. 1(20), pp. 17–21, Jan. 2020.
[22.]E. A. Shmeleva, N. I. Kolchugina, T. K. Phan, and P. A. Kislyakov, “Hardiness and psychological safety of a teacher in an educational environment,” Образование и наука, vol. 24, no. 9, pp. 143–173, Nov. 2022.
[23.]Cs. Kollár, A mesterséges intelligencia megjelenése a biztonságtudományban. In: T. J. Karlovitz (szerk.) What will our Future be Like? 2 essays in German, 7 in English, 30 in Hungarian language, Grosspetersdorf: Sozial und Wirtschafts Forschungsgruppe, 2023, 448 p. pp. 242-256. , 15 p.
[24.]Z. Rajnai and B. Fregan, “Kritikus infrastruktúrák védelme (jogi szabályozás),” Műszaki Tudományos Közlemények, vol. 5, pp. 349–352, 2016, doi: 10.33895/MTK-2016.05.78.
[25.]Cs. Kollár, "A biztonság megjelenése a humán tudományokban (1. rész)," Biztonságtudományi Szemle / Biztonságfilozófia és -történet, vol. 6, no. 2, pp. 13-22, 2024.
[26.]Cs. Kollár, "A mesterséges intelligencia kapcsolata a humán biztonsággal," Nemzetbiztonsági Szemle, vol. 6, no. 1, pp. 5-23, 2018.
[27.]A. Arifin, S. Suryaningsih, and O. Arifudin, “The Relationship Between Classroom Environment, Teacher Professional Development, and Student Academic Performance in Secondary Education,” International Education Trend Issues, vol. 2, no. 2, pp. 151–159, Mar. 2024.
[28.]B. R. Werang, “Exploring the Simultaneous Impact of Parental Support, School Environment, Teacher Morale, and Student Learning Motivation on Student Academic Performance,” International Journal of Religion, vol. 5, no. 2, pp. 510–520, Mar. 2024.
[29.]M. Garai-Fodor, L. Vasa, and K. Jäckel, “Characteristics of consumer segments based on perceptions of the impact of digitalisation,” Decis. Mak.: Appl. Manag. Eng., vol. 6, no. 2, pp. 975-993, 2023.
[30.]M. Garai-Fodor, L. Vasa, and K. Jäckel, “Characteristics of segments according to the preference system for job selection, opportunities for effective incentives in each employee group,” Decis. Mak.: Appl. Manag. Eng., vol. 6, no. 2, pp. 557-580, 2023.
[31.]J. Varga, “A szervezetek versenyképességének alapjai: a vállalati versenyképesség erősítésének lehetőségei,” in Vállalkozásfejlesztés a XXI. században: VII. tanulmánykötet, Á. Csiszárik-Kocsir, Ed. Budapest, Magyarország: Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2017, pp. 725-743.
[32.]J. Varga, “SMEs as the innovation flagships - where are the real economic drivers?” in IEEE 23rd International Symposium on Computational Intelligence and Informatics (CINTI 2023) Proceedings, Danvers (MA), USA, pp. 373-377.
[33.]J. Varga, “The potential benefits of innovation as seen by some domestic businesses,” in SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics, Budapest, Magyarország: IEEE Hungary Section, pp. 223-228.

EXAMINATION OF GAS AND ALARM WEAPONS, THE ACQUISITION AND POSSESSION OF THEM

GÁZ-ÉS RIASZTÓFEGYVEREK, MEGSZERZÉSÜK ÉS TARTÁSUK SZABÁLYOZÁSÁNAK VIZSGÁLATA

MORVAY László[1] – SZŰCS Endre[2]

Abstract

"COMMISSION IMPLEMENTING DIRECTIVE (EU) 2019/69 of 16 January 2019 laying down technical specifications for alarm and signal weapons under Council Directive 91/477/EEC on control of the acquisition and possession of weapons" entered into force in our country on January 1, 2023 directive that redefines the concept of individual firearms as well as technical parameters of gas- and alarm weapons. The referenced EU 69/2019 Implementation Directive entered into force on January 1, 2021 as Annex No. 2 of XXIV of 2004 Firearms and Ammunition Act and defines the system of requirements for gas and alarm weapons. After a brief historical overview of gas and alarm weapons, the article presents the types of gas-alarm weapons. Subsequently, EU Implementation Directive 69/2019 and related legislation will examine the modified conditions for the classification, technical parameters, placing on the market, acquisition and possession of weapons.

Keywords

gas and alarm weapons, weapons law, Directive (EU) 2019/69, gas cartridges, alarm cartridges, gas-alarm agents

Absztrakt

Hazánkban 2023. január 01-től lépett életbe a „Bizottság (EU) 2019/69 végrehajtási irányelve (2019. január 16.) a fegyverek megszerzésének és tartásának ellenőrzéséről szóló 91/477/EGK tanácsi irányelv szerinti riasztó- és jelzőfegyverekre vonatkozó műszaki előírások meghatározásáról” irányelv, amely újra definiálja az egyes tűzfegyverek fogalmát, valamint a gáz. és riasztófegyverek műszaki paramétereit. A hivatkozott EU 69/2019 Implementációs direktíva a 2004. évi XXIV. törvény a lőfegyverekről és lőszerekről 2. számú mellékleteként 2021. január 1-én emelkedett jogerőre és határozza meg a gáz- és riasztófegyverek követelményrendszerét. A cikk a gáz- és riasztófegyverek rövid történeti áttekintése után bemutatja a gáz-riasztó fegyverek típusait. Ezt követően az EU 69/2019 Implementációs direktíva, valamint a kapcsolódó jogszabályok vizsgálatán keresztül foglalkozik a fegyverek besorolásának, műszaki paramétereinek, forgalomba hozatalának, beszerzésének és tartásának módosított feltételeivel.

Kulcsszavak

gáz- és riasztófegyverek, fegyvertörvény, (EU) 2019/69 Direktíva, gáztöltény, riasztótöltény, gáz-riasztó hatóanyagok

[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

INTRODUCTION

The first domestically produced gas pistols were manufactured at the Arms and Machine Factory Joint Stock Company founded in Budapest on February 24, 1891, after the company merged with the Metal and Lamp Factory Joint Stock Company (Lampart) in 1935. [4] Over the next few decades, the legal environment governing their commercialization, purchase and possession was, from today's point of view, contradictory. For example, BM Decree 2/1968 only laid down regulations regarding their purchase, and did not cover their possession. In many cases, those entitled to purchase have purchased gas and alarm weapons for others, illegally putting weapons into the hands of unauthorized persons. [1] After the change of regime, Government Decree No. 115/1991 (IX.10.) was published on small arms and ammunition, gas and alarm weapons, as well as air guns and shooting ranges, which already provided a comprehensive legal background for the acquisition and possession of gas and alarm weapons. [1] The contents of this legislation provided the legal background for the legal purchase of gas and alarm weapons offered by Hungarian arms manufacturing companies appearing after the regime change. Hungary joined the European Union as a full member on 1 May 2004, and through the related legislative harmonization, Act XXIV of 2004 on Firearms and Ammunition and Government Decree No 253/2004 of 31 August 2004 on arms and ammunition were established. This legislation is based on Council Directive 91/477/EEC of 18 June 1991 on control of the acquisition and possession of weapons, as amended several times. The latest amendment to Implementing Directive (EU) 2019/69 on gas and alarm weapons entered into force in Hungary on 1 January 2023 as Annex 2 to Act XXIV of 2004.

DEFINITION, CLASIFICATION AND TECHNICAL PARAMETERS OF GAS-ALARM WEAPONS

According to Section § 2 (32) of Act XXIV of 2004 on Firearms and Ammunition, "gas and alarm weapons: devices which are only suitable for operating gas cartridges and alarm cartridges." [2] The law therefore classifies both types into one category, but it is worth distinguishing between these two types on the basis of their ammunition, their use and the purpose for which they are used.

Alarm weapon

Eur.Ing. Frank Gy. et al. (1995), "the operation of an alarm weapon actually mimics the light and sound effect of a real firearm." [1, p. 52] It is worth noting, however, that the appearance of the alarm weapon is the same as that of a handgun capable of directly killing, therefore the deterrent power of the alarm weapon cannot be neglected. Its cartridge does not contain a projectile, therefore it can be used primarily for alarm, signalling, surprising the attacker, and stopping and, if necessary, averting the attack. The requirement of a permit to carry an alarm weapon is strongly justified, because alarm weapons can cause serious injury or, in extreme cases, death, despite the absence of a projectile, especially in the case of innocent, negligent or knowingly violation of the rules. This can occur if the shot is fired directly at the body surface (e.g. head) or on thin clothing. The magnitude of the safe distance depends on the calibre of the weapon. [1]

Gas weapon

In its construction, operation and design, it is basically identical to the alarm weapon, the difference is to be found in the cartridges used. The solid tear-exciting substance placed in its cartridge becomes gaseous due to the high temperature and pressure generated when the weapon is fired and escapes through the barrel of the weapon in the direction of the attacker, into the open air. The effect of the gas cloud is close to that of tear gas sprays, but may be more effective due to the significant light and sound effects associated with firing and the increased range due to higher pressure. [1] Depending on the active ingredients used in the cartridge, which will be described in detail later, the inability to fight is between 5 and 15 minutes. [6] Figure 1 shows a human test with a gas weapon using a 9 mm PAK cartridge with the active substance CN (chloroacetophenone). The use of the weapon is visibly effective because it has a serious effect on the target.

Figure 1: Gas weapon in use [13]

CALIBRE FOR GAS-ALARM PISTOLS

Like live weapons, gas pistols have different calibres, but in the case of gas pistols – in the absence of a projectile – the calibre is equal to the diameter of the cartridge-case.[1] Figure 2 shows the range of alarm and gas cartridges:

Figure 2: Ammunition used in gas-alarm pistols [7]

6 mm flóbert platz

Figure 3: 6 mm flóbert platz gas and alarm cartridge [7], [14]

The mouth of cartridge-case of the alarm (start) cartridge is contracted like a star. In the gas version, 60-65 mg of chloroacetophenone gas-forming agent and wax/paraffin wad/insulation are placed above the initiating agent in the form of crystalline powder, as shown in Figure 3. Gunpowder is not contained in either version, the cartridge-case is soft copper. It has a range of 1-1.5 meters, which is comparable to the range of gas spray. Typically cartridges for gas and alarm weapons with a sliding block magazine. [7]

.22 Lang Knall alarm cartridge

Figure 4: .22 Lang Knall alarm cartridge [15]

Figure 4 shows the .22 Lang Knall alarm cartridge. The rim-firing 15mm long .22 LR cartridge-case delivers impressive volume and is effective from 2 meters. The gas charge is always chloroacetophenone, up to a maximum of 125 mg. [7]

.315 Knall

Figure 5: .315 Knall alarm cartridge [15]

The .315 Knall alarm cartridge shown in Figure 5 is the smallest cartridge for self-loading pistols. The centrefire cartridge with groove is filled with smokeless gunpowder, the length of the brass cartridge-case is 15 mm. The gas pressure is 45 MPa, which exceeds the significantly larger 9 mm PAK cartridge, and the range is 3-3.5 meters. [7]

9 mm Knall

Figure 6: 9 mm Knall cartridge [15]

The 9 mm Knall cartridge shown in Figure 6 is a flanged centrefire cartridge with a cartridge-case length of 17 mm, plastic cap and cartridge-case material with a contracted closure. It is filled with nitro powder as a gas cartridge and contains black powder or a mixture of the two as an alarm cartridge. Its range exceeds 3 meters, and its gas pressure is 26 MPa. [7]

9 mm PAK

Figure 7: 9 mm PAK alarm cartridge [16]

The 9 mm PAK alarm cartridge shown in Figure 7 is a cartridge with a 22 mm cartridge-case length, groove and centrefire system for self-loading gas-alarm weapons. It has a gas pressure of up to 45 MPa, an average range of 4 meters, and its sound and muzzle fire have a truly deterrent effect. [7]

CONSTRUCTION, FUNCTION AND ACTIVE SUBSTANCES OF GAS CARTRIDGES

The primary purpose of the gas cartridge is non-lethal self-defence, its effect is achieved by special gases emanating from the cartridge when fired. In terms of structure, its parts are: cartridge-case, initiating agent, crystalline active substance (wrapped in a protective film) and wad. The force caused by the firing pin forces the initiating agent to explode, and then the crystalline material sublimates from the heat released. Due to the increase in pressure caused by the developed gas, the front of the cartridge-case opens and the active substance forms a cloud in the form of a gas cloud. Irritants come into contact with skin or mucous membrane or if they are inhaled. [8] The type of charge is indicated by colours for grooved cartridges for semi-automatic gas weapons and by the mark milled into the base for flanked cartridges made for revolvers. [8]

A summary of the different active substances is given in Table 1.

Name	Active ingredient	Colour	Effect	Note
alarm cartridge	no	green	no	-
CS	o-chlorobenzylidene malononitrile (80 mg)	yellow	Mucous membrane irritation, coughing, lacrimation, vomiting	if the target person is under the influence of alcohol, it is less effective; burning, stinging eyes and very severe tearing, skin irritation
CN	chloroacetophenone (220–240 mg)	blue, purple, black	Cough, tearing	It is outdated, weak in terms of its effect, harmful to health
PV OC	pelargonic acid vanillylamide / oleoresin capsicum (20, 45, 120 mg)	brown, red, orange	Mucous membrane irritation, coughing, lacrimation, vomiting	State-of-the-art, natural active substance (capsaicin) It is also called paprika. (pepper).
CR	Dibenzoxazepine (20, 45, 120 mg)	-	Cough, lacrimation, temporary blindness, vomiting	Banned in Europe! It has 6-10 times the effect of CS. It has a serious health-damaging effect.

Table 1: Chemical properties and physiological effects of irritant chemicals most commonly used in gas cartridges (or gas sprays) of gas-alarm weapons [8]

The physical and chemical properties of some of the active substances listed in Table 1, the symptoms caused by their use, first aid information in case of symptoms, exposure and health effects, potential environmental hazards and management tasks are set out in International Chemical Safety Cards issued within the framework of a project of the World Health Organisation (WHO) and the International Labour Organisation (ILO) with the European Commission.

o-chlorobenzylidene malononitrile

Formula: ..... $C_{10}H_5ClN_2$ / $ClC_6H_4CH=C(CN)_2$
Molecular weight: ..... 188.6 g/mol
Boiling point: ..... 310-315 °C
Melting point: ..... 93-96 °C
Solubility in water: ..... at 20 °C: 0.1-0.5 g/100ml
Vapour pressure: ..... 0.0045 Pa
Relative vapour density (air=1): ..... 6.5 [20]

In terms of physical condition and appearance, it is a white, crystalline powder with a characteristic odour, which reacts with strong bases and strong acids, forming ammonia. On combustion, it decomposes, resulting in toxic fumes containing hydrochloric acid, hydrogen cyanide and nitrogen oxides. In terms of routes of exposure, the substance can be absorbed by inhalation, dermal or ingestion. [20]

Chloroacetophenone

Formula: ..... C_8H_7ClO / $C_6H_5COCH_2Cl$
Molecular weight: ..... 154.6 g/mol
Boiling point: ..... 244-245 °C
Melting point: ..... 54-59 °C
Density: ..... 1.3 g/cm³
Solubility in water, at 25 °C: 1.64 g/100ml
Vapour pressure at 20 °C: ..... 0.7 Pa
Relative vapour density (air=1): 5.3
Relative density of the vapour/air-mixture at 20 °C (air=1): 1.0
Flash point: ..... 118° C
Octanol/water partition coefficient as log Pow: ..... 2.08 [21]

Colourless or pale grey crystals decompose on combustion, forming toxic and corrosive fumes that also contain hydrochloric acid. The substance may enter the body by inhalation and ingestion. In terms of its short-term exposure effects, it causes lacrimation, severe irritation of the eyes, skin and respiratory tract. Inhalation of vapour or aerosol causes pulmonary oedema. [21]

Pelargonic acid vanillylamide

Molecular formula: ..... $C_{17}H_{27}NO_3$
Molar mass: ..... 293,4 g/mol
State of matter: ..... solid
Form: ..... powder
Colour: ..... white - whitish - light yellow
Odour: ..... pungent
Melting point/Freezing point: ..... 52 – 57 °C
Flash point: ..... 190 °C
Density: ..... 1,1 g/cm³ at 25 °C [22]

When burning white, whitish or light-yellow powder, nitrogen oxides (NOx), carbon monoxide (CO) and carbon dioxide (CO_2) are formed. The substance causes severe skin irritation, allergic skin reaction, severe eye irritation and respiratory tract irritation. [22]

Capsicum oleoresin (Capsaicin)

Molecular formula: ..... $C_{18}H_{27}NO_3$
Molar mass: ..... 305,4 g/mol
State of matter: ..... solid
Form: ..... crystalline powder
Colour: ..... white - whitish - light yellow
Odour: ..... odourless
Melting point/Freezing point: ..... 62 – 65 °C
Boiling point: ..... 210 °C
Flash point: ..... 113 °C [23]

The active ingredient extracted from red chili pepper (capsaicin). It is a skin irritant causing severe eye irritation and respiratory irritation. It can be ingested by inhalation, absorption through the skin and ingestion route of exposure. When capsaicin is burned, nitrogen oxides (NOx), carbon monoxide (CO) and carbon dioxide (CO_2) can be formed. [23]

Dibenzoxazepine

Molecular formula: ..... $C_{13}H_9NO_{\_}$
Molar mass: ..... 195,22 g/mol
Density: ..... 1,160±0,10 g/cm^3
State of matter: ..... solid
Form: ..... crystalline powder
Colour: ..... pale yellow
Odour: ..... pepper-like
Mlting point: ..... 73 °C [24]

It is poorly soluble in water, does not decompose in it. At room temperature, it is a micro-grained, pale-yellow substance with a pepper-like odour. Its effect is 6-10 times stronger than CS gas (o-chlorobenzylidenemalononitrile). Its effects include intense skin irritation, temporary blindness, coughing, wheezing, panic. It can cause immediate incapacitation and is thought to have carcinogenic effects. [24]

GROUPING OF GAS WEAPONS

According to their system of operation, three types of gas weapons are distinguished:

- sliding block magazine,
- revolver,
- self-charging. [1]

Gas pistols with sliding block magazine

The gas pistols with sliding block magazine have the calibre of 5.6-6 mm and a copper-sleeved, rim-firing cartridge. On the left side of Figure 8 is the gas cartridge filled with tear-exciting material. The opened mouth of cartridge-case is covered with red wax, which refers to the active substance (capsaicin) in the cartridge. The mouth of cartridge-

case of the alarm cartridge shown to the right of the picture is contracted. For both cartridges, the cartridge base is filled with fulminating powder. In the gas cartridge, the tear-exciting material is located above the fulminating powder. [1]

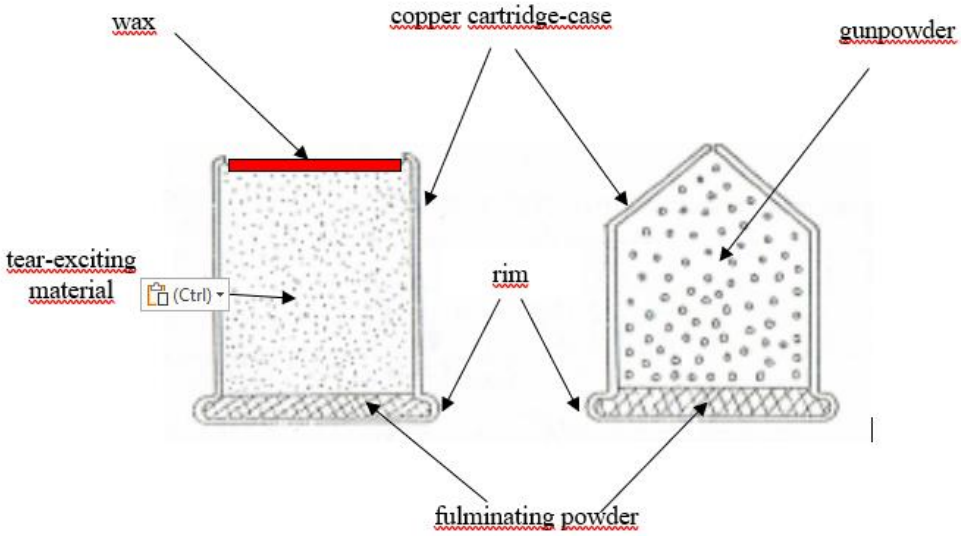


Figure 8: 6 mm flóbert platz gas-alarm cartridge [1]

Figure 9: sliding block magazine [17]

Next to the cartridge holes, the sliding block magazine shown in Figure 9 has grooves necessary for the operation of the forwarding arm. The structure of the gas pistol with a sliding block magazine is shown in Figure 10.

Figure 10: Gaspistol with a sliding block magazine [6] és [1, p.55.]

Its advantage is a constant state of readiness for fire, small size and less sensitivity to dirt. The disadvantages are the small range (1-2 m) due to the small volume size, the insignificant sound effect in particularly open space, the cumbersome reloading and the considerable effort required to pull the trigger back. [1]

Revolvers

Figure 11: Revolver [6], [1, p.58.]

The calibre of gas revolvers shown in Figure 11 are 5.6 (.22) and 9 (.38) mm and therefore use 5.6 mm rim-firing and 9 mm flanged, centre-firing cartridges with copper cartridge-case, which are depicted in Figure 12. [1]

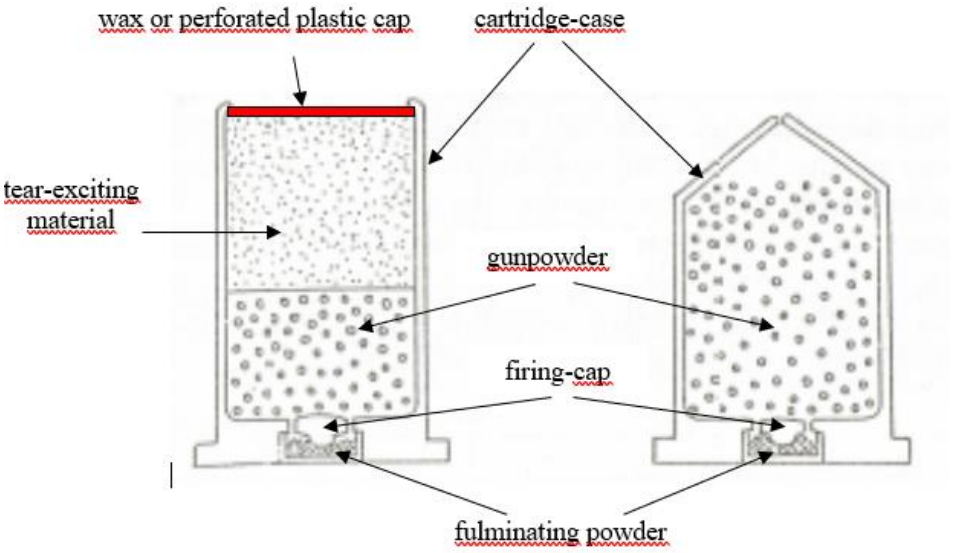


Figure 12: – Gas- and alarm cartridge of revolvers [1, p.57.]

The rotary drum is cast iron with a carbide insert that partially covers the chamber to prevent projectiles from leaving the barrel. It can only operate with its own flanged cartridge, and with other, more powerful cartridges, the drum explodes during firing, causing serious injuries to the user of the weapon. Such a state after an explosion can be seen in Figure 13. [1]

Figure 13: Gas weapon exploded due to improper use of ammunition [18]

Its range is 3-3.5 meters with 6 mm ammunition, while with 9 mm ammunition it averages 4-5 meters, but in favourable weather conditions (low humidity, tailwind, clean air) it can reach 10 meters. Depending on the structural design, the rotary magazine can hold 5-12 rounds and can be made of steel, spiater (Zn-AL-Cu casting) or aluminium. [6] The gas revolver is less sensitive to dirt and bullet pressure variations, and its construction is relatively simple and therefore reliable. The disadvantage is that emptying used cartridge cases and then reloading the magazine, especially in dark conditions, is cumbersome and lengthy. The capacity of the rotary magazine is limited and not all types have a fuse mechanism, so the latter are not protected from accidental discharge. [1]

Self-loading gas pistols

Figure 14: - Self-loading gas pistol [19] és [1, p.63].

The self-loading gas pistol shown in Figure 14 has the same structure and structure as civilian and military semi-automatic pistols with live ammunition, but in the case of gas pistols there is a plate 2 mm thick along the longitudinal axis of the barrel along the entire length and diameter of the barrel, which prevents a projectile from leaving the muzzle of the weapon. Their material is usually spiater, with a magazine capacity of 5-12 rounds. 8 and 9 mm grooved, centre-ignition, copper-sleeved cartridges can be loaded into the magazine. They can be fired with tear gaseous cartridges (CS, OC/PV, CN — see Table 1) or with simple alarm cartridges. [6]

The different coloured plastic pressed into the cartridge-case indicates that it is not an alarm cartridge but a gas cartridge, and the colour of the plastic also indicates the strength of the active substance in the cartridge. The cone colour of the alarm cartridge may be white or green, while that of the gas cartridges may be yellow, red or blue, as shown in Table 1. [1]

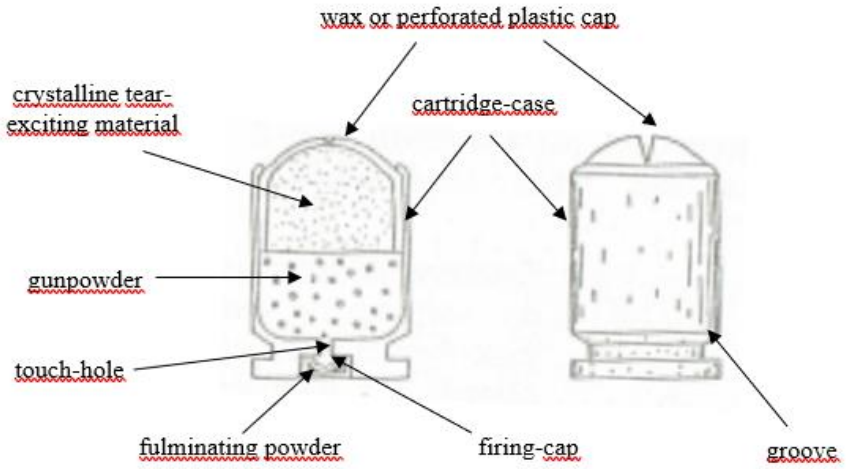


Figure 15: Gas- and alarm cartridge of self-loading gas weapons [1, p.62.]

In the case of the gas cartridge shown Figure 15, the firing-cap in the cartridge-base is used to ignite the gunpowder charge. The gunpowder charge placed above the touch-hole is exploded through the touch-hole by a jet flame from the fulminating powder in the firing-cap. Above the gunpowder charge, in the plastic cone but still inside the cartridge-case, there is a crystalline tear-exciting substance, which is transformed into a gaseous substance under the influence of heat effect and pressure from the combustion of gunpowder. [1]

All self-loading gas pistols must be insured against accidental discharge, which is achieved by two solutions: in the case of cheaper types, they mechanically prevent the trigger from being pulled back, while in the case of more expensive gas weapons with a complex firing mechanism, the movement of the firing pin is prevented. [1] The barrel narrowing shown in Figure 16, the 2 mm steel-plate hook in the barrel as shown in Figure 17, and the eccentric bore shown in Figure 18 are used against the use of live ammunition or rubber shell. [6]

Figure 16: Barrel narrowing [6]

Figure 17: Steel-plate hook in the barrel [10]

Figure 18:Eccentric bore [6]

The signal rocket extension shown in Figure 19 can be screwed into the thread formed on the inner surface of the muzzle, but its use is subject to legislation in Hungary. [6]

Figure 19: Signal rocket extension with signal rocket [9]

The technical parameters of gas alarm weapons should also be summarised in tabular form for a better overview. The summary is given in Table 2.

PARAMETER	SLIDING BLOCK MAGAZINE	REVOLVER	SELF LOADING PISTOL
Caliber [mm]	5,6 – 6	5,6 9	8 9
Magazine capacity [pcs]	6	5-12	5-18
Cartridge	copper cartridge-case, rim-firing	copper cartridge-case, rim-firing (5,6 mm) copper cartridge-case, flanged centrefire cartridge (9 mm)	grooved, centrefire cartridge with copper cartridge-case
Range [m]	1-2	3-3,5 (5,6 mm) 4-5 (9 mm)	< 10

Table 1: Technical parameters of gas-alarm weapons (authors' own editing)

The advantages and disadvantages of gas-alarm weapons listed above are shown in Table 3.

TYPE	ADVANTAGES	DISADVANTAGES
Sliding block magazine	Permanent ready to fire. Small size (can be carried in a pocket). Low sensitivity to impurities. No firing chamber.	Low range (1-2 m). Insignificant sound effect (outdoors). Cumbersome manual reloading. Significant force required to pull back the trigger.
Revolver	It is less susceptible to contamination and variations in cartridge peak pressure than a self-loading gas weapon. Relatively simple mechanics, therefore reliable.	Manual emptying and refilling are cumbersome, lengthy (especially in the dark). Limited capacity. Due to the absence of a locking device, there is a risk of accidental discharge.
Self-loading pistols	It is only necessary to pull it up before the first shot. High rate of fire. Indicates that the library is empty. Fast and safe recharging. Range: 10-12 meters. It can be carried in a pocket unobtrusively.	Sensitive to contamination and variations in cartridge peak pressure. Headwinds, snowfall, rain reduce the range.

Table 2:- Pros and cons of gas-alarm weapons (authors' own editing)

REGULATION OF THE ACQUISITION, POSSESSION AND CARRYING OF GAS AND ALARM WEAPONS

According to the legislation in force, gas and alarm weapons can be purchased and kept freely, but their carrying is subject to a permit. The permit can be applied for by any adult citizen (over 18 years of age) Hungarian citizen who has unlimited capacity of action, without criminal record, solely for self-defence purposes, if he or she has the theoretical and practical knowledge necessary for the carrying and lawful use of a weapon. [5]

Section 3/A(2) of Act XXIV of 2004 on Firearms and Ammunition lists in detail the grounds for refusal in which an applicant may not be issued with a permit to carry weapons. These include:

- criminal record,
- no criminal record, but the court has found the applicant criminally responsible [2]

The carrying of both types of weapons for self-defence purposes is subject to an official permit according to Section 4 (2) of Government Decree 253/2004 (VIII.31) on weapons and ammunition, namely that "the carrying of gas and alarm weapons shall be permitted by the police station competent for the place of residence of the applicant, or by the Budapest Police Headquarters in Budapest."[3] In order to conduct the procedure, a form downloadable from the website of the Police must be filled in and sent to the competent Police Station. The application for a permit to carry gas and alarm weapons for self-defence can also be submitted through the Client Gate using Form RI-0600.

Government Decree No. 253/2004 (VIII.31.) on arms and ammunition pursuant to Section 38 (1) (a) (not quoting the text of the Act verbatim): weapons may be transported in built-up areas, public places, public means of transport only with empty magazines, weapons and ammunition separately, in a closed box, and all measures must be taken to prevent them falling into unauthorized hands. Even with a permit to carry a gas weapon, it can only be carried concealed (e.g. covered by clothing). Under the influence of alcohol, narcotic drugs or other psychotropic substances, gas and alarm weapons may not be carried. [3]

According to Section 6 (6) of Government Decree No 253/2004 (VIII.31) on arms and ammunition, "Gas and alarm weapons may be brought into the territory of the country or traded if they do not contain a firearm and are unsuitable for firing solid projectiles." [3]

LEGISLATIVE CHANGES FROM 01 JANUARY 2023

On 01 January 2021, the amendment to Act XXIV of 2004 on Firearms and Ammunition entered into force, where the technical requirements of EU Implementation Directive 69/2019 became part of the Act in Annex 2. According to experts, the amendment, which entered into force on January 1, 2023, mainly affects manufacturers, importers and traders. [10]

The legislation does not have retroactive effect, therefore the treatment of gas and alarm weapons put into circulation before 2023 and the permits issued for them will not change, the weapons will remain gas and alarm weapons, and valid carrying permits will still be valid. (Act XXIV of 2004, § 2, 32 cb))

Annex 2 appearing in the amendment of Act XXIV of 2004 on Firearms and Ammunition that entered into force on 01 January 2021 contains the following. (Due to changes in the legal environment, it is worth going through the individual passages in detail and interpreting them.)

Annex 2 to Act XXIV of 2004

'Technical specifications for gas and alarm weapons

1. *A device with its own chamber which is intended to operate only gas or alarm cartridges shall be regarded as a gas and alarm weapon if:*
   - 1.1. *they are capable of shooting pyrotechnic signalling rounds only if an adaptor at the muzzle is attached;" [25]*

According to point 1.1, e.g. Röhm RG77, RG79 or Reck King Cobra, which contain an integrated signal rocket launcher, cannot be manufactured and placed on the market in the future. It is worth noting that lawmakers do not set an energy limit on the missile launcher extension and do not impose an obligation to clearly mark the extension with the weapon.

- 1.2. *„they have a durable device within the device that prevents the firing of cartridges loaded with single or multiple solid shots, solid bullets or solid projectiles;" [25]*

The term 'durable device' may give rise to confusion because the legislator presumably did not mean a separate instrument, but rather an obstacle already well-known, such as the barrel narrowing, steel-plate hook and eccentric bore shown in Figures 17, 18 and 19 shown in this article.

1.3. *„they are designed for a cartridge listed in, and complying with the dimensions and other standards referred to in, Table VIII of the Tables of Dimensions of Cartridges and Chambers (TDCC) established by the Permanent International Commission for the Proof of Small Arms (C.I.P.), as that Table applies in the version in effect at the time of adoption of this Directive." [25]*

Point 1.3 is effectively the subject of Article 2 of this Article, which entered into force on 16 January 2019. It represents a freeze on cartridge sizes in the EU, meaning that the existing supply of cartridges will not be expanded in the future. This is likely to reduce the willingness to innovate to some extent.

1.4. *„The devices are not capable of being modified through the use of ordinary tools to expel, or to become capable of being converted to expel, a shot, bullet or projectile by the action of a combustible propellant.*

1.5. *All essential components of the devices are such that they cannot be fitted or used as essential components of firearms.*

1.6. *Barrels of the devices are not capable of being removed or modified without significantly damaging or destroying the device." [25]*

Under clause 1.6, the conversion of tipper-barrelled shotguns into gas-alarm weapons will be prohibited, with some types being excused by welding off barrel removal elements.

1.7. *„In the case of devices with a barrel not exceeding 30 centimetres or whose overall length does not exceed 60 centimetres, the device incorporates irremovable barriers along the full length of the barrel such that a shot, bullet or projectile is not able to pass through the barrel by the action of a combustible propellant, and such that any free space left at the muzzle is no more than 1 cm in length." [25]*

Section 1.7 therefore EXCLUDES rubber bullet gas revolvers from legal compliance.

1.8. *„In the case of devices not falling within point 1.7, the device incorporates irremovable barriers on at least one third of the barrel length such that a shot, bullet or projectile is not able to pass through the barrel by the action of a combustible propellant, and such that any free space left at the muzzle is no more than 1 cm in length." [25]*

According to experts, point 1.8 applies to gas-alarm rifles, where the law does not require the obstruction to run along the entire length of the barrel, it is sufficient to place the hook on one-third of the tail side. [10]

1.9. *„the first barrier in the barrel is placed as close as possible after the chamber of the device while allowing the expulsion of gases through exit holes.*

1.10. *For devices designed to fire only blanks, the barriers referred to in point 1.7 or point 1.8 wholly block the barrel apart from one or more exit holes for gas pressure. In addition, the barriers wholly block the barrel in such a way that no gas can be fired from the front of the device." [25]*

Section 1.10 applies to old starter pistols used exclusively as alarm weapons and Western traditional weapons.

1.11.„All barriers are permanent and incapable of being knocked out without destroying the chamber or barrel of the device.

1.12.For devices designed to fire only blanks, the barriers are wholly made of a material which is resistant to being cut, drilled, bored or ground (or any similar process) and which has a minimum hardness of 700 HV 30 (according to the Vickers hardness test).

1.13.For devices not covered by the second subparagraph of this point, the barriers are made of a material which is resistant to being cut, drilled, bored or ground (or any similar process) and which has a minimum hardness of 610 HV 30. The barrel may have a channel along its axis to enable the irritants or other active substances to be expelled from the device.

1.14.The barriers are such that they prevent occurrence of the following:

(a) creation or enlargement of a hole in the barrel along its axis;" [25]

Here, the legislature presumably meant a kind of hole or opening by the name "hole".

„b) removal of the barrel, except where the frame and chamber area of the device is rendered useless as a result of the removal, or where the integrity of the device is so compromised that it cannot be used to form the basis of a firearm without significant repair or addition.

1.15.The cartridge chamber and barrel are both offset or tilted or staggered in such a way as to prevent ammunition from being loaded in and fired from the device." [25]

The longitudinal axis of the chamber and the part of the barrel of the weapon fitted with the hook must not overlap. It is important that there is an OR relationship between the above, i.e. either one can be applied, the simultaneous use of all three named solutions ("offset, tilted or staggered") is not required.

CONCLUSIONS, PROPOSALS

The purchase of gas-alarm weapons is not subject to a permit, their carrying is already regulated by law. Keeping them requires care, discipline and skill to ensure that weapons and ammunition do not fall into the hands of unauthorized persons, especially children. In stressful situations, gas and alarm pistols are easier to use, if lucky, they render the attacker unable to fight for a while, the weapon and ammunition are relatively cheap to obtain, and due to their small size, the weapons can be conveniently placed in a small bag or pocket. However, due to the short range, in an unfortunate case (headwinds or confined spaces), the user may also be endangered by the active substance intended for the attacker.

Perceived or actual deterioration of public safety, especially in some areas of large cities, may encourage people living locally and in the surrounding area to carry an alarm or gas weapon for safety. However, these advantages can create a false sense of security in the owner of the weapon, which can be fatal for him in the given situation, and therefore the wearer should receive comprehensive education. This should be an integral part of an information forum of its kind to make known to those concerned the circumstances of those considering buying and carrying gas-alarm weapons. Here, potential buyers would have the opportunity to clarify for what purpose they are buying a gas-alarm weapon. Knowing the

purpose of buying and wearing it can help them decide what type and size of weapon to buy. As legislators, it would be worth considering that already in high school, graduates should become familiar with the laws and regulations referred to several times, paying particular attention to knowledge about the possession, carrying and use of weapons. Experienced experts could introduce young people to gas-alarm weapons through practical demonstrations, where "live" shooting would also take place.

In Hungary, security guards performing armed service in the private security sector (factories, companies, cooperatives, etc.) currently possess and carry gas-alarm weapons, which can be justified by deterrence, a greater range than gas spray, and self-defence purposes while performing the task. The gas-alarm weapon can also be named as an alternative to gas spray, therefore we recommend its use also for persons performing public tasks, primarily serving in law enforcement directorates, such as public space inspectors, members of the animal protection guard service and members of the nature conservation guard service (mountain guard, fish guard).

The amendments to the law are mainly about how to prevent the use of live ammunition and rubber bullets in alarm and gas weapons, suggesting that easy access to these types of weapons leads to an increasing number of abuses. In order to verify this phenomenon and to determine the evolution of the number of injuries and crimes resulting from irregular and unlawful transformations, it would be worthwhile to carry out separate research in the future.

Manuscript completed on 14 September, 2024.

REFERENCE

[1] Eur.ing. Frank György – Kováts László – Nán Jenő – Tóth Lóránd: Fegyverismeret – Jegyzet a biztonságtechnikai mérnök hallgatók részére I. kötet – PRO LEX Oktató és Szolgáltató Kkt. – Budapest, 1995
[2] 2004. évi XXIV. törvény a lőfegyverekről és lőszerekről
[3] 253/2004. (VIII. 31.) Korm. rendelet a fegyverekről és lőszerekről
[4] Új magyar lexikon VIII.: Kiegészítő kötet (A–Z, 1962–1980). Szerk. Maros Istvánné, Zsilinszky Sándor Budapest: Akadémiai. 1981. ISBN 963-05-3852-0 ISBN 963052803 7 sorozat ISBN 963 05 2810 X kiegészítő kötet, p.167.
[5] Dr. Bokros Gábor: Jog & Fegyver – Kaliber Magazin Vol.105, January, 2007, http://drbokros.hu/wp-content/uploads/2012/09/105.-sz%C3%A1m-2007.-janu%C3%A1r.pdf, (downloaded: 14.09.2024.)
[6] Bartha Tibor - ÓE-BGK – Őrzésvédelem, fegyverismeret I. tantárgy – oktatási anyag (pptx) – Gáz_riasztó_fegyverek (23rd January, 2009 – 27 pages)
[7] Vass Gábor: Gáz-riasztó kaliberek, https://web.archive.org/web/20090227015918/http://www.gazpisztoly.hu/gazpisztoly/kaliberek.14.php (downloaded: 14.09.2024.)
[8] Vass Gábor: Hatóanyagok, https://web.archive.org/web/20090227170754/http://www.gazpisztoly.hu/gazpisztoly/cn_cs_oc_cr.10.php (downloaded: 14.09.2024.)
[9] Vass Gábor – Tűzijáték gázpisztolyból, https://web.archive.org/web/20090213193214/http://gazpisztoly.hu/gazpisztoly/tuzijatek.8.php, (downloaded: 14.09.2024.)

[10] Vass Gábor: Ez lesz a gázpisztoly 2023-tól! – Kaliber Info (14.09.2024.), http://www.kaliberinfo.hu/cikkek/ez-lesz-a-gazpisztoly-2023-tol/, (downloaded: 14.09.2024.)
[11] Új magyar lexikon 6. kötet (S–Z). Szerk. Berki Andor Budapest: Akadémiai Kiadó 1962. p.330.
[12] Nádasdy Ferenc: Alapmérések – Anyagvizsgálatok, Nemzeti Tankönyvkiadó / Tankönyvmester Kiadó, 2001, ISBN 963 92 6490 3, p.47
[13] CN humán teszt – 9 mm PAK gázpisztolyból, Kaliberinfó, 31st May 2013. http://www.kaliberinfo.hu/fegyvervideok/human-teszt/cn-human-teszt-9-mm-pak-gazpisztolybol/ (Downloaded: 14.09.2024.)
[14] Geco schreckschuss platzpatronen kal. 6mm flobert - 300 stück, shoot-club GmbH, https://www.shoot-club.de/Geco-Schreckschuss-Platzpatronen-Kal-6mm-Flobert-300-Stueck (downloaded: 14.09.2024.)
[15] .22 lang knall, 4komma5 Outdoor & Shooting Equipment GmbH, https://www.4komma5.de/index.php?jtl_token=f036e23582be74174c05b52f50cc1ee096afa2809ddb565491cd8ffc0cae2502&qs=.22+lang+knall&search= (downloaded: 14.09.2024.)
[16] Walther 9mm PAK, Tüskevár vadászbolt, https://tuskevb.hu/shop/walther-9mm-p-a-k/ (downloaded: 14.09.2024.)
[17] Csúszótár gáz-riasztó pisztolyhoz – 1, Vatera.hu, Extreme Digital-eMAG Kft., https://www.vatera.hu/csuszotar-gaz-riaszto-pisztolyhoz-1-3212838056.html (downloaded: 2022.10.16.)
[18] Vass Gábor – Hogyan tedd tönkre a Pitbullodat? - http://www.kaliberinfo.hu/cikkek/hogyan-tedd-tonkre-a-pitbullodat/, 6th November 2017 (downloaded: 14.09.2024.)
[19] EKOL Volga gázpisztoly fekete, Halcapone Vadász és Horgászcentrum, https://www.halcapone.hu/Ekol-Volga-Gazpisztoly-Fekete, (downloaded: 14.09.2024.)
[20] Nemzetközi Kémiai Biztonsági Kártyák – ICSC adatbázis – ILO, (o-KLÓRBENZILIDÉN)MALONONITRIL, ICSC: 1065 (September, 2002) https://www.ilo.org/dyn/icsc/showcard.display?p_lang=hu&p_card_id=1065&p_version=2 (downloaded: 14.09.2024.)
[21] Nemzetközi Kémiai Biztonsági Kártyák – ICSC adatbázis – ILO, KLÓRACETOFENON, ICSC: 0128, (2002 augusztus) https://www.ilo.org/dyn/icsc/showcard.display?p_card_id=0128&p_version=2&p_lang=hu (downloaded: 14.09.2024.)
[22] Biztonsági adatlap, Pelargonsav vanillilamid ≥97 %, Roth, Issued: 26th April, 2016, Reviewed: 15th July, 2021. https://www.carlroth.com/com/en/aliphatic-carboxylic-acids/pelargonic-acid/p/7015.1 (downloaded: 14.09.2024.)
[23] Biztonsági adatlap, Kapszaicin, Roth, Issued: 23rd January, 2017., Reviewed: 1st January,2024, https://www.carlroth.com/com/en/more-reference-substances/capsaicin/p/8804.1 (downloaded: 14.09.2024.)
[24] Gijsen HJ, Berthelot D, Zaja M, Brône B, Geuens I, Mercken M. " Analogues of morphanthridine and the tear gas CR as extremely potent activators of the human TRPA1 receptor ". J Med Chem. 53 (19): 7011–7020. doi: 10.1021/jm100477n. PMID 20806939. (downloaded: 14.09.2024.)

[25] COMMISSION IMPLEMENTING DIRECTIVE (EU) 2019/69 of 16 January 2019 laying down technical specifications for alarm and signal weapons under Council Directive 91/477/EEC on control of the acquisition and possession of weapons. L 15/22; 17.1.2019. (downloaded: 14.09.2024.)

THE EVOLUTION AND FUTURE OF SOCIAL ENGINEERING: EXPLOITING PSYCHOLOGICAL VULNERABILITIES IN THE DIGITAL AGE

A SOCIAL ENGINEERING FEJLŐDÉSE ÉS JÖVŐJE: A PSZICHOLÓGIAI SEBEZHETŐSÉGEK KIHASZNÁLÁSA A DIGITÁLIS KORBAN

MÁRTON Zoltán[1] – RAJNAI Zoltán[2]

Abstract

The study presents the history, evolution, and current threats of social engineering, with a focus on exploiting human psychological vulnerabilities. It discusses both early and modern techniques, such as spear phishing, pretexting, and deepfake manipulation, which are becoming even more targeted with the use of artificial intelligence and machine learning technologies. The study also addresses defense strategies, emphasizing the importance of education, technological safeguards, and strict organizational protocols, while highlighting the future risks of social engineering and the need for continuous protective measures.

Keywords

social engineering, psychological vulnerabilities, spear phishing, pretexting deepfake manipulation, Artificial intelligence, machine learning, cybersecurity, defense strategies, organizational protocols

Absztrakt

A tanulmány a social engineering történetét, fejlődési irányait és jelenlegi fenyegetéseit mutatja be, különös tekintettel az emberi pszichológiai sebezhetőségek kihasználására. Bemutatásra kerülnek a korai és modern technikák, mint a „spear phishing”, „pretexting” és a „deepfake” manipuláció, amelyek a mesterséges intelligencia és a gépi tanulás technológiákkal még célzottabbá válnak. A tanulmány kitér a védekezési stratégiákra is, kiemelve az oktatás, technológiai védelem és a szigorú szervezeti protokollok fontosságát, valamint figyelmeztet a social engineering jövőbeli veszélyeire és a folyamatos védelem szükségességére.

Kulcsszavak

social engineering, pszichológiai sebezhetőségek, spear phishing, pretexting, deepfake manipuláció, mesterséges intelligencia, gépi tanulás, kiberbiztonság, védelmi stratégiák, szervezeti protokollok

[1] marton.zoltan@uni-obuda.hu | ORCID: 0009-0006-7795-076X | PhD Student, Doctoral School on Safety and Security Sciences Obuda University | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] rajnai.zoltan@uni-obuda.hu | ORCID: 0000-0002-9139-736X | professor, Obuda University, Banki Donat Faculty of Mechanical and Safety Engineering | egyetemi tanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A social engineering az információbiztonság egyik leggyorsabban fejlődő területe, mivel a támadók egyre kifinomultabb eszközöket alkalmaznak az emberi pszichológiai sebezhetőségek kihasználására. Az ilyen típusú támadások középpontjában az emberi természet alapvető jellemzői, mint a bizalom, segítőkészség és kíváncsiság állnak, melyeket a támadók manipuláció révén használnak ki a céljaik elérésére. A social engineering a technológiai fejlődéssel párhuzamosan fejlődik: a digitális kommunikáció és az online adatmegosztás növekedésével egyre több támadási csatorna válik elérhetővé a támadók számára, legyen szó e-mailes, közösségi média vagy mobilalapú támadásokról.

A tanulmány célja, hogy átfogó képet nyújtson a social engineering technikák történeti fejlődéséről és jelenlegi alkalmazásairól, bemutatva a legelterjedtebb támadási formákat és azok pszichológiai alapjait. Emellett részletesen kitér a védekezési stratégiákra, melyek segítségével a szervezetek és egyének csökkenthetik a social engineering támadások kockázatát. A jövőbeli kilátások ismertetésével a tanulmány felhívja a figyelmet azokra az új technológiákra, mint a mesterséges intelligencia és gépi tanulás, amelyek lehetőséget adnak a támadások további személyre szabására és hatékonyságuk növelésére.

A SOCIAL ENGINEERING FOGALMA ÉS KORAI PÉLDÁI

A social engineering technikái alapvetően az emberi pszichológia sajátosságain alapulnak, és a támadók tudatosan kihasználják az olyan ösztönös emberi tulajdonságokat, mint a bizalom, a segítőkészség, a félelem, vagy a kíváncsiság. [1] Ezeknek a pszichológiai tényezőknek a kihasználásával a támadók az áldozatokból olyan cselekvéseket váltanak ki, amelyek különben nem állnának szándékukban, így tehát érzékeny információkat adnak át vagy jogosulatlan hozzáférést biztosítanak rendszerekhez. [2] A támadások pszichológiai háttere különösen hatékonynak bizonyul, mivel az emberek többsége nem rendelkezik megfelelő ismeretekkel és tudatossággal a social engineering technikáival szemben, és így hajlamosak információkat kiadni akkor is, ha a kérés forrása gyanúsnak tűnhet. [3] A támadók gyakran építenek a hatóság, a szakmai hierarchia vagy a sürgősség érzetére, melyek mind hatást gyakorolhatnak az áldozatok döntéseire, különösen olyan helyzetekben, ahol a felhasználók saját kritikus gondolkodásukat háttérbe szorítva cselekszenek. [4]

Korai social engineering technikák

A korai social engineering módszerek a manipuláció alapvető, de hatékony technikáira épültek, melyek már ekkor bizonyították a támadók pszichológiai hatalomgyakorlásának erejét. Az egyik legismertebb módszer a „pretexting” volt, amely során a támadók kidolgozott fedősztorikkal operáltak, és mesterséges helyzeteket hoztak létre annak érdekében, hogy az áldozatokat megtévesszék és a hitelesség látszatát keltsék. [2] Ilyenkor a támadók egy megbízható személy, adott esetben egy banki alkalmazott vagy kormányzati tisztviselő képviselőjeként jelentek meg, így növelve annak esélyét, hogy az áldozatok önként rendelkezésre bocsájtsák a bizalmas információkat. [1]

A „baiting” technika különösen alattomos volt, hiszen a támadók olyan csalogató eszközöket – „talált” USB-meghajtókat vagy ingyenes szoftvereket – használtak, amelyekkel kihasználták az áldozatok természetes kíváncsiságát. Az ilyen eszközöket a támadók kártékony szoftverrel fertőzték meg, amely az áldozat rendszerébe kerülve azonnal aktiválódott, ezzel lehetővé téve a támadó számára a rendszer teljes körű hozzáférését. [4] Az

ilyen korai technikák rávilágítanak arra, hogy a social engineering hogyan használja ki a felhasználói figyelmetlenséget és bizalmat, kihasználva az emberi természet alapvető hajlamait az adathalászat, rendszerhozzáférés és további kártékony tevékenységek eléréséhez. [3]

A social engineering kezdeti hatékonysága és jelentősége

A social engineering korai története világosan bemutatja, hogy a támadók miként igazodtak az adott korszak technológiai és társadalmi környezetéhez, folyamatosan tökéletesítve módszereiket. E technikák nemcsak egyszerű manipulációs eszközök voltak, hanem alapvető szociálpszichológiai törvényszerűségekre építkeztek, amelyek a bizalom, a segítőkészség, valamint a félelem ösztönös emberi reakcióit használták ki. [1] Az emberi természet ezen alapvető jellemzőinek kihasználása révén a social engineering lehetővé teszi, hogy a támadók az áldozatok viselkedését precízen irányítsák, gyakran az áldozatok tudtán kívül. [3]

A módszer történelmi jelentősége különösen abban rejlik, hogy rámutat az emberi tényező sebezhetőségére, amely semmilyen technikai védelemmel nem küszöbölhető ki teljesen. Az emberek természetes reakcióit nem képesek befolyásolni még a legkifinomultabb kiberbiztonsági rendszerek sem. A social engineering ezen sebezhetőség kiaknázására épült, és alapját képezi a modern kibertámadási módszereknek, amelyek napjainkban is jelentős fenyegetést jelentenek. [2] A korai technikák, mint a „pretexting” és „baiting”, megágyaztak azoknak a kifinomult támadási formáknak, amelyek csak folyamatos oktatással, a felhasználói tudatosság növelésével, valamint a szociálpszichológiai tényezők mély megértésével kezelhetők hatékonyan. [3]

FEJLŐDÉSE ÉS A SOCIAL ENGINEERING EVOLÚCIÓJA

Az internet megjelenése és az e-mail alapú támadások

Az internet térhódítása forradalmi hatást gyakorolt a social engineering technikák fejlődésére, új lehetőségeket nyitva a támadók számára, és ezáltal jelentős kihívást jelentve az információbiztonság számára. [1] Az e-mail alapú adathalászat, vagy „phishing”, az egyik legelterjedtebb módszerré vált, mivel viszonylag alacsony költséggel és kockázattal jár a támadók számára, ugyanakkor széleskörű elérhetőséget biztosít számukra. Az ilyen támadások során az e-mailek gyakran hivatalos szervezetek - bankok vagy neves vállalatok nevében érkeznek, és megtévesztő tartalommal manipulálják a felhasználókat, arra ösztönözve őket, hogy bizalmas információikat – jelszavaikat és banki azonosítóikat – kiadják.

A Verizon Data Breach Investigations Report (2021) adatai szerint a kibertámadások több mint 90%-a social engineering technikákra épít, különösen az adathalászat révén, amely egyre finomodik és egyre több formát ölt. [5] Az e-mailes adathalászat különböző típusai, a hamis számlaértesítések és megtévesztő promóciós ajánlatok, tovább növelték a social engineering fenyegetését azáltal, hogy az áldozatok hitelesség iránti bizalmára építenek, így könnyen manipulálhatók a gyanútlan felhasználók.

Közösségi média és social engineering

A közösségi média platformok, mint a Facebook, Twitter vagy Instagram, új csatornákat nyitottak a social engineering számára, mivel a felhasználók személyes információkat osztanak meg, amelyeket a támadók célzott támadások kivitelezésére használnak fel.

[1] Ezeken a platformokon végzett adatgyűjtés során a támadók képesek részletes személyes profilokat kialakítani az áldozatok kapcsolatai, érdeklődési körei és mindennapi tevékenységei alapján, lehetővé téve a támadások finomhangolását és a személyre szabott megközelítést. Ezen közösségi oldalak különösen alkalmassá teszik a „spear phishing" típusú támadások lebonyolítását, ahol a támadók konkrét személyeket céloznak meg az emberek közösségi kapcsolatait és online viselkedési mintáit kihasználva, így növelve a siker valószínűségét. [5], [6]

Mobiltechnológia és social engineering

A mobiltelefonok és okoseszközök széles körű elterjedése új támadási felületeket biztosított a social engineering számára. Az SMS-alapú adathalászat, vagy „smishing", valamint a hangalapú adathalászat, azaz „vishing", lehetőséget adnak a támadóknak arra, hogy közvetlen üzenetekben, sürgősséget színlelve manipulálják áldozataikat. [4] Az ilyen támadások gyakran fenyegető vagy sürgető üzeneteket tartalmaznak - banki műveletek vagy szolgáltatások felfüggesztésének hivatkozásával -, amellyel az áldozatokat azonnali cselekvésre késztetik. A mobil eszközök adathalászat elleni védelme kiemelt biztonsági kihívás, mivel a felhasználók gyakran kevésbé körültekintőek mobil eszközeiken, mint asztali környezetben, így nagyobb eséllyel válnak támadások áldozataivá.

MODERN SOCIAL ENGINEERING TECHNIKÁK

„Spear phishing"

A „spear phishing" célzott adathalász támadás, amely során a támadók részletes információgyűjtést követően egy adott személyt vagy szervezetet céloznak meg, hogy megtévesszék és érzékeny adatokat szerezzenek tőle. [5] A támadók gyakran átfogó kutatást végeznek a célpontjukról, beleértve annak munkahelyi szerepét, érdeklődési köreit, szokásait és közösségi média jelenlétét, hogy az üzenet a lehető leghitelesebbnek tűnjön. Az ilyen típusú támadások sokkal kifinomultabbak, mint az általános „phishing" kísérletek, mivel a személyre szabott üzenetek fokozzák a hitelességet, és növelik a siker esélyét. Konkrét esetet nézve, egy pénzügyi vezető számára küldött üzenet belső üzleti szabályozásokra hivatkozhat, vagy akár valós kapcsolati neveket és eseményeket tartalmazhat, hogy elérje a kívánt manipulációs hatást. [8]

A „spear phishing" támadások jellemzően alaposan megtervezettek, hogy a hagyományos biztonsági szűrők elől rejtve maradjanak. Ezt a hatást a támadók egyre gyakrabban mesterséges intelligencia segítségével érik el, amely képes a célpont online aktivitását figyelemmel kísérni, és az érdeklődési körök alapján optimalizálni a támadási módszereket. [8] Az 1. ábrán látható a „spear phishing" támadás teljes folyamata, amely bemutatja a támadó adatgyűjtési fázisától kezdve a célzott üzenet kidolgozásán át egészen az áldozat reakciójáig.

1. ábra - A "spear phishing" támadás lépései (saját ábra)

A „spear phishing” támadás lépései

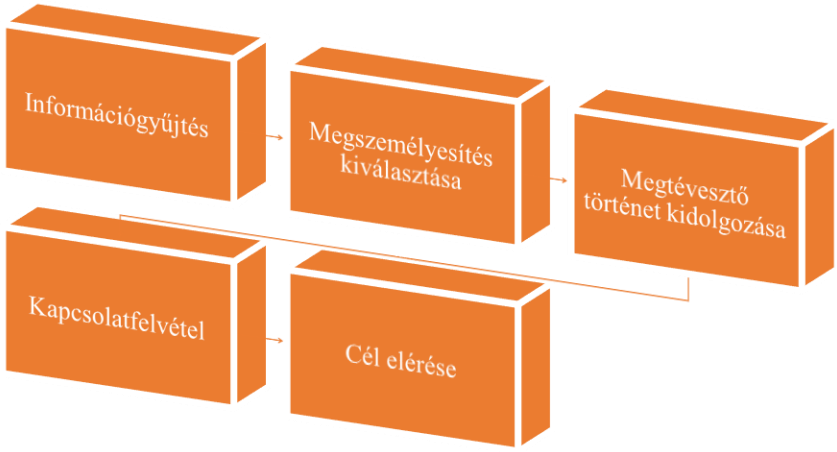
- A támadó kiválaszt egy konkrét személyt vagy szervezetet, akit célba kíván venni. Ezt követően részletes információkat gyűjt róla, beleértve személyes, szakmai vagy online jelenlétéhez kapcsolódó adatokat, hogy a támadás hitelesnek tűnjön és növelje a megtévesztés esélyét.
- Az információgyűjtést követően a támadó egy hitelesnek látszó e-mailt hoz létre, amely megfelel a célpont érdeklődési körének, szakmai környezetének vagy kapcsolatainak. Az üzenet formázása és tartalma a megtévesztést szolgálja, gyakran megbízhatónak tűnő forrásként, például egy ismerős személy vagy szervezet nevében érkezik.
- A célpont megkapja az e-mailt, és amint megnyitja vagy rákattint az üzenetben található linkre, a rosszindulatú program aktiválódik. Ez lehet egy rejtett malware, amely hozzáférést biztosít a támadónak a célpont eszközeihez vagy hálózatához.
- Miután a rosszindulatú program települt, a támadó hozzáférést nyer a célpont érzékeny adataihoz, beleértve bizalmas információkat, jelszavakat vagy egyéb fontos adatokat, amelyeket később visszaélés céljából felhasználhat.

„Pretexting”

A „pretexting” egy kifinomult social engineering technika, amelynek célja, hogy a támadó előre megtervezett és részletesen kidolgozott történetet – pretextet – használjon az áldozat megtévesztésére. A támadó részletes előkészületeket tesz, beleértve az áldozat munkahelyi vagy személyes környezetének, érdeklődési köreinek és kapcsolatrendszerének tanulmányozását, hogy minden elem hitelesnek tűnjön, így meggyőző szerepjátékot tudjon folytatni. Ennek során a támadó akár egy hivatalos szereplő – akár egy IT-támogató vagy egy pénzügyi tanácsadó – bőrébe bújik, akinek látszólag jogosult hozzáférése van az áldozat bizalmas információihoz.

A „pretexting” különösen veszélyes, mert az áldozatok gyakran hajlamosak megbízni olyan személyekben, akikről feltételezik, hogy hivatalos pozícióban vagy megbízható intézmény képviseletében állnak. Az ilyen támadások gyakran hosszú távú meggyőzési stratégián alapulnak: a támadó fokozatosan építi fel az áldozat bizalmát, hogy az végül önként adjon át érzékeny adatokat. [9]

Mouton, Leenen és Venter social engineering támadási keretrendszere szerint a „pretexting” az egyik legnehezebben felismerhető social engineering módszer. Ennek oka, hogy a támadók komplex, többfázisú stratégiákat használnak, amelyek során az áldozat érzelmi biztonságérzetére és segítőkészségére építenek. A támadó gyakran személyre szabott történetekkel, részletes szerepjátékokkal erősíti a hitelesség látszatát, így még a jól képzett felhasználók számára is nehéz felismerni a megtévesztést.[7]



2. ábra - A "pretexting" támadás lépései (saját ábra)

A „pretexting” egy komplex social engineering módszer, amelynek során a támadó részletesen kidolgozott történetet vagy szerepet használ annak érdekében, hogy bizalmat építsen ki és megtévessze az áldozatot. A „pretexting” támadás sikeressége gyakran a támadó előkészületein és az áldozat bizalmának fokozatos megszerzésén alapul. Az alábbiakban bemutatjuk a „pretexting” támadás fő lépéseit, amelyet a 2. ábra szemléltet. [8]

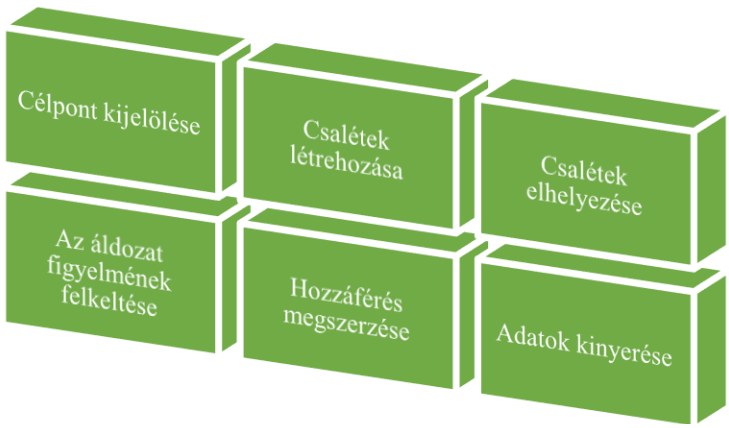
- Az első lépésben a kiberbűnöző alapos kutatást végez az áldozatról. Célja, hogy minél több személyes vagy szakmai adatot gyűjtsön össze, amelyek később felhasználhatók a megtévesztés során. Ezek az információk lehetnek az áldozat munkahelyi szerepkörei, kapcsolati hálója, online jelenléte vagy akár a közösségi médián megosztott személyes információk. A támadó ezek alapján megérti, milyen adatok és kapcsolatok révén közelíthet az áldozathoz hitelesen. [8]
- Az információgyűjtést követően a támadó kiválasztja a megfelelő megszemélyesítést, vagyis eldönti, hogy milyen szerepet fog betölteni az áldozattal való kommunikáció során. A támadó gyakran egy megbízhatónak tekintett személy vagy pozíció szerepébe helyezkedik, például egy banki alkalmazott, egy munkahelyi felettes vagy egy közeli ismerős szerepét ölti magára. A megfelelő személy vagy szerep kiválasztása alapvető fontosságú, mivel ez biztosítja a támadás hitelességét az áldozat szemében. [8]
- Miután kiválasztotta a megszemélyesítést, a kiberbűnöző részletes, hitelesnek tűnő történetet dolgoz ki. Ez a narratíva gyakran valósághű eseményekre vagy helyzetekre épül, amelyekkel az áldozat valószínűleg találkozott már, vagy amelyek kapcsolódnak az áldozat környezetéhez. A megtévesztő történet célja, hogy felkeltse az áldozat bizalmát és elhitesse vele, hogy a támadó valóban az, akinek mondja

magát. Ez a történet lehet sürgető vagy bizalmas jellegű, hogy az áldozat úgy érezze, gyorsan kell cselekednie. [8]

- A támadó ezután kapcsolatba lép az áldozattal a kiválasztott szerep és megtévesztő történet felhasználásával. A kapcsolatfelvétel történhet e-mailben, telefonhíváson, közösségi média üzeneten vagy más kommunikációs csatornán keresztül. Ebben a lépésben a támadó célja, hogy az áldozat figyelmét felkeltse, és bizalmi kapcsolatot alakítson ki vele, így megteremtve a sikeres támadás alapját. A támadó gyakran kifinomult szerepjátékot alkalmaz, amely révén képes elérni, hogy az áldozat ne érezze gyanúsnak a megkeresést. **[**8]
- A támadás végső célja, hogy a támadó megszerezze az áldozattól a kívánt információt vagy anyagi javakat. Ezt a támadó a hitelesen előadott történeten és a kialakult bizalmi kapcsolaton keresztül éri el. Gyakori cél lehet pénz átutalása, bizalmas adatok, jelszavak, azonosítók vagy egyéb érzékeny információk megszerzése. A támadó a bizalomra és hitelességre alapozva manipulálja az áldozatot, hogy saját döntéséből, önként adja ki a kért információkat vagy kövesse a támadó utasításait. [8]

„Baiting”

A „baiting” során a támadók valamilyen csábító ajánlatot vagy ígéretet használnak arra, hogy az áldozatokat káros cselekvésre késztessék (lásd: 3 ábra): fertőzött fájl letöltésére vagy kártékony weboldalak felkeresésére. [2] Gyakori eset az ingyenes zene- vagy filmletöltés, amely mögött kártékony szoftverek rejtőznek. A támadók előnyükre fordítják az áldozatok kíváncsiságát és érdeklődését, így gyakran elegendő egy vonzó, de megtévesztő üzenetet közvetíteniük ahhoz, hogy elérjék céljukat. Karen, Ryan, Shay, Daphana tanulmánya szerint a „baiting” hatékonysága nagymértékben azon múlik, hogy mennyire igazodik a célcsoport érdeklődési köreihez. A támadás sikeresnek ítélhető, ha a csaléteknek használt ajánlat vonzó és releváns a célzott felhasználók számára, ezáltal növelve annak esélyét, hogy az áldozatok figyelmen kívül hagyják az esetleges biztonsági kockázatokat. [9]



3. ábra - A "baiting" támadás lépései (saját ábra)

A „baiting” az egyik leggyakrabban használt szociális manipulációs technika a kiberbiztonság területén, amely egy vonzó ajánlat vagy fájl segítségével próbálja rávenni az

áldozatot arra, hogy önkéntesen biztosítson hozzáférést a támadónak. Az alábbiakban bemutatjuk a baiting technika működését lépésről lépésre, amelyet a 3. ábra szemléltet:

- A támadó kiválaszt egy megfelelő célpontot – lehet ez egy vállalat vagy egy egyén –, aki valószínűleg érdeklődést mutat a csali iránt.
- A támadó vonzó csalit hoz létre, egy érdekesnek tűnő digitális fájlt (program, zene, dokumentum) vagy egy elhagyott USB meghajtót akár.
- A csalit elhelyezhetik digitális térben, így e-mailekben vagy közösségi média linkek formájában, vagy fizikai térben, tehát egy munkahely közelében elhagyott USB meghajtón.
- A csali célja az áldozat kíváncsiságának felkeltése. Az áldozat gyakran azt hiszi, hogy a csali valamilyen előnnyel jár, példának kedvéért: hasznos információkat vagy ingyenes hozzáférést biztosít.
- Amikor az áldozat rákattint egy linkre vagy megnyitja a csalival ellátott fájlt, a támadó hozzáférést szerez az áldozat eszközéhez vagy hálózatához, malware vagy adatgyűjtő szoftver révén.
- A támadó a megszerzett hozzáférés révén érzékeny adatokat szerezhet meg, amelyeket felhasználhat vagy akár zsarolásra is alkalmazhat.

VÉDEKEZÉSI STRATÉGIÁK A SOCIAL ENGINEERING ELLEN

Oktatás és tudatosság

Az egyik leghatékonyabb védekezési stratégia a social engineering támadásokkal szemben a felhasználók folyamatos oktatása és tudatosságnövelése. A social engineering támadások sikeressége gyakran a felhasználók tájékozatlanságán múlik, ezért fontos, hogy rendszeres képzésekkel, szemináriumokkal és szimulációkkal fejlesszék a dolgozók éberségét és felkészültségét. [1] A szimulációk lehetőséget adnak arra, hogy a felhasználók biztonságos környezetben tanulják meg felismerni a gyanús e-maileket, linkeket vagy telefonhívásokat, és hogy azonnal felismerjék a manipulációs kísérleteket, így tehát a „phishing" vagy a „pretexting" technikákat. Karen, Ryan, Shay, Daphana tanulmánya szerint a rendszeres oktatás és a folyamatos tudatosságnövelés nemcsak a támadások észlelésében, hanem a felhasználók gyors és megfelelő reagálásában is jelentős javulást eredményez. Az oktatási programok során a felhasználók nagyobb elkötelezettséget mutatnak a kibervédelmi protokollok betartása iránt, ezáltal csökkentve a szervezet sebezhetőségét. [9]

Technikai megoldások

A technológiai eszközök használata szintén fontos szerepet játszik a social engineering támadások elleni védekezésben. A kétfaktoros hitelesítés (2FA) jelentősen csökkentheti a támadások sikerességét azáltal, hogy további védelmi réteget biztosít, melyet a támadóknak le kell küzdeniük. [10] Emellett a fejlett spamszűrők és a biztonsági szoftverek használata fontos az adathalász e-mailek kiszűrésére, valamint a hálózati fenyegetések automatikus észlelésére. A rendszeres szoftverfrissítések és biztonsági javítások kulcsfontosságúak, mivel számos social engineering támadás a sebezhetőségeken alapul. Tushaar, Jaidhar & Bhabesh tanulmánya szerint a gépi tanulással támogatott korszerű spamszűrők jelentős fejlődést képviselnek a célzott támadások, ezáltal a „phishing" e-mailek kiszűrésé-

ben. Ezek a rendszerek képesek hatékonyan azonosítani az e-mailekben rejlő gyanús mintákat és anomáliákat, ezáltal fokozva a támadásokkal szembeni védekezés hatékonyságát. [11]

Szervezeti intézkedések

A vállalati biztonság erősítése érdekében a szervezeteknek szigorú biztonsági protokollokat kell bevezetniük. Az információkhoz való hozzáférés szigorú szabályozása, a minimális hozzáférés elvével (principle of least privilege), csökkenti a social engineering kockázatát azáltal, hogy csak a szükséges információkat és rendszereket teszi elérhetővé az alkalmazottak számára. [7] Emellett a gyanús tevékenységek azonnali jelentésének ösztönzése – egy egyszerűen használható bejelentési rendszer révén – gyorsabb reagálást tesz lehetővé. A belső auditok, biztonsági tesztek és sérülékenységvizsgálatok szintén segíthetnek a lehetséges sebezhetőségek feltárásában és orvoslásában, mielőtt azok valódi támadások célpontjává válnának. [12] A rendszeres belső ellenőrzés és a biztonsági incidensek kivizsgálása tovább növeli a szervezet ellenálló képességét.

JÖVŐBELI KILÁTÁSOK ÉS A SOCIAL ENGINEERING VÁRHATÓ FEJLŐDÉSE

A social engineering támadások egyre kifinomultabbá és célzottabbá válnak, mivel a támadók gyorsan alkalmazkodnak a technológiai újításokhoz, kihasználva a mesterséges intelligencia (továbbiakban: AI), a gépi tanulás (továbbiakban: ML) és az adatelemzés által kínált lehetőségeket. Ezek a technológiák lehetővé teszik a támadók számára, hogy sokkal pontosabb és személyre szabottabb támadásokat hajtsanak végre, miközben minimalizálják a felfedezés kockázatát. Az elkövetkező években ezek a technikák még összetettebbé és nehezebben felismerhetővé válhatnak, különösen az alábbi területeken.

AI és ML alapú célzott támadások

Az AI és a gépi tanulás ML lehetőséget biztosítanak a támadók számára, hogy nagy mennyiségű adatot gyorsan feldolgozzanak és rendszerezzenek, ezzel jelentősen növelve a célzott támadások hatékonyságát. Az AI segítségével a támadók képesek automatikusan feltérképezni a célpontok közösségi média profiljait és egyéb nyilvános adatforrásokat, hogy személyre szabott támadási stratégiákat dolgozzanak ki. Az ML-algoritmusok folyamatos tanulási képessége révén optimalizálják a támadások sikerességét, például olyan adathalász üzenetek generálásával, amelyek pontosabban célozzák az áldozatok gyenge pontjait, növelve a bizalmas információk kiszivárogtatásának valószínűségét. [13]

„Deepfake” technológia és hamisított tartalom

A „deepfake” technológia, amely AI-alapú képi és hangmanipulációt használ, különösen veszélyes lehet a social engineering területén. A támadók a „deepfake” eszközöket arra használhatják, hogy meggyőző hamis videókat és hangfelvételeket hozzanak létre, például egy vállalat vezetőjének „hangján” adjanak utasítást egy pénzügyi tranzakció végrehajtására. Mivel ez a technológia egyre fejlettebbé válik, a hamis tartalmak egyre hitelesebbek lesznek, és így nehezebb lesz felismerni az ilyen jellegű csalásokat. [14]

Széles körű adatelemzés és célzott social engineering kampányok

A „big data” és az adatelemzés eszközeinek fejlődése lehetőséget nyújt a támadóknak arra, hogy részletes profilt alkossanak az áldozatokról. Az adatelemzés lehetővé teszi, hogy a támadók még inkább személyre szabott módszerekkel célozzák meg az egyéneket és a szervezeteket. A célzott kampányok során egyéni érdeklődési körökre és viselkedési mintákra szabott csalogató üzeneteket készítenek, amelyek sokkal nagyobb eséllyel vezetik félre az áldozatot. [7]

Automatizált social engineering rendszerek

Az automatizálás terén elért eredmények szintén jelentős hatással lehetnek a social engineering fejlődésére. Az automatizált rendszerek segítségével a támadók nagyobb mennyiségű támadást képesek végrehajtani kevesebb idő és erőforrás felhasználásával. Az automatizált chatbotok generálhatnak olyan üzeneteket, amelyek utánzási algoritmusokat használnak az emberi beszélgetéshez, így megtévesztve az áldozatokat. Az ilyen rendszerek különösen veszélyesek a vállalati ügyfélszolgálatok számára, mivel az automatizált chatbotok könnyen beépíthetők az adathalász támadásokba, növelve azok hatékonyságát és csökkentve a detektálhatóság esélyeit. A támadók olyan gépi tanulási algoritmusokat is beépíthetnek, amelyek folyamatosan optimalizálják az interakciókat a sikeres manipuláció érdekében. [15]

IoT és social engineering

Az „Internet of Things” (továbbiakban: IoT) eszközök térhódítása újabb támadási felületeket biztosít a social engineering számára. Az IoT-eszközök gyakran kevésbé biztonságosak, és nem minden esetben frissíthetők megfelelően, így a támadók könnyebben hozzáférhetnek az ilyen eszközökön keresztül tárolt vagy továbbított információkhoz. A támadók kihasználhatják ezeket a gyenge pontokat, hogy manipulálják a felhasználókat, hamis biztonsági figyelmeztetések küldésével, amelyek arra ösztönzik az áldozatokat, hogy bizonyos adatokhoz vagy rendszerekhez biztosítsanak hozzáférést. Az IoT-eszközöket így a támadók a social engineering új eszközeiként használhatják. [16]

ÖSSZEGZÉS

A social engineering egy összetett és folyamatosan fejlődő fenyegetés, amely az emberi pszichológiai tényezők kihasználásával manipulálja az áldozatokat, és az adatbiztonság egyik legsúlyosabb kihívását jelenti. A tanulmány áttekintést nyújtott a social engineering történeti fejlődéséről, bemutatva a korai technikákat, valamint a modern támadási formák kialakulását, amelyek közé tartozik a „phishing”, a „pretexting” és a „deepfake” manipuláció. A technológiai fejlődés – különösen az AI és ML alapú módszerek elterjedése – lehetővé teszi, hogy a támadások még célzottabbá és nehezebben felismerhetővé váljanak, ami tovább növeli a social engineering veszélyeit.

A védekezési stratégiák bemutatásával a tanulmány hangsúlyozza az oktatás, a technikai eszközök és a szigorú szervezeti protokollok fontosságát a social engineering elleni harcban. A jövőben elengedhetetlen lesz a védekezési mechanizmusok folyamatos fejlesztése és a felhasználók rendszeres oktatása annak érdekében, hogy lépést tarthassanak a social engineering támadások gyors ütemű fejlődésével.

FELHASZNÁLT IRODALOM

[1] [1] C. Hadnagy, Social Engineering: The Science of Human Hacking, 2nd ed. Hoboken, NJ, USA: Wiley, 2018. ISBN: 978-1-119-43338-5.

[2] K. D. Mitnick és W. L. Simon, The Art of Deception: Controlling the Human Element of Security. Indianapolis, IN, USA: Wiley, 2002. ISBN: 978-0-471-23712-9.

[3] R. B. Cialdini, Influence: The Psychology of Persuasion, Revised ed. New York, NY, USA: HarperCollins, 2009. ISBN: 978-0-06-189987-4.

[4] D. Gragg, "A Multi-Level Defense Against Social Engineering," SANS Institute, 2003. [Online]. Elérhető: https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-1232. [Hozzáférés dátuma: 2024. november 15.].

[5] P. Bányász, "Közösségi média és social engineering," Nemzetbiztonsági Szemle, vol. 5, no. 1, pp. 59–77, 2017. ISSN: 2064-3756.

[6] K. Krombholz, H. Hobel, M. Huber és E. Weippl, "Advanced social engineering attacks," Journal of Information Security and Applications, vol. 22, pp. 113–122, 2015. doi: 10.1016/j.jisa.2014.09.005.

[7] F. Mouton, M. Malan, L. Leenen és H. S. Venter, "Social Engineering Attack Framework," in Proceedings of the Information Security for South Africa Conference, Johannesburg, South Africa, 2014, pp. 1–9. doi: 10.1109/ISSA.2014.6950510.

[8] A. Trevino, "What Is a Pretexting Attack?", Keeper Security Blog, 2023. [Online]. Elérhető: https://www.keepersecurity.com/blog/2023/06/02/what-is-a-pretexting-attack/. [Hozzáférés dátuma: 2024. november 15.].

[9] M. J. Guitton, "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies," Journal of Cybersecurity, vol. 7, no. 1, tyab019, 2021. doi: 10.1093/cybsec/tyab019.

[10] P. A. Grassi, M. E. Garcia és J. L. Fenton, "Digital Identity Guidelines," NIST Special Publication 800-63-3, 2017. [Online]. Elérhető: https://doi.org/10.6028/NIST.SP.800-63-3. [Hozzáférés dátuma: 2024. november 15.].

[11] T. Gangavarapu, C. D. Jaidhar és B. Chanduka, "Applicability of machine learning in spam and phishing email filtering: review and approaches," Artificial Intelligence Review, vol. 53, no. 7, pp. 5019–5081, 2020. doi: 10.1007/s10462-020-09814-9.

[12] Deloitte Insights, "The value of cyber investments," 2020. [Online]. Elérhető: https://www2.deloitte.com/content/dam/insights/us/articles/5002_Value-of-cyber-investments/DI_Value-of-cyber-investments.pdf. [Hozzáférés dátuma: 2024. november 15.].

[13] M. Malatji és A. Tolah, "Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI," AI and Ethics, 2024. doi: 10.1007/s43681-024-00427-4.

[14] D. K. Citron és R. Chesney, "Deepfakes and the New Disinformation War," Foreign Affairs, vol. 98, no. 1, pp. 147–155, 2019. [Online]. Elérhető: https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war. [Hozzáférés dátuma: 2024. november 15.].

[15] World Economic Forum, "AI could empower and proliferate social engineering cyberattacks," 2024. [Online]. Elérhető: https://www.weforum.org/agenda/2024/10/ai-

agents-in-cybersecurity-the-augmented-risks-we-all-need-to-know-about/. [Hozzáférés dátuma: 2024. november 15.].
[16] N. Zlatanov, "Computer Security and Mobile Security Challenges," 2015. [Online]. Elérhető: https://www.researchgate.net/publication/283349998_Computer_Security_and_Mobile_Security_Challenges. [Hozzáférés dátuma: 2024. november 15.].

THE SUPER-APPLICATIONS INNOVATION: THE FULL DIGITAL CUSTOMER EXPERIENCE

A SZUPERALKALMAZÁSOK INNOVÁCIÓJA: A TELJESKÖRŰ DIGITÁLIS ÜGYFÉLÉLMÉNY

BALOGH Attila[1] – VARGA János[2]

Abstract

The following paper focuses on the so-called SuperApps. The concept of a SuperApp and a TOP10 visual ranking of apps are presented. The research aims to collect and define the basic characteristics that define a super-application as a solution. In order to achieve the above objectives, the present study uses a bibliometric mapping approach to process scientific articles available in Scopus and Web of Science databases. The conducted research identifies a significant gap in the scientific research opportunities in Scopus- and Web of Science-indexed do-cuments. Based on the experience gained from Scopus and Web of Science, a six-item list of the most relevant articles on the subject has been compiled by processing and analysing the most relevant articles in Google Scholar, which summarises the most important features of the super-applications. Finally, these essential features are briefly analysed and presented, providing a comprehensive picture of their importance and functionality in the super-application system.

Keywords

superapp, super-app, innovation, mobile app, digital customer experience

Absztrakt

Az alábbi tanulmány az ún. SuperApp-okra, azaz magyarul szuperalkalmazásokra összpontosít. Bemutatásra kerül a szuperalkalmazás fogalma és egy TOP10-es aktuális rangsor. A kutatás célja, hogy összegyűjtse és meghatározza azokat az alapvető jellemzőket, amelyek a szuperalkalmazást, mint megoldást definiálják. A fenti célok elérése érdekében jelen tanulmány bibliometriai feltérképezés módszertanát alkalmazva a Scopus és a Web of Science adatbázisban elérhető tudományos cikkeket dolgozza fel. Az elvégzett kutatás jelentős hiánypótló jellegű tudományos kutatási lehetőséget azonosít a Scopus- és Web of Science-indexált dokumentumokban. A Scopus és a Web of Science segítségével szerzett tapasztalatok alapján, a Google Scholar a témában leginkább releváns cikkeinek feldolgozásával és elemzésének eredményeképpen egy olyan hat elemből álló lista került összeállításra, amely a szuperalkalmazások legfontosabb jellemzőit foglalja magába. Végül ezek az alapvető jellemzők röviden elemzésre és bemutatásra kerülnek, átfogó képet nyújtva jelentőségükről és funkcionalitásukról a szuperalkalmazások rendszerében.

Kulcsszavak

superapp, szuperalkalmazás, innováció, mobilalkalmazás, digitális ügyfélélmény

[1] balogh.attila@kgk.uni-obuda.hu | ORCID: 0009-0001-1078-6874 | PhD student, Innovation Management Doctoral School of the Óbuda University | doktorandusz hallgató, Innováció Menedzsment Doktori Iskola

[2] varga.janos@kgk.uni-obuda.hu | ORCID: 0000-0002-1891-7269 | associate professor, Óbuda University Keleti Károly Faculty of Business and Management | egyetemi docens, Óbudai Egyetem, Keleti Károly Gazdasági Kar

BEVEZETÉS

A mobilalkalmazások használata világszerte elképesztő szintet ért el. A mobileszközökön elérhető alkalmazásoknak is köszönhető, egyre többféle funkcióra - például telekonferencia, navigáció, vagy éppen online fizetés - tudjuk használni telefonjainkat. Az alkalmazások elterjedése, amelyet az egyre megfizethetőbb áru okostelefonok és adatszolgáltatási csomagok, illetve a növekvő lefedettségű és kapacitású mobilhálózat tesz lehetővé, alapvetően három hajtóerő és egy eredő tényező kedvező egybeeséséből ered: a) a telefonok és adatszolgáltatási csomagok csökkenő ára, amelyhez növekvő lefedettség társul, b) a mobilalkalmazások fejlesztésének csökkenő költsége, és c) számos személyes és vállalati funkció mobiltelefonokra történő átterjedése. 2023-ban világszerte 8,93 millió mobilalkalmazás volt, amelyeket összesen 255 milliárd alkalommal töltöttek le [1]. Ha figyelembe vesszük, hogy világszerte 7,21 milliárd okostelefont tartunk számon, amelyeket 4,88 milliárd felhasználó tulajdonol, ez azt jelenti, hogy egy felhasználó átlagosan 32 alkalommal tölti le ugyanazt az alkalmazást az valamelyik telefonjára. Egy tipikus felhasználó 40 alkalmazást birtokol az okostelefonján, napi szinten 9-10-et, havonta pedig 30-at használ [2]. Az előrejelzések szerint 2025-re a mobilalkalmazások 613 milliárd amerikai dollár bevételt fognak generálni, ami nagyjából az IMF által Argentínára (604,26 milliárd USD) és Írországra (564,2 milliárd USD) 2024-re prognosztizált teljes GDP-értékek köré helyezi ezt a piacot [3].

A mobilalkalmazások kiterjedt használata és széles körű alkalmazhatósága miatt alapvető kérdésként merül fel, hogy akár az ügyfelek, akár a szolgáltatók milyen módszerekkel egyszerűsíthetik tovább és tehetik még ügyfélbaráttabbá a mobilok segítségével elvégezhető jelenlegi és jövőbeli tevékenységeiket. Ezt a kérdést a „SuperApp", azaz szuperalkalmazás fogalmának megalkotásával igyekeztünk megválaszolni. A „SuperApp" kifejezés, ahogyan azt Roa et al. [4] 2021-ben leírta, „olyan mobilalkalmazásokra utal, amelyek ugyanabban a környezetben a fogyasztók különböző napi igényeit igyekeznek kielégíteni anélkül, hogy egy másik alkalmazás letöltését igényelnék".

Mivel a szuperalkalmazásokkal kapcsolatos tudományos anyagok számossága még mindig viszonylag korlátozott, ez a tanulmány nyilvánosan hozzáférhető forrásokat is felhasznál a fő kutatási témákra vonatkozó adatok összeállításához. A szuperalkalmazásokra vonatkozó elérhető találatok száma a „superapp*" vagy „super-app*" keresőszavak használatával a következők (2024. április 28-án):

Forrás / keresőszó	superapp*	super-app*
Google Scholar	4 360	3 680
Scopus	37	110
Web of Science	42	159

1. táblázat: SuperApp szóra történő keresőtalálatok
Forrás: szerzők saját szerkesztése Google Scholar, Scopus és WoS keresések alapján

A szuperalkalmazásokról szóló akadémiai szakirodalom szűkössége arra utal, hogy ez a terület még nagyrészt feltérképezetlen, ami széleskörű lehetőségeket kínál a további feltáró munkák és tudományos kutatások számára. A meglévő tanulmányok viszonylag

korlátozott száma kiemeli, hogy további kutatásokra van szükség a SuperApp-ok összetettségének és további lehetőségeinek átfogó megértéséhez, akár a különböző vizsgált területek összefüggéseiben is. Ez a tudományos ismeretekben mutatkozó hiányosság a kutatók számára kiváló lehetőséget jelent új megállapítások megtételére, összefüggések feltárására, a tendenciák elemzésére és az elméleti keretek továbbfejlesztésére. Napjaink gyorsan változó világa megköveteli és megköveteli ezeket a projektalapú kezdeményezéseket [5][6], amelyekben megvan az innovációs és jövőformáló potenciál. Ezek a feladatok és fejlesztési lehetőségek mind egyéni, mind vállalati szinten kiemelkedő jelentőségűek [7][8][9][10][11].

Ezt a tanulmány három fő célt tűzött ki maga elé. A digitalizáció gyorsan változó területén belül a munka rövid történeti áttekintést nyújt, amely a legújabb tudományos szakirodalom átfogó strukturált elemzéséből származik. Ezen elemzés célja, hogy bemutassa a „szuperalkalmazások" néven ismert mobilalkalmazások jelenlegi piaci helyzetét, feltárva azok használati szokásait, a jellemző fogyasztói igényeket, és azt, hogy ezeket az igényeket hogyan elégítik ki. A bibliometriai elemzést elsődleges kutatási módszerként használva a cél az, hogy általánosságban is definiálni és tanulmányozni lehessen a szuperalkalmazások fő jellemzőt és meghatározó tulajdonságait. Emellett megvizsgálja a felhasználók előtt álló kihívásokat, és felvázolja a szuperalkalmazások fejlesztésének lehetséges jövőbeli irányait, figyelembe véve a folyamatban lévő piaci és technológiai változásokat. A kutatás alapvető célja, hogy bővebb információt adjon a szuperalkalmazások megértéséhez, és hozzájáruljon a digitális innovációról és a felhasználók mobiltechnológiai színtéren történő bevonásáról szóló szélesebb körű vitához.

SZUPERALKALMAZÁSOK VILÁGVISZONYLATBAN

Az világ első szuperalkalmazásnak a WeChat-et tekinthető [12]. Az április 27-én végzett Google Scholar keresés alapján a „wechat" kulcsszóra 3 080 000 találat érkezett, ami még a legnépszerűbb közösségi médiaalkalmazásokkal, vagy néhány konkrét egyéb elterjedt mobilalkalmazással összehasonlítva is meglehetősen magas szám.

A szerző saját keresése alapján a 2. táblázat a Google Scholar 2024. április 27-én kiadott találatait mutatja:

Keresőszó	Google Scholar találatok száma
facebook	7 530 000
instagram	4 830 000
wechat	3 080 000
revolut	35 200
waze	23 900
alipay	22 200

2. táblázat: Mobilalkalmazások keresőtalálatainak száma
Forrás: szerzők saját szerkesztése, a Google Scholar keresések alapján

A legfrissebb információk alapján a WeChat egyike annak az öt alkalmazásnak világszerte, amelynek több mint egymilliárd aktív felhasználója van [13]. A különböző szuperalkalmazások rangsorolásához számos különböző ismérvet lehetne használni. Ahhoz, hogy egységes nézetből lehessen vizsgálni a területet és megfelelő betekintést nyerjünk a témakörbe és a különböző jellemzőibe, szükség van egy választott szempont alapján történő rangsorra.

A pénzügyi teljesítménymutatók vizsgálata és értékelése - különösen azon szuperalkalmazások esetében, ahol FinTech szolgáltatások és pénzügyi ügynöki tevékenységek is jelen vannak -, a pontos számadatok beszerzése és ellenőrzése komoly feladatot jelent. Különböző források például arról számolnak be, hogy a WeChat 2023-ban körülbelül 16,38 milliárd amerikai dollár éves bevételt termelt. Ezzel szemben az Alibaba leányvállalata, az AliPay a jelentések szerint 2022-ben körülbelül 280 milliárd dollár tranzakciós bevételt bonyolított le. Ez a szám jelentősen meghaladja a WeChat-ét. Mivel azonban ez a feldolgozott tranzakciók összértékét jelenti, és nem az AliPay közvetlen bevételét, a vállalat számára hozzáadott érték pontos mérték, azaz a valódi és összehasonlítható saját bevétele továbbra is ellenőrizhetetlen adat.

Szuperalkalmazás neve	**Aktív felhasználók száma (millió)**	**Felhasználói számadat dátuma és forrása**
WeChat	1 330	2023, [13]
Alipay	1 300	2023, [14]
PhonePe	350	2023, [19]
Uber	150	2023, [17]
Tata Neu	120	2022, [20]
Paytm	58-90	2023, [18], [19]
Gojek	38	2024, [21]
Grab	35	2023, [22]
Rappi	30	2022, [15]
Revolut	30	2023, [16]

3. táblázat: TOP10 szuperalkalmazás az aktív felhasználók száma alapján
Forrás: szerzők saját szerkesztése a fenti megjelölt források alapján

Ezen tanulmány készítése során összegyűjtött és közreadott alábbi szuperalkalmazás TOP listában a rangsor az adott alkalmazás aktív felhasználóinak száma szerint alakult ki. Lényeges megjegyezni, hogy az aktív felhasználókra vonatkozó adatok eredete sokféle lehet: vállalati adatbázisok, tudományos szakirodalom, valamint különböző statisztikai vagy szakmai weboldalak nyújtanak információt a témakörben. Amint azt az alábbi példák is szemléltetik, megállapítható, hogy ezek a számadatok még a tudományos források között is jelentősen eltérhetnek. Több helyen megjelent információk szerint a

PhonePe körülbelül 350 millió aktív felhasználóval rendelkezik; a vállalat azonban hivatalosan nem tette közzé ezeket az adatokat. Ezzel szemben egy 2023-as akadémiai tanulmány mindössze 165 millió aktív felhasználóról számol be. Sőt, maguk a tudományos források között is megfigyelhetők eltérések. Neethu (2023) például csak 58 millió aktív felhasználót dokumentál a PayTM kapcsán [18], míg egy másik tudományos munka Das-t (2023) idézi, aki ugyanabban az évben már 90 millió aktív felhasználóról számol be [19]. A rendelkezésre álló adatok alapján elmondható, hogy 2024 áprilisától (lásd a 3. táblázatban szereplő információk dátumát) egy szuperalkalmazásnak legalább 30 millió aktivált felhasználóra van szükség ahhoz, hogy a világ szuperalkalmazásait tartalmazó SuperApps TOP10-be bekerüljön.

Számos tanulmány foglalkozott és foglalkozik a szuperalkalmazások megjelenésével, amint azt az 1. táblázat is mutatja, amelyből kiderül, hogy a WeChat, az úttörő és jelenleg a legnagyobb felhasználói bázist tekintve a legnagyobb szakirodalommal rendelkezik. Jelen kutatás célkitűzései miatt és terjedelmi okokból ez a tanulmány nem vizsgálja a szuperalkalmazások kialakulásának okait, sem azt az innovatív fejlődési utat, amelyen keresztül a meglévő mobilalkalmazások szuperalkalmazásokká váltak, vagy eredetileg azzal a szándékkal indultak, hogy szuperalkalmazásként jelenjenek meg a piacon.

A kutatás céljait szem előtt tartva, a munka a jelenlegi szuperalkalmazások kapcsán elérhető tudományos szakirodalmat veszi alapul, ezekre támaszkodva vizsgálja meg azokat a tulajdonságokat és jellemzőket, amelyekkel ezek a milliós nagyságrendű ügyfélbázist napi szinten kiszolgáló komplex ügyfélélményt biztosító mobilalkalmazások rendelkeznek.

MÓDSZERTAN

A Scopus és a Web of Science tudományos adatbázisok felhasználásával a szuperalkalmazásokhoz kapcsolódó kulcsszavas keresésekhez a Scopus-ban a következő keresések történtek:

- TITLE-ABS-KEY (superapp*) és
- TITLE-ABS-KEY (super-app*)

A „superapp*” keresés 37 dokumentumot, míg a „super-app*” keresés 110 dokumentumot adott vissza. Bár a terminológia használatának ellenőrzése nem volt e kutatás elsődleges célja, a Scopus-keresések eredményei azt mutatják, hogy a „super-app” kifejezés sokkal elterjedtebb, mint a “superapp” kifejezés, legalábbis az tudományos szakirodalomban.

Az adatfeldolgozás módszertana az alábbiakban vázolt szigorú protokollt követte:

1. Átfogó keresés történt a Scopus és a Web of Science (WoS) adatbázisok segítségével, majd az összes dokumentumról export készült.ris és .csv formátumban.
2. A VOSviewer szoftver segítségével hálózati vizualizációs térképek készültek, a térképek alapjául a szöveges fájlokban szereplő exportált adatok szolgáltak. Ennek adatforrásai a Scopusból és a WoS-ból származó fájlok voltak az 1. pontban leírtak szerint.
3. A kulcsszavas absztrakcióhoz a dokumentumok címeit és kivonatát használtuk fel, a strukturált absztrakt címkék és a szerzői jogi nyilatkozatok kivételével.
4. A szoftveren belüli alkalmazott számlálási módszertan a Full Counting volt.

5. Egy adott kifejezés minimális előfordulási küszöbértéke kezdetben 10-ben lett meghatározva, majd ezt később 5-re lett módosítva.
6. A megjelenítendő kifejezések kiválasztása a relevancia pontszám alapján történt, amelyet kezdetben az alapértékként szereplő 60%-on volt, később ez manuálisan átállításra került.

Tekintettel arra, hogy az 5. és 6. pont vonatkozásában a VOSViewer által alapértelmezettként megadott értékek nem biztosítottak megfelelő mennyiségű vizsgálható kulcsszó eredményt, így ezeket a beállítások manuálisan átállításra kerültek. Ennek megfelelően a találati mennyiségekről és további beállításokról, illetve a VOSViewer kulcsszavas kifejezések kapcsán használt relevanciapontszám módosítása kapcsán a részletek az alábbiakban közreadott 5. táblázat és 6. táblázatban találhatóak:

SCOPUS	**super-app* keresés dokumentumaiban**	**superapp* keresés dokumentumaiban**
Megtalált kifejezések száma	3011	406
Kulcsszó kifejezések száma n = 10 gyakoriság vagy a felett	37	7
Kulcsszó kifejezések száma n = 5 gyakoriság vagy a felett	136	7
Kulcsszó kifejezések száma relevanciapontszám = 60% esetében	82	4
Manuálisan beállított áttekintendő kulcsszó kifejezések száma	100	7

4. táblázat: VOSViewer szoftver kulcsszó kifejezés hálózati térkép eljárás eredményei, Forrás: szerzők saját szerkesztése Scopus adatbázis találatok és a VOSViewer eredményei alapján

WEB OF SCIENCE	**super-app* keresés dokumentumaiban**	**superapp* keresés dokumentumaiban**
Megtalált kifejezések száma	3531	618
Kulcsszó kifejezések száma n = 10 gyakoriság vagy a felett	40	9

WEB OF SCIENCE	super-app* keresés dokumentumaiban	superapp* keresés dokumentumaiban
Kulcsszó kifejezések száma n = 5 gyakoriság vagy a felett	147	33
Kulcsszó kifejezések száma relevanciapontszám = 60% esetében	88	20
Manuálisan beállított áttekintendő kulcsszó kifejezések száma	100	33

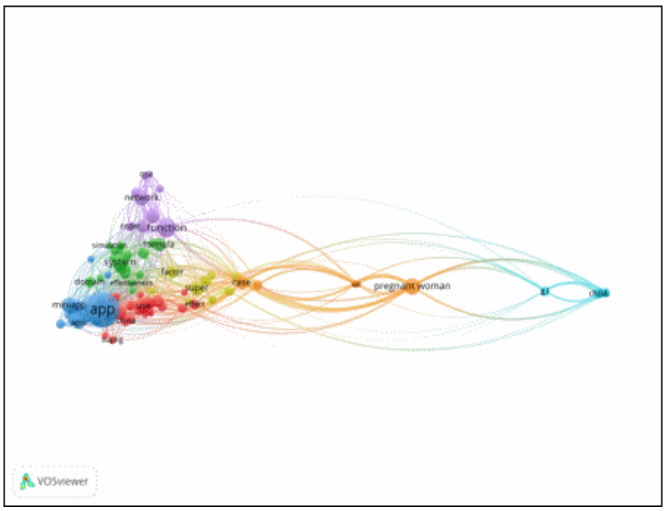
5. táblázat: VOSViewer szoftver kulcsszó kifejezés hálózati térkép eljárás eredményei,
Forrás: szerzők saját szerkesztése WoS adatbázis találatok és a VOSViewer eredményei alapján

Eredmények a "super-app*" keresőszó használata alapján

A Scopus és WoS forrásból származó "szuper-app*" keresőszó alapján előállt eredmények esetében a bibliográfiai keresés és a kulcsszavas keresési módszertan után az összes 2x100 találat manuális áttekintésre és értékelésre került. A listában a következő kulcsszavak kerültek beazonosításra, amelyek csak a Scopus alapú listában szerepelnek, a WoS forrású papíron belül a 100 tételben egyetlen releváns kifejezés sem jelent meg.

Kulcsszó	100-as rangsorban elfoglalt hely	Kulcsszó előfordulás száma a viszgált dokumentumokban	Forrás
Biztonság – "Security"	23.	14	Scopus lista
Digitális tárca – "Digital wallet"	95.	5	Scopus lista
Digitális transzformáció – "Digital transformation"	96.	6	Scopus lista

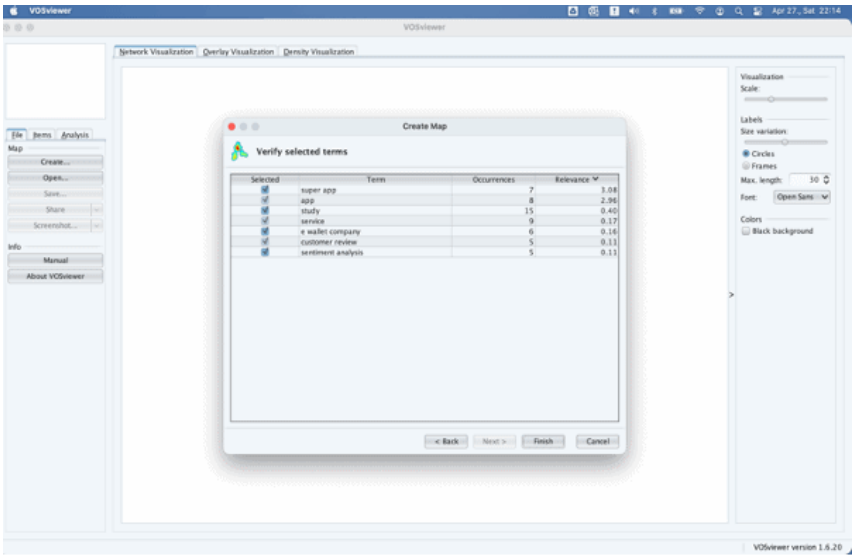
6. táblázat: VOSViewer szoftver által kiadott kulcsszó kifejezés
hálózati térkép eljárás minősített eredményei,
Forrás: szerzők saját szerkesztése Scopus adatbázis találatok és a VOSViewer eredményei alapján



1. ábra: VOSviewer hálózati vizualizációs térkép a "super-app" Scopus keresés dokumentumai alapján, Forrás: VOSviewer hálózati térkép*

Eredmények a "superapp*" keresőszó használata alapján

A „superapp*" keresési eredmények a bibliográfiai keresés és a fejlett kulcsszavas keresési módszertan után összesen 7 találatot mutattak a Scopus alapú dokumentumok és 33 találatot a WoS alapú dokumentumok esetében, amely eredmények szintén manuális áttekintésen és értékelésen estek át. Ezen áttekintés alapján sem a Scopus, sem pedig a WoS találati listában meglévő dokumentumok feldolgozása során a szuperalkalmazásokhoz a kutatáshoz kapcsolódó funkció vonatkozásában egyetlen kulcsszót sem lehetett hozzárendelni.



2. ábra: VOSviewer kulcsszó kifejezés összesítő találati lista a "superapp"*
Scopus keresés dokumentumai alapján,
Forrás: VOSviewer hálózati térkép

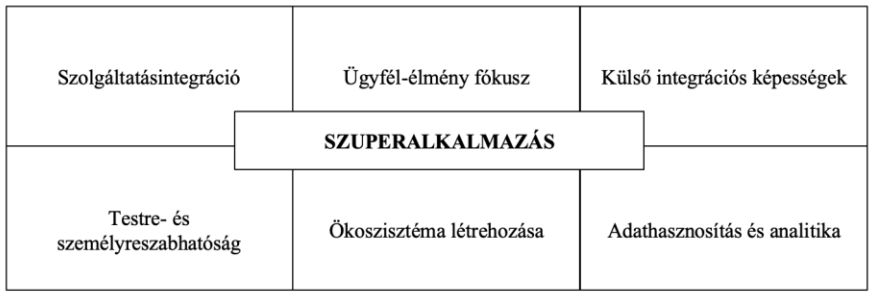
Összefoglaló eredmények a Scopus és a WoS eredmények alapján

A VOSViewer szoftverrel végzett kulcsszó előfordulási elemzés alapján, amely a Scopus és a Web of Science adatbázisokban található cikkek címeit és absztraktjait tekinti át, megállapítható, hogy a bibliográfiai elemzés alapján az áttekintések és a meglévő tanulmányok ezen a tudományterületen még nem érték el azt a szintet, ahol a legfontosabb jellemzőket ilyen módszertannal azonosítani lehetne.

Tekintettel arra, hogy a Scopus-ban és a WoS-ban található cikkek vizsgálata nem járult hozzá a kutatás eredeti céljához, nevezetesen annak megállapításához, hogy melyek a szuperalkalmazások főbb jellemzői, és mitől lesz egy mobilalkalmazás szuperalkalmazás, a tanulmány a Google Scholar hasonló témájú cikkeinek elemzésére helyezte át a hangsúlyt.

MEGÁLLAPÍTÁSOK

A legtekintélyesebb tudományos adatbázisokból származó megállapításokon alapuló fenti elemzés elvégzése után a Google Scholar-ban található, magasan idézett tudományos cikkek átfogó felülvizsgálatára került sor. Ez az átfogó értékelés mintegy 30 cikk részletes elolvasását és jegyzetelését foglalta magában. Ebből az alapos vizsgálatból hat fő jellemzőt sikerült megállapítani, mint olyan alapvető kritériumokat, amelyek egy mobilalkalmazást szuperalkalmazás státuszba emelnek. Ezek a jellemzők további részletesen áttekintésen és azonosításon estek át, annak érdekében, hogy mélyebb megértést nyújtsanak arról, hogy mi különbözteti meg a szuperalkalmazásokat a többi mobilalkalmazástól.



3. ábra: A szuperalkalmazások hat alapvető jellemzője
Forrás: szerzők saját szerkesztése, a későbbiekben megjelölt forrásmunkák feldolgozása alapján

A szuperalkalmazások hat fő jellemzője

1. Szolgáltatásintegráció: A szuperalkalmazás alapvető lényege, hogy egyetlen mobilalkalmazáson keresztül különböző szolgáltatásokat nyújt [23]. Jellemzően valamilyen tranzakciós szolgáltatási tevékenységhez kapcsolódóan különböző egyéb szolgáltatásokat fejlesztenek ki [24]. Ez az eredeti alaptevékenység lehet közösségi médiakommunikáció (mint a WeChat esetében), kereskedelem (mint az AliPay esetében), vagy szállítási szolgáltatás (mint az Uber esetében). Ez

természeténél fogva jelentős hatással van a felhasználói élményre, különösen az egyszeri felhasználói azonosítás, a biztonság, az adattárolás és a kezelhetőség tekintetében [25]. Ha az adott szuperalkalmazás kapcsán nem az alapfunkció részét képzi maga a pénzügyi szolgáltatás, akkor ezeket jellemzően harmadik féltől származó bevont FinTech megoldások segítségével teszik elérhetővé a szuperalkalmazáson belül. A pénzügyi szolgáltatásokhoz kapcsolódó funkciókat alapvetően a legtöbb szuperalkalmazás alaptartalmának egyik alapvető szolgáltatási kínálataként tartják számon [26], [27].

2. Ügyfél-élmény fókusz: A számítógépekkel szemben a mobilalkalmazások egyik legnagyobb előnye a felhasználó szempontjából a gyors, egyszerű használhatóság és az intuitív működés. Ami az ügyfélélmény fokozását illeti, adott szuperalkalmazás általában számos különböző funkciót jelenít meg egy jól definiált keretrendszeren belül, amelyet a felhasználók különösen nagyra értékelnek [28]. Az adott rendszeren belül a felhasználóknak jellemzően csak egyszer kell hitelesíteniük magukat. A felhasználók kezelése központosított és egységes, ami lehetővé teszi a meglévő adatok és információk (például számlázási adatok, szállítási címek és bankkártyaadatok) zökkenőmentes integrálását. Ez jelentősen hozzájárul a különböző szolgáltatások használatának egyszerűségéhez és gyorsaságához. [29].
3. Külső integrációs képességek: A szuperalkalmazások egyik legfontosabb célkitűzése, hogy a komplex szolgáltatási portfoliójukkal minél több aktív felhasználót vonzzanak és kössenek magukhoz, ideális esetben hosszú távon. Ennek eléréséhez kulcsfontosságú stratégia a mobilalkalmazáson belüli funkciók folyamatos fejlesztése, olykor külső szervezetekkel való partnerség, vagy az adatokhoz való hozzáférés lehetővé tétele révén [30]. A nyitott innovációs stratégia már számtalan esetben bizonyította a helytállóságát, a vállalat együttműködési hálózatába különböző más vállalati, intézményi kulcsszereplők bevonásának egyik fontos előfeltételeként és lehetőségeként [31]. Ezt a célkitűzést a szabványos adatátviteli interfészek, például az API-k (Application Programming Interfaces, azaz alkalmazásprogramozási interfészek) használata is támogatja [32].
4. Testre- és személyreszabhatóság: A mobileszközökön elérhető különféle szolgáltatások, az egyéni és egyedi beállítások, sőt gyakran még a képernyő megjelenítési felületének testreszabása is egyre inkább alapvető igénynek számít a felhasználók részéről. Minél egyszerűbb, kényelmesebb, vizuálisan tetszetősebb és egyediesíthetőbb egy alkalmazás, annál nagyobb valószínűséggel térnek vissza a felhasználók, és potenciálisan terjesztik a jó hírnevét, különösen igaz ez a szuperalkalmazások esetében [33]. A testreszabhatóság és az egyedi felhasználói élmény megteremtésének képessége nemcsak a felhasználók igényeinek kiszolgálása céljából fontos, hanem értékes visszajelzési lehetőséget biztosít a szuperalkalmazás tulajdonosai és üzemeltetői számára is [34]. Ezek az előnyök részletesebben a 6) pontban az Adathasznosítás és analitika című fejezetben kerülnek áttekintésre.
5. Ökoszisztéma létrehozása: Amint azt korábban bemutatásra került, a szuperalkalmazások egyik jellemzője a közös platformon kínált sokféle funkció és szolgáltatás sokasága. Gyakran még a TOP 10 szuperalkalmazás platformok között

is előfordul, hogy az egyetlen felületről, vagy alkalmazási keretrendszerből nyújtott szolgáltatások nemcsak belső szolgáltatókat, hanem a felhasználók számára elérhető külső partnereket is magukban foglalnak [35]. A szuperalkalmazások többsége, amelyek néhány alapvető szolgáltatást, például a pénzügyi tranzakciók egy részét vagy egészét egy külső, kapcsolódó szolgáltatón keresztül kínálják (pl. UBER), kiemelten mutatja az ökoszisztéma kiépítésének fontosságát. Minél megbízhatóbb, jobb hírű és az ügyfeleket sikeresen kiszolgáló ökoszisztéma-hálózattal rendelkezik egy szuperalkalmazás, annál hatékonyabban tud működni, és annál nagyobb forgalmat generál és nagyobb létszámú aktív ügyfélkört tud kialakítani. Természetesen egy szuperalkalmazás ökoszisztéma nemcsak belső vagy külső szolgáltatókat és alkalmazottakat foglal magában, hanem szabályozó hatóságokat is - hiszen általában olyan vállalatokról van szó, amelyek országokon és akár kontinenseken is átnyúló nemzetközi szolgáltatásokat nyújtanak. Emellett természetesen az ökoszisztémai részeinek tekinthetőek a különböző egyéb partnerek és maguk a szuperalkalmazás felhasználói is, akik közösségekbe szerveződnek, és így döntő szerepet játszanak az alkalmazás hosszú távú elkötelezettségének biztosításában. Mint korábban említésre került, a világ első és máig legnagyobb szuperalkalmazása, a WeChat üzenetküldő alkalmazásként indult, és a KakaoTalk is kiváló példája ennek a kiindulási helyzetnek [36].

6. Adathasznosítás és analitika: „Az adat az új arany” - ez a mondás különösen igaz a szuperalkalmazások világában. Ezt a birodalmat az egységes ügyfélkezelés, a bővülő szolgáltatási portfólió, a konszolidált adatbázisok és a folyamatosan és online érkező, exponenciálisan növekvő adatmennyiség jellemzi. Ez a környezet nemcsak az online és valós idejű elemzést könnyíti meg, hanem az elemzési eredmények és konkrét szándékok alapján azonnali beavatkozásokat is lehetővé tesz [37]. Alapvetően ezeknek az adatfeldolgozási és -kezelési gyakorlatoknak az a célja, hogy az ügyfelek számára gyorsabb, jobb és testreszabhatóbb szolgáltatást nyújtsanak, ezáltal egyszerre javítva a szuperalkalmazások szolgáltatási minőségét és kijelölve a leendő fejlesztési irányokat [38]. Egy egyszerű példával szemléltetve, ha egy Budapesten rutinszerűen használt bankkártyát hirtelen több egymást követő tranzakcióra használnának egy másik kontinensen, a Revolut-ban is használt adat- és forgalomfigyelő algoritmusok riasztást indítanának, értesítve a felhasználót és kérve annak igazolását, hogy valóban ő használja az adott kártyát. A szuperalkalmazások által folyamatosan gyűjtött adatok és információk azonban soha nem látott mélységű elemzéseket tesznek lehetővé az egyéni felhasználói viselkedésről és különösen a személyes jellemzőikről és szokásaikról. Az ilyen kiterjedt adatfelhasználás ezért jelentős aggályokat vet fel a felhasználói biztonság és az adatvédelem tekintetében is [39][40][41].

KÖVETKEZTETÉSEK

Jelen kutatás a megfogalmazott eredeti célkitűzések mentén először is bemutatta a szuperalkalmazás fogalmát, és átfogó szakirodalmi feldolgozás mellett aktuális áttekintést nyújtott erről a területről, rangsort felállítva az aktív felhasználói szám alapján jelenleg tíz legnagyobb innovatív mobilszolgáltatás kapcsán, amelyek adott ismérvek alapján

szuperalkalmazásnak minősülnek. A tanulmány jól dokumentált tudományos vizsgálat segítségével megállapította, hogy a szuperalkalmazások egyértelmű térnyerése, óriási aktív felhasználói bázisa és jelentősége ellenére a magasan jegyzett tudományos publikációkban - különösen a Scopus és a Web of Science indexeiben - meglepően kevéssé jelennek meg. Az elemzés számos dimenziót érintett, többek között az innovációt, a digitális átalakulást, az ügyfélélmény radikális javítását és a mobilszolgáltatások piacának fejlődését, és ezáltal bemutatta, hogy a SuperApp-ok milyen további széleskörű és figyelemre méltó kutatási lehetőségeket kínálnak.

Ez a tudományos vizsgálat hatékonyan mutatott rá a szuperalkalmazások területén fennálló jelentős kutatási hiányosságokra és a potenciális tanulmányok kiaknázatlan forrásaira. A Google Scholar forrásainak felhasználásával a tanulmány hat alapvető jellemzőt azonosított, amelyek meghatározóak a szuperalkalmazások kapcsán. A kutatás definiálta a hat főbb elemet, leíró jelleggel részleteket mutatott be és több szempont alapján leírta a digitális ökoszisztémán belüli jelentőségüket és szerepüket. Ezen túlmenően kiemelésre kerültek a szuperalkalmazások digitális transzformációt támogató potenciálja mind a piaci dinamikák, mind pedig a felhasználói elköteleződési stratégiák átalakításában. A feltárt eredmények és a téma aktualitása és jelentősége kapcsán a kutatás további tudományos kutatás szükségességét hangsúlyozza ezen a szuperalkalmazások és a hozzájuk szervesen kapcsolódó digitális ügyfélélmény területén.

KUTATÁSI JAVASLATOK

Ezen munka jelentős kutatásterületi hiányt állapított meg a szuperalkalmazások lefedettségével kapcsolatos magasan jegyzet tudományos adatbázisokban szereplő cikkek vonatkozásában. A forrásanyagok elemzése során nyilvánvalóvá vált, hogy sem a felhasználók száma, sem a szuperalkalmazások árbevételi információi nem azonosíthatók egyértelműen, és a különböző források között jelentős eltérések figyelhetők meg. Ez az ellentmondás még inkább kihangsúlyozza a további tudományos kutatás és hiteles információ-összegyűjtés és dokumentálás szükségességét. A jövőbeli kutatásoknak érdemes arra törekedniük, hogy az információs hiányokat és ellentmondásokat strukturáltan rögzítsék és kezeljék, megbízható és ellenőrzött forrásból származó adatokat összegyűjtve egy hiteles információkon alapuló elemzői kiindulási pontot hozzanak létre [42][43]. Ennek és erre alapuló további elsődleges kutatások segítségével jobban megérhetővé válnak a szuperalkalmazások gazdasági és működési dinamikái. Ezek az erőfeszítések elengedhetetlenek ahhoz, hogy olyan megbízható mérőszámok és keretek jöhessenek létre, amelyek pontosan tükrözik ezeknek az szuperalkalmazásoknak nevezett összetett, rendkívül innovatív digitális ökoszisztémáknak a folyamatos fejlődését és jövőbeli lehetőségeit.

FELHASZNÁLT IRODALOM

[1] How Many Apps are There in the World (2024) website: https://www.bankmycell.com/blog/number-of-mobile-apps-worldwide), accessed: 27th April 2024

[2] How Many Smartphones Are In The World? (2024) (Source: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world), accessed: 27th April 2024
[3] World Economic Outlook (2024) https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWORLD, accessed: 27th April 2024
[4] Roa, L., Correa-Bahnsen, A., Suarez, G., Cortés-Tejada, F., Luque, M. A., & Bravo, C. (2021). Super-app behavioral patterns in credit risk models: Financial, statistical and regulatory implications. Expert Systems with Applications, 169, 114486. https://doi.org/10.1016/j.eswa.2020.114486
[5] Ubaid, U.K., Yousaf, A., Garai-Fodor, M., Csiszárik-Kocsir, Á. (2023). Application of Project Management Techniques for Timeline and Budgeting Estimates of Startups. Sustainability, 15 : 21 Paper: 15526
[6] Blaskovics, B., Maró, Z.M., Klimkó, G., Papp-Horváth, V., Csiszárik-Kocsir, Á. (2023). Differences between Public-Sector and Private-Sector Project Management Practices in Hungary from a Competency Point of View. Sustainability 2023, 15, 11236. https://doi.org/10.3390/su151411236
[7] Csiszárik-Kocsir, Á., Dobos, O. (2022). Hungarian SMEs' role and opinion about research, development and innovation projects. In: Szakál, Anikó (szerk.) IEEE 20th Jubilee International Symposium on Intelligent Systems and Informatics (SISY 2022) Szabadka, Szerbia. pp. 199-203.
[8] Csiszárik-Kocsir, Á., Dobos, O. (2023a). The aspects of RDI project management in Hungary and Romania in the light of the pandemic. In: Szakál, Anikó (szerk.) SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics, Budapest, Magyarország : IEEE Hungary Section, pp. 179-184.
[9] Csiszárik-Kocsir, Á., Dobos, O. (2023b). The place and role of research, development and innovation activities in the life of domestic enterprises along business characteristics. In: Szakál, Anikó (szerk.) IEEE 17th International Symposium on Applied Computational Intelligence and Informatics SACI 2023 : Proceedings Budapest, Magyarország : Óbudai Egyetem, IEEE Hungary Section pp. 279-286.
[10] Csiszárik-Kocsir, Á., Dobos, O. (2023c). The place and role of research, development and innovation projects in the life of Hungarian and Polish micro, small and medium-sized enterprises after the pandemic. In: Szakál, Anikó (szerk.) SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics Budapest, Magyarország : IEEE Hungary Section, pp. 185-189.
[11] Dobos, O., Csiszárik-Kocsir, Á. (2023). Individual-level perception of research, development and innovation in the life of Hungarian enterprises. In: Szakál, Anikó (szerk.) IEEE 17th International Symposium on Applied Computational Intelligence and Informatics SACI 2023 : Proceedings Budapest, Magyarország : Óbudai Egyetem, IEEE Hungary Section, pp. 343-348.
[12] Shimota, K. (2023). The first super app: Inside China's WeChat and the new digital revolution. Earnshaw Books.
[13] WeChat Revenue and Usage Statistics (2024), website:https://www.businessofapps.com/data/wechat-statistics/ accessed on 27th April 2024

[14] [7] Alipay Statistics 2023 – Market Share, Facts and Marketing Trends (2023), website: https://www.enterpriseappstoday.com/stats/alipay-statistics.html accessed on 27th April 2024
[15] Amadeus partners with Rappi, the leading super-app in the Americas, (2022) website: https://amadeus.com/en/insights/press-release/amadeus-partners-with-rappi-the-leading-super-app-in-americas, accessed on 27th April 2024
[16] Revolut surpasses 30 million retail customers worldwide (2023), website: https://www.revolut.com/news/revolut_surpasses_30_million_retail_customers_worldwide/, accessed 27th April 2024
[17] Uber Technologies- statistics & facts (2024), website: https://www.statista.com/topics/4826/uber-technologies/#topicOverview, accessed 27th April 2024
[18] Neethu, K. (2023). Comparative Analysis between the Fintech Companies of India. Editorial Desk, 132.
[19] Basu, B., Sebastian, M. P., & Kar, A. K. (2024). What affects the promoting intention of mobile banking services? Insights from mining consumer reviews. Journal of Retailing and Consumer Services, 77, 103695.
[20] Press Release: India logs into Tata's super-app, Tata Neu (2022), website: https://www.tata.com/newsroom/business/tata-neu, accessed on 28th April 2024
[21] Gojek Statistics and User Count for 2024 (2024), website: https://expandedramblings.com/index.php/go-jek-statistics-and-facts/ accessed on 27th April 2024
[22] Grab Reports Second Quarter 2023 Results (2023), website: https://investors.grab.com/news-releases/news-release-details/grab-reports-second-quarter-2023-results accessed on 27th April 2024
[23] Diaz Baquero, A. P. (2021). Super apps: Opportunities and challenges (Doctoral dissertation, Massachusetts Institute of Technology).
[24] Zhu, Y. Q., Fang, Y. H., & Lim, S. Y. (2023). Investigating drivers of service extension success for a super app. Computers in Human Behavior, 149, 107928.
[25] Hasselwander, M. (2024). Digital platforms' growth strategies and the rise of super apps. Heliyon, 10(5).
[26] Ota, F. K. C., de Oliveira, C. G., Silva, R. M., & State, R. (2023, July). A Decentralized Super App. In 2023 24th IEEE International Conference on Mobile Data Management (MDM) (pp. 81-88). IEEE.
[27] Kavitha, D., Uma Maheswari, B., & Sujatha, R. (2023). Super Apps: The Natural Progression in Fin-Tech. In M. Naved, V. Ajantha Devi, & A. K. Gupta (Eds.), Fintech and Cryptocurrency (1st ed., pp. 383–412). Wiley. https://doi.org/10.1002/9781119905028.ch17
[28] Han, S., Li, X., & Hwang, H. (2022, June). Analysis of news data on 'super app'using topic modeling. In International Conference on Human-Computer Interaction (pp. 33-39). Cham: Springer Nature Switzerland.
[29] Minghai, Y., Wenqing, L., Akbar Khan, W., & Nurhalim, W. (2023). The SuperApp Implementation in Business: Revolutionizing Business Operations for a Seamless Future. Bincang Sains Dan Teknologi, 2(03), 118–123. https://doi.org/10.56741/bst.v2i03.436

[30] Fasnacht, D. (2021). Banking 4.0: Digital Ecosystems and Super-Apps. In: Wendt, K. (eds) Theories of Change. Sustainable Finance. Springer, Cham. https://doi.org/10.1007/978-3-030-52275-9_15
[31] Varga, J., Balogh, A., & Veres, R., (2023). A versenyképesség finn csodája, az innováció országépítő hatása. In: Varga, János; Csiszárik-Kocsir, Ágnes; Garai-Fodor, Mónika (szerk.) Vállalkozásfejlesztés a XXI. században 2023/2. kötet : A jelen kor gazdasági kihívásainak és társadalmi változásainak interdiszciplináris megközelítései Budapest, Magyarország: Óbudai Egyetem, Keleti Károly Gazdasági Kar (2023) 444 p. pp. 404-412. , 9 p.
[32] Wang, C., Zhang, Y., & Lin, Z. (2023). Uncovering and Exploiting Hidden APIs in Mobile Super Apps. Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, 2471–2485. https://doi.org/10.1145/3576915.3616676
[33] Şimşekler, S. (2024). The effects of service design on super app brand perception and user experience [M.S. - Master of Science]. Middle East Technical University.
[34] Yang, Y., Wang, C., Zhang, Y., & Lin, Z. (2023). SoK: Decoding the Super App Enigma: The Security Mechanisms, Threats, and Trade-offs in OS-alike Apps. https://doi.org/10.48550/ARXIV.2306.07495
[35] Van Der Vlist, F. N., Helmond, A., Dieter, M., & Weltevrede, E. (2024). Super-appification: Conglomeration in the global digital economy. New Media & Society, 14614448231223419. https://doi.org/10.1177/14614448231223419
[36] Steinberg, M., Mukherjee, R., & Punathambekar, A. (2022). Media power in digital Asia: Super apps and megacorps. Media, Culture & Society, 44(8), 1405-1419.
[37] Acevedo-Viloria, J. D., Pérez, S. S., Solano, J., Zarruk-Valencia, D., Paulin, F. G., & Correa-Bahnsen, A. (2021. november). Feature-Level Fusion of Super-App and Telecommunication Alternative Data Sources for Credit Card Fraud Detection. In 2021 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 1-6). IEEE.
[38] Roa, L., Correa-Bahnsen, A., Suarez, G., Cortés-Tejada, F., Luque, M. A., & Bravo, C. (2021). Super-app behavioral patterns in credit risk models: Financial, statistical and regulatory implications. Expert Systems with Applications, 169, 114486.
[39] Carvalho Ota F.K., C. G. B. de Oliveira, R. M. Silva and R. State, "A Decentralized Super App," 2023 24th IEEE International Conference on Mobile Data Management (MDM), Singapore, Singapore, 2023, pp. 81-88, doi: 10.1109/MDM58254.2023.00024.
[40] Kollár, Cs. (2018). A mesterséges intelligencia kapcsolata a humán biztonsággal. Nemzetbiztonsági Szemle, vol. 6, no. 1, pp. 5-23.
[41] Kollár, Cs. (2024). A biztonság megjelenése a humán tudományokban (1. rész). Biztonságtudományi Szemle, vol. 6, no. 2, pp. 13-22.
[42] Forgács, A., Lukács, J., Csiszárik-Kocsir, Á., Horváth, R. (2024). Towards the Investigation of Online Shopping Behaviours Using a Fuzzy Inference System. Decission Making Applications in Management and Engieneering, 7(2), pp. 337-354.
[43] Csiszárik-Kocisr, Á. (2023). The Purposes and Motivations of Savings Accumulation based on Generational Affiliation, Financial Education and Financial Literacy, Acta Polytechnica Hungarica, 20(3), pp. 195-210. DOI: 10.12700/APH.20.3.2023.3.12

STATUS OF CYBER PROTECTION REGULATION OF THE HUNGARIAN ELECTRICITY SYSTEM

A MAGYAR VILLAMOSENERGIA RENDSZER KIBERVÉDELMI SZABÁLYOZÁS HELYZETE

DÉR Attila[1]

Abstract

Critical infrastructures are the focus of attention around the world. Not without reason, as they play a key role in every aspect of life in every country, including our own. In Hungary, there are several of them, such as the health care system, transport and transportation, energy supply systems, etc. In this study, the focus will be on the electricity system within the energy supply systems. Unfortunately, based on the experience of the last years, the number of cyber attacks has increased sharply, especially in the energy sector. The spread of digitalisation throughout the management and control systems of electricity supply plays a major role in this. As a consequence, it is important to have an appropriate domestic legislative framework to ensure cyber security. This article makes proposals for this existing legislative framework to reduce the vulnerability of the Hungarian electricity system in a strategic and legislative context. Possible adaptation of the Swiss model in Hungary through EU-level directives Advantages, disadvantages, taking into account the specificities of the electricity supply system.

Keywords

Cybersecurity, electricity supply, critical infrastructure, digitalisation

Absztrakt

A kritikus infrastruktúrákat az egész világon kiemelt figyelem övezi. Nem véletlenül, hiszen minden országban és természetesen hazánkban is kulcsfontosságú szerepet töltenek be az élet minden területén. Magyarországon több ilyen is van, mint például az egészségügyi rendszer, közlekedés és szállítás, energiaellátó rendszerek stb. Ebben a tanulmányban az energiaellátó rendszereken belül a villamosenergia rendszere lesz fokuszálva. Sajnos az utóbbi évek tapasztalataiból kiindulva a kibertámadások száma erőteljesen megnőtt, különösen az energiaszektorban. Nagy szerepet játszik ebben a digitalizáció elterjedése a villamosenergia ellátás teljes irányítási és szabályozási rendszereiben. Ennek következtében fontos, hogy megfelelő hazai jogszabályi keret legyen a kiberbiztonság megteremtéséhez. A cikk erre a meglévő jogszabályi környezetre tesz Javaslatokat a magyar villamos-energiaellátó rendszer sérülékenységének csökkentésére stratégiai és jogszabályi összefüggésében. Európai Uniós szintű irányelveken keresztül a svájci modellnek a lehetséges adaptációja Magyarországon Előnyök, hátrányok, villamos-energiaellátó rendszer sajátosságainak figyelembe vételével.

Kulcsszavak

Kiberbiztonság, villamosenergia-ellátás, kritikus infrastruktúra, digitalizáció

[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-rendszer fő célja a villamosenergia-termelése, -átvitele és –szállítása az erőművektől a végfelhasználókig, amelyek közé tartoznak a háztartások, a kereskedelmi épületek és az ipar. 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 Magyarországon 750kV-, 400kV és 220kV értékek között szállítják a villamos-energiát alap átviteli hálózatként. Ennek a gerinc hálózatnak a feszültségszint határa letranszformálva 120kV feszültségszint, ahol már az elosztó hálózat kezdődik. Az elosztó hálózatot üzemeltetők tovább csökkenti a 120kV feszültségszintet ipari fogyasztók számára szükséges különféle 35kV-, 20kV és 10kV középfeszültségű szintekre. A lakossági fogyasztóknál, pedig a 0,4kV kisfeszültségű hálózatot, mint a legkisebb tovább nem transzformált feszültség értéket figyelhetjük meg.[1] [2]

Magyarországon az erőművek feladatuk szerint lehetnek közcélúak, ahol egy ország ipari vagy kommunális fogyasztóinak ellátása a cél vagy nem közcélúak, ahol pedig csak egyes speciális üzemeknek az energiaellátása a feladat. Továbbá lehet a magyar villamosenergia-rendszerrel együttműködő, ahol a teherelosztást a diszpécserközpont végzi vagy nem együttműködő csak egy létesítményt szolgál ki. Kihasználtság szempontjából három csoportot különböztetünk meg az egyik az alap erőművek, ilyen például a paksi. A másik a villamosenergia igény változásai szerint működő menetrendtartó erőművek, mint a Mátrai és a Dunamenti. A harmadik típusúak pedig a csúcserőművek, amelyek nyilván a nevükből is kikövetkeztethetőek, hogy csak maximális energiafogyasztásnál termelnek. Későbbi leírásnál fontos lehet még, hogy mely szervezetek irányítják a magyar villamosenergia-rendszert, amely több szintet különböztet meg egymástól. Az egyik ilyen szervezet a Magyar Villamosenergia-ipari Átviteli Rendszerirányító Zártkörűen Működő Részvénytársaság (MAVIR Zrt), amely országos szinten felel az ellátásbiztonságért. Továbbá gondoskodik fogyasztás pillanatnyi egyensúlyának fenntartásáért, ellenőrzi a hálózat túlterheltségét, illetve megfelelő feszültségszintjét. A területi áramszolgáltatóknál a Körzeti Diszpécseri Szolgálatok végzik az üzemirányítást, ahol a 120 kV-os és alacsonyabb feszültségszintű elosztóhálózatok helyezkednek el. Végül a legalsóbb feszültségszintű elosztóhálózatokat Üzemirányító Központok működtetik, felügyelik és karbantartják. A magyar energiaszektor piacának és ellátásbiztonságának szabályozásáért felelős hatóság a Magyar Energetikai és Közmű-szabályozási Hivatal. Kiberbiztonság területén fontos elemként létrehozta az információmegosztó és elemző központot, amely az érintett energiaellátó szervezetek közötti fenyegetésfelderítési adatfolyam megosztásában, elemzésében és a korai felderítésben kulcsfontosságú szerepet tölt be.[3]

SZABÁLYOZÁS

Európai Uniós szabályozás

Az Európai Unió magasabb szinten csak a 2000. évektől kezdte el komolyabban vizsgálni a tagállamok infrastruktúráinak védelmi helyzetét. Ehhez nagymértékben hozzájárult több terrortámadás, amely főként kritikus infrastruktúrák ellen irányult globális és európai szinten. Az első ilyen kezdeményezés a kritikus infrastruktúrák védelméről szóló európai programcsomag (European Programme for Critical Infrastructure Protection) volt.

Majd ebből lett egy irányelv, amelynek a frissítése 2008.-ban 114/2008/EK irányelvként volt ismeretes, amelyben már olyan fontosabb pontokat is megemlítenek, mint az energia és közlekedés ágazatok prioritásként történő kezelése; sebezhetőségi pontok meghatározásának kötelezettsége; azonosítás és kijelölés folyamatának meghatározása stb.[14]

Az Európai Parlament és Tanács kritikus szervezetek ellenállóképességéről szóló Irányelve (CER) a statikus fizikai rendszerszemléletről a rezilienciára, ellenállóképességre tolja el a szabályozás irányát, amely a rendszer minél kisebb megszakítását vagy a már megtörtént incidensek mielőbbi visszaállítását célozza meg. Ebben az ajánlásban a kritikus infrastruktúráknak is bővült a körük, így nem csak az energia és a közlekedésre koncentrál, mint az előző szabályozások, hanem a többi kulcsfontosságú nemzetgazdasági ágazatra is.[15]

A Hálózati és Információs Rendszerek (Network and Information System) röviden: NIS, amely 2016/1148 irányelvként lett kiadva már részletesen lefekteti a kiberbiztonsági alapokat az egész Unió területén. Különösebben nem foglalkoznék ezzel a NIS-el inkább az újabb verziójával a NIS2 2022/2555 irányelvre térnék ki, amely például az előbb említett CER direktívával kézen fogva szabályozza a kritikus infrastruktúrákat, úgy hogy az egyik szabályozás ne üsse a másikat. A NIS2 kiberbiztonsági kockázatok nem jelennek meg a CER-ben, de amiket nem fektetett le a NIS2 azokat a rizikófaktorokat viszont tartalmazza a CER.[13]

ENISA (European Network and Information Security Agency), amely az Unió egyik legfontosabb kiberbiztonsági szervezete. Tanácsadó szervezetként különféle ajánlásokkal, dokumentumokkal segíti a tagállamokat stratégiáik kialakításában. Bizonyos kritikus infrastruktúráknál a bejelentési kötelezettséget ír elő, ha valamilyen váratlan incidens éri a kiemel rendszerelemet. Az Európai tagállamok, mint Magyarország is nagyon közel van a NIS2 irányelv bevezetéséhez, amely 2024.10.18.-tól már hatályba fog lépni.

Külön a pénzügyi szektorra is készült rendelet, amely a bankok informatikai biztonsági előírásait szigorítja a digitális működési ellenálló képességről szóló rendelet (Digital Operational Resilience Act, DORA)

Magyar szabályozás

2007. évi LXXXVI. törvény a villamos energiáról ennek a törvénynek a legfőbb csapásvonala a biztonságos villamosenergia versenypiac kialakítása.[16]

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Magyarországon ez az első törvénybe iktatott szabályozás, ahol konkrétan a kritikus infrastruktúrákról szól, habár nem ezzel az elnevezéssel szerepel a törvényben. Nyílván a legfontosabb célja a törvénynek, hogy kijelölje nemzeti létfontosságú rendszerelemeket, ahol az üzemeltetői azonosítás vizsgálat elkészítését követően az ágazati kijelölő szakhatóság dönt, hogy ki tartozik ezen törvény hatálya alá. A törvény megemlíti a hatóság és a már besorolt létesítmények közötti kapcsolat biztosítására szolgáló összekötő személy kötelező kijelölését és feladatát. Továbbá a hivatásos katasztrófavédelmi szervet kijelöli, hogy hatósági eljárásokban hivatalosan járjon el. A jogszabály meghatározza, hogy mely rendszerelemek kapcsolódhatnak az Európai Unió rendszereihez és létesítményeihez. Végül az 1. számú mellékletében 10 darab ágazatot sorol fel, ahol az energia ágazatnál említi meg a villamosenergia rendszer létesítményeit kivétel Paks nukleáris biztonságának kérdéskörét.[17]

Az előző törvény tartalmának konkrét gyakorlati megvalósítását a 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló rendelet részletesen tárgyalja. Megtalálhatjuk például az 1. mellékletében a horizontális elvárásokat vagy a 2. mellékletében az üzemeltetői biztonsági terv részletes tartalmi követelményeit.[20]

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról a magyar kiberbiztonság általánosságban megfogalmazott alapjait célját és feladatait fekteti le. Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat a NIS ezt egészítette ki, de villamosenergia szektor problematikájával nem foglakozik.[18]

Magyarországon a 2013. évi információbiztosági törvény(Ibtv) fektette le elsőként két legfontosabb információs rendszerek biztonsági felügyeltét megszervező intézményt. Az egyik a Nemzetbiztonsági Szakszolgálat a civil platformot képviseli, itt is főként az államigazgatási szerveket. A másik a Katonai Nemzetbiztonsági Szolgálat, amely a katonasággal kapcsolatos biztonsági eseményeket kezeli. Ezen eseményközpontok feladatait eljárásaikra vonatkozó általános rendelkezéseit a „187/2015. (VII. 13.) Korm. rendelet részletezi az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelőfeladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról".[19][21]

„271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól biztonsági események bejelentéséről szól." [22] A kritikus infrastruktúrák sérülékenységvizsgálatát a polgári nemzetbiztonsági szolgálat végzi, hogy megvizsgálja ezen elektronikus rendszerek ellenálló képességét. A megtalált hiányosságokat a hatóság informatikai szakemberei górcső alá helyezik, kiértékelik és ezekre javaslatokat, megoldásokat tesznek, hogy az érintett kritikus rendszereket még biztonságosabbá tegyék.

2020. évi CLXXVI. törvény a villamos energiáról szóló 2007. évi LXXXVI. törvény módosításáról főként energiaközösségeket, átviteli rendszerirányítói feladatokat és elosztói rugalmassági szolgáltatásokat érint.[24]

Viszont a Nemzeti Energiastratégiában már megemlítik a villamosenergia szektor infókommunikációs védettségét és ezekkel összefüggő elhárítási lehetőségeit. Ugyan ebben az évben jelent meg a 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, amelyben a kibertér kutatására és fejlesztésére és annak védelmi összetevőire hívja fel a figyelmet. Továbbá rávilágít arra a tényre is, hogy ebben a témában kutatással és fejlesztéssel foglalkozó intézmények jóval kevesebben vannak jelen Magyarországon, mint más nagyobb nyugat-európai országban, mint például Németországban vagy Franciaországban. Ezzel összhangban az oktatás fejlesztését is figyelembe kell venni, mivel a fenti törekvések alapja és kiindulópontja. [1163/2020. (IV. 21.) Korm.]

A villamosenergia-rendszer hatókörében lévő kiemelt kockázatú infrastruktúrák ágazati besorolására a Magyar Energetikai és Közmű-szabályozási Hivatalt jelölte meg a 374/2020. (VII. 30.) Korm. rendelet, mint eljáró hatóság. Megemlítésre kerül a hazai és Uniós kiemelt kockázatú rendszerelemek besorolása különböző paraméterek szerint. Fontos jelenség a rendeletben, hogy pontosan meghatározza a kritikus zavarokat, küszöbértékeket és a kiemelkedő kockázatú eseményeket.[23]

Sajnos az 526/2022. (XII. 16.) Korm. rendelet sem említi a kibevédelemet csak az orosz-ukrán háború következtében kialakult vészhelyzeti intézkedéseket, amely a villamos energiáról szóló 2007. évi LXXXVI. törvény eltérő alkalmazásából fakadóan adtak ki. Ugyan ez a helyzet a 2021. évi XCIII. törvénnyel kapcsolatosan is, amely szintén nem szól kiberbiztonságról se energetikai biztonságról.[25][26]

Viszont a legfrissebb kiberbiztonsági törvényünk: 2023. évi XXIII. törvény, amelyet a 10/2023. (V. 15.) Szabályozott Tevékenységek Felügyeleti Hatósága azaz röviden SZTFH rendelete egészíti ki. Nyilván ezek és a fent említett szabályzatok a NIS2 irányelvvel összhangban vannak, sőt mint Európai Uniós tagállamként ez kötelező keretrendszerrel bír még, akkor is, ha élesítve csak ez év végén lesz. [27]

A kiberbiztonsági törvénybe az (EU) 2019/881 uniós rendelet szövegét illesztették be tanúsítási hatóság feladatainak meghatározásához. Magyarország területén belül e törvényben meghatározott kiberbiztonságot érintő rendszereket a következő csoportosításba tehetők alap (alapvető kockázatok), jelentős (korlátozott szakértelemmel és erőforrásokkal rendelkező) és magas (jelentős szakértelemmel és erőforrásokkal) szintekbe. Ellenőrzésre kijelöltek körét, így határozta meg a törvény: kiemelten kockázatos, kockázatos és olyan vállalkozások, amelyek elektronikus információs technológiához szorosan köthetőek. Ezeket a felügyelt piaci vagy nem piaci szegmenseket kétévente független auditor fogja megvizsgálni, akiket SZTFH elnöke biz meg az ellenőrzésre.[28]

NIS2 IMPLEMENTÁLÁSA MAGYARORSZÁGON

A NIS2-irányelv kiterjeszti elődjének tárgyi hatályát új ágazatokra, amelyek kockázatos és kiemelten kockázatos kategóriába vannak besorolva, illetve vannak még olyan NIS2-es szabályozás alá eső piaci szegmensek, akik az információbiztonság szempontjából meghatározó jelentőségűek.

A 2022/2555-ös európai direktíva hatálya alá tartozó szervezetekre korábbinál sokkal szigorúbb követelmények vonatkoznak, mint például a kiberbiztonsági szintek tesztelésének és a titkosításának hatékonyabb használatának feltételei vagy akár megemlíthető a vizsgálandó rendszerek biztonsági réseire vonatkozó szigorítások is. Az új szabályozás az incidensek jelentése terén is pontosabb rendelkezéseket tartalmaz. Ezen túlmenően a tagállamok megkövetelhetik, hogy az alapvető és fontos szervezetek kötelezően tanúsítsák a termékeket, szolgáltatásokat és folyamatokat a kiberbiztonsági törvényben előírt európai tanúsítási rendszereknek megfelelően. Az 5G hálózati elvárásokkal összhangban a kritikus infrastruktúrák kockázatértékelése is sokkal komplexeben lesz. Így ildomos lenne az Európai Unión belül a kockázatos ellátási láncok megfelelő felügyeletét a tagállamoknak az ENISA-val együttműködve ellátni. Újdonság még a kockázatkezeléssel kapcsolatosan, hogy a piaci és az állami szereplők legfelsőbb vezetőinek meghatározott felelősséggel kell majd rendelkezniük. Továbbá bevezetése kerül majd a jogsértések visszaszorítására szolgáló nagyobb pénzbírság is.[4][13]

IS2 menetrend Magyarországon

Az első és lefontosabb dolog, hogy megállapítást nyerjen az érintettség jogi aktusa a NIS2 direktívában meghatározottak szerint. A menetrend első szakasza 2024 január elsejétől 2024 június 30.-ig terjedő időszak, ahol az érintett szervezeteket osztályba sorolják, a

hatóság lajstromba veszi, illetve információbiztonságért felelős vezetőt kijelölik. 2024 október 18-án a tagállamokban és hazánkban is hatályba lép a 2022/2555-ös direktíva. 2024 december 31-ig kell az érintett szegmenseknek szerződni az auditorokkal, akiket Szabályozott Tevékenységek Felügyeleti Hatósága választ ki és a névjegyzékébe felveszi őket. 2025 december 31.-ig kötelező lesz lefolytatni az első kiberbiztonsági ellenőrzési vizsgálatot, majd a következőt 2 év múlva 2027-ben, illetve kettő évente kell ismételten lefolytani, igazodva az első audithoz eredményeihez.[5]

Fontosabb felkészülési feladatok

Első lépés a 2022/2555 irányelv alá tartozó infrastruktúrák vagy szolgáltatók kockázatelemzése meghatározott paraméterek szerint, majd ezek kiértékelése. Az értékelések alapján létrejön egy hiányosságokat feltáró GAP-elemzés. Ennek az analízisnek az eredményéből születik, majd egy forgatókönyv, amelynek tartalmaznia kell az érintett létesítmények biztonsági réseinek javítását és a jövőre vonatkozó fejlesztési javaslatokat. Következő lépésben lehetne konkretizálni a vizsgált rendszerek, illetve a technikai összetevők szabályzatit az adott rendszerelemeknél. Feladatok közé tartozik még a NIS2 által előírt technikai kontrollok bevezetése (pl. SIEM, többfaktoros hitelesítés, hálózati eszközök integrációja, sérülékenységek kezelése stb.). A kutatásom tárgyából fontosabb megemlítenem a főként kritikus infrastruktúráknál előforduló információs technológia(IT) és az operatív technológia(OT) megfelelő szintű szabályozása. Az IT-nél érdemes a frissített Nemzeti Szabványügyi és Technológiai Intézet (NIST) 800-53 rev5. amerikai szabványát alkalmazni, míg az OT-nél a NIST 800-82 biztonsági előírásokat. Továbbá előírás még, hogy az érintett szervezeteknél ki kell jelölni egy információbiztonsági vezetőt, aki a kibertan törvényben meghatározott végzettséggel és szakmai tapasztalattal rendelkezik és a törvényben meghatározott feladatokért egyetemlegesen felel.[6]

SVÁJCI MODELL

Röviden a svájci villamosellátás felépítéséről a felelhető legfrissebb adatok alapján mintegy 610 aktív hálózatüzemeltető működök az alpesi ország teljes területén. Ezek összesen mintegy 5,65 millió fogyasztót látnak el, és mintegy 5,9 millió mérési pontot szolgálnak ki. Az ország természeti adottságiból kifolyólag jelentős eltérések vannak a szolgáltatók között, mivel a legnagyobb szolgáltató több mint 300 000 fős ügyfelkörrel rendelkezik, addig a legkisebbnek mindössze csak 45 fogyasztó csatlakozik. Egyébként az átlagos ügyfélkörrel rendelkező hálózatüzemeltetők megközelítőleg 1620 háztartást vagy egyéb ipari fogyasztót látnak el. [7]

Általánosságban is elmondható, hogy Svájc helyzete Európában eléggé egyedi, ami megmutatkozik villamosenergia piacának kialakításával kapcsolatosan is. Ugyanis ebben a kis államban a piaci versenyhelyzet korlátozott volt bizonyos kritikus infrastruktúrák tekintetében. Míg a nagy ipari fogyasztók nemrégiben lehetőséget kaptak arra, hogy megválaszszák szolgáltatójukat, addig a kisebb ipari szegmenseket vagy magánfogyasztókat továbbra is többnyire helyi monopóliumnak számító önkormányzati közműszolgáltatók látják el. [8]

„Svájc nem termel szénhidrogéneket. Az ország energiatermelése 2021-ben atomenergiából (45%), vízenergiából (28%), bioenergiából és hulladékból (25%) állt, és csak kis arányban (2,8%) váltakozó megújuló energiákból.” [9]

A hazai termelés a teljes energiaszükséglet 50%-át fedezi, a fennmaradó rész pedig importált fosszilis tüzelőanyagokból áll. Ettől függetlenül a kis alpesi országban a villamosenergia-ellátás biztonsága nagyon magas színvonalon áll. Európa többi tagállamához hasonlítva a legelitebb országokhoz tartozik, mint például Németország vagy Dánia. [9]

Svájcban a közelmúltban csak önkéntes intézkedések és ajánlások voltak érvényben a kritikus infrastruktúrák területén, nyilván ez a hagyományos politikai berendezkedésből is fakadt. Mostanra viszont – a cikkem bevezető részére is utalva a kibertámadások gyakoriságára - már nem kérdéses, hogy egyes intézkedések kötelező jellegűek a magas kockázatú intézmények számára.

Energetikailag és így nyilvánvaló kiberbiztonságilag is a környező országokkal (Németországgal, Franciaországgal, Olaszországgal és Ausztriával) területi elhelyezkedéséből fakadóan szimbiózisban van.

Svájcban az első kifejezetten elektronikus támadások elleni intézkedésekre a 2018.-ban kiadott nemzeti kiberbiztonsági stratégia adott konkrét javaslatokat és válaszokat. Előtérbe került a kritikus infrastruktúrák elektronikus és infókommunikációs védelmének hathatós előmozdítása vagy az incidensek vonatkozó bejelentési kötelezettségek és a válságkezelési gyakorlatok forgatókönyveinek fontossága.

A Szövetségi Gazdasági Ellátási Hivatalra (FONES) együttműködve tevékenykedik a Svájci Villamosenergia-ipari Társaságok Szövetségével (AES)

„A gyakorlatias megközelítés és az „egy az egyben" megoldásra való svájci törekvés eredményeként született meg a Minimum standards for improving ICT resilience (Swiss Federal Office for National Economic Supply, 2018) és egy kapcsolódó értékelési eszköz, amelyben a NIST kiberbiztonsági keretrendszerén (identify, protect, detect, respond, recovery) alapuló 106 pontból álló, visszafogott ellenőrző lista segítségével a vállalatok ellenőrizhetik kiberbiztonsági érettségi szintjüket. Az egyes ellenőrzési pontok olyan nemzetközi szabványokra hivatkoznak, mint többek között a NIST kiberbiztonsági keretrendszer, az ISO 27001 és az ISO 27019." [8]

Svájci modell elemzése

Az Uniós Intelligens hálózati munkacsoport már 2014-ben ajánlotta a kiemelt rendszerelemek üzemeltetőinek, hogy kiberbiztonsági intézkedéseit igazítsák az ISO/IEC 27001, ISO/IEC27002 és ISO/IEC27019 szabványaihoz. Később 2018-ban a Svájci Szövetségi Energiaügyi Hivatal (SFOE) a Nemzeti Szabványügyi és Technológiai Intézet (National Institute of Standards and Technology, röviden: NIST) amerikai szabvány mintája alapján alkotta meg az infókommunikációs technológiára épülő úgynevezett minimumszabványt.

Fabian Heymann felmérése a svájci villamosipar résztvevőinek operatív technológia (OT) és információs technológia (IT) fejlettségére irányult. A kutatás szerint a NIST fokozatait felhasználva az információs technológia fejlettsége a legtöbb kategóriában el sem éri az 1. alapszintet. A legnagyobb átlagértéket Svájcban az operatív technológia érte el 1,10-es fokozattal. Ez többnyire annak volt köszönhető, hogy a múltban nagyobb hangsúlyt fektettek a megelőző képességekre, mint az észlelésre és a reagálásra. A villamosipari infrastruktúrák felügyeleti és vezérlő rendszerei Svájcban még most is a beszállítók általi szab-

ványok alapján védettek. Amivel első olvasatra nem is lenne gond, csak éppen nincs összhang a két fél között, nincs közös oda-vissza csatolás és közös kutatás kiberbiztonsági és egyéb védelmi szempontokat figyelembe véve. [8]

A svájciak általában minden döntést azon a szinten hozzák meg és hajtják végre, ahol a legnagyobb szakértelemmel rendelkeznek az érintettek. Nincs ez másként az elektronikus eszközök védelmével sem, ami azt az alomáliát eredményezi, hogy az egyik kanton energiaágazata korszerűbben van felvértezve logikailag és fizikailag, mint a másik térség, pedig egy államról beszélünk. Habár az Európai Uniónak nincs közel sem, olyan joghatása a svájci döntéshozatalra, mint hazánknak, ennek ellenére bizonyos Uniós rendelkezéseket saját biztonságuk érdekében érdemes lenne átvenniük. Nyílván vannak erre már kezdeményezések, mint például a villamosenergia-rendszer kooperációja a szomszédos államokkal, ahol nem lehetőség hanem kötelező a szükséges mértékű európai szabályozás harmonizálása. [8]

Érdemes megemlíteni ebben a fejezetben a kibervédelem fontos védvonalát a Számítógép-biztonsági Incidenskezelő Csoportokat (Computer Security Incident Response Team), ahol szintén erőteljesen érvényesül Svájcra oly jellemző szerződés szabadság elve. Ennek következtében a nagy autonómia miatt, kevés kötelező jellegű jogi szabályozás vonatkozik ezekre a csoportokra. Így az egységes szabályozás erősen háttérbe szorul, amelyre Svájcnak igencsak oda kellene figyelnie majd a közeljövőben. [10]

Végül Pozitívumként a svájci szakpolitika már évek óta több innovációs stratégiát kidolgozott, amelyben a villamosenergia-ellátás jelenlegi állapota jól fejleszthető. Egyik ilyen „eszköz” például sandbox magyarul homokozó, ahol olyan biztonsági teszteléseket tudnak végrehajtani a villamosiparban, amelyek jelenlegi szabályozás keretek között nem lehetne megvalósítani. A homokozók szolgáltatások kifejlesztésére is módot adhat, ahol új intézkedések jelenlegi hiányosságait lehetne felderíteni és koordinálni anélkül, hogy az egész élő rendszert megbolygatnánk. [11]

A SVÁJCI MODELL ADAPTÁCIÓJA MAGYARORSZÁGON

Elsőként szeretném hangsúlyozni, hogy mivel hazánk az Európai Unió közösség tagja, így hiába van annyiféle modell és irányelv szerte a világban, mindenféleképpen prioritást élveznek az EU-s jogi normák a magyar szabályozásra. Gondolok itt például a kutatás szempontjából releváns NIS2 irányelvre, amelyet előző fejezetben már kifejtettem. Ennek ellenére érdemes elemezni más országok sajátos ipari rendszereit és stratégiáit. Mivel valóságos ipari környezetben szerezhetünk tapasztalatokat, amelyeket lehetetlen volna leteszteln szimulációs szoftverekkel. Így került előtérbe például a svájci modell, amely hasonló méretű ország, mint Magyarország, de eltérő ipari adottságokkal és szabályozásokkal rendelkezik, amelyek tanulságosak lehetnek hazánk energiabiztonsága számára. Ennek megfelelően szakértői interjúk és a Secosys csoport ajánlását figyelembe véve egy lehetséges adaptáció lehetne a Common Criteria, amely a 2022/2555 Uniós keretrendszerrel harmonizál, több éves szakmai tapasztalaton nyugszik, a beszállítóknak nemzetközi elfogadást biztosít és hazai bevezetése viszonylag rövid időn belül kivitelezhető lehetne. Első lépésként egy forgatókönyvet kellen elkészíteni, amelyben már tesztüzem értékelése és a problémák feltárása elkezdődik. Majd a további lépéseknél ISO 27000-es szabványcsaládot alapul véve a svájci gyakorlat hibáinak kiszűrésével hazai jól bevált módszertanokra épülve kialakítani egy elfogadható és precíz villamosenergia rendszert védő kibervédelmi szabályozást. [12]

Másfajta megközelítésben a villamos ágazat tanúsítási és ellenőrzési rendszerét differenciáltan kockázati kategóriák mentén kellene növelni a követelményeket a korábban említett Svájci modell kapcsán, ahol sok kisebb villamosenergia elosztó szolgáltató kibújt a központi kötelezettség alól, mivel se szakmailag se gazdaságilag nem volt indokolt bevezetésük.

ÖSSZEFOGLALÁS

Nem kétséges, hogy a magyar kritikus infrastruktúra egyik legmeghatározóbb képviselője a villamosenergia ágazat teljes rendszere. Így védelmére különösen nagyobb hangsúlyt kell fektetni, mint általában más ágazatokra, mivel a többi kritikus infrastruktúra működésére is jelentős hatást gyakorol. Mivel a technológiai és fizikai adottságai megkövetelik, ezért folyamatos a nap 24 órájában üzemeltetni kell ezeket a rendszereket. Pár perces kiesés is hatalmas problémákat okozhatnak az ország villamosenergia-ellátásban. Kutatásomban inkább jogszabályi oldalról közelítettem meg az elektronikus információs rendszerek védelmének problémakörét. Ennek következtében a NIS2-es európai szintű szabályozást emeltem ki, amely 2024 október 18-tól már teljes hatállyal Magyarországot is fogja érinti. Természetesen implementálása hazánkban már folyamatban van, ahogy ezt a cikkben ki is fejtettem. Továbbá megvizsgáltam a svájci villamosenergia-rendszer sajátosságait az európai normatívákat figyelembe véve és ezekre a tapasztalatokra építve kialakítottam egy javaslati szinten lévő magyar adaptációt. Nyílván több ország szakági gyakorlatát is lehetett volna elemezni, de ennek a cikknek meghaladta volna a terjedelmét. A jövőben biztosan kiterjesztem majd a kutatásomat más európai és/vagy Európán kívüli országokra is. Összefoglalva a kutatással kapcsolatos tapasztalataimat a következő fontosabb javaslataim lennének: célszerű lenne az Európai Unión belül a kockázatos ellátási láncok megfelelő felügyeletét a tagállamoknak az ENISA-val együttműködve ellátni. A tagállamok közötti információmegosztás intézményesítésére létre kellen hozni egy európai sajátoságokra épülő szabványcsaládot. Továbbá javaslom az IT-nél alkalmazott NIST 800-53 rev5. és az OT-nél a NIST 800-82 biztonsági előírásokat Uniós sajátosságokra tovább fejleszteni. [3]

FELHASZNÁLT IRODALOM

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

[2] 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.

[3] C. Krasznay és G. Gyebnar, „Possibilities and Limitations of Cyber Threat Intelligence in Energy Systems”, in *2021 13th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia: IEEE, máj. 2021, o. 171–188. doi: 10.23919/CyCon51939.2021.9468289.

[4] A. Besiekierska, „Legal Assessment of the National Cybersecurity System in Poland in the Light of the New Developments in the NIS2 Directive”, in *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*, Opatija, Croatia: IEEE, máj. 2023, o. 1474–1477. doi: 10.23919/MIPRO57284.2023.10159958.

[5] Tóth Tamás, „A NIS2 irányelv az Európai Unió kiberbiztonsági szabályozása”. [Online]. Elérhető: https://nis2iranyelv.hu/
[6] H. Altaleb és Z. Rajnai, „Malware Attacks on SCADA Systems: Assessing Risks and Strengthening Cybersecurity Measures”, in *2023 IEEE 21st Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, Pula, Croatia: IEEE, szept. 2023, o. 000625–000630. doi: 10.1109/SISY60376.2023.10417951.
[7] Swiss Federal Electricity Commission ElCom, „Report on the activities of ElCom 2022”, Bern, 6/2023, 2023. Elérés: 2024. május 28. [Online]. Elérhető: https://www.elcom.admin.ch/elcom/en/home/documentation/reports-and-studies/taetigkeitsberichte.html
[8] F. Heymann, S. Henry, és M. Galus, „Cybersecurity and resilience in the swiss electricity sector: Status and policy options”, *Utilities Policy*, köt. 79, o. 101432, dec. 2022, doi: 10.1016/j.jup.2022.101432.
[9] INTERNATIONAL ENERGY és AGENCY, „Switzerland 2023 Energy Policy Review”, Switzerland, Review, 2023. Elérés: 2024. május 30. [Online]. Elérhető: https://iea.blob.core.windows.net/assets/b6451900-e6ef-45a8-922d-117520e09a82/Switzerland2023.pdf
[10] P. Meyer és S. Métille, „Computer security incident response teams: are they legally regulated? The Swiss example”, *Int. Cybersecur. Law Rev.*, köt. 4, sz. 1, o. 39–60, márc. 2023, doi: 10.1365/s43439-022-00070-x.
[11] F. Heymann, J. Schmid, M. Vazquez, és M. Galus, „Regulatory sandboxes in the energy sector - review and learnings for the case of Switzerland”, in *CIRED 2021 - The 26th International Conference and Exhibition on Electricity Distribution*, , Online Conference: Institution of Engineering and Technology, 2021, o. 3229–3233. doi: 10.1049/icp.2021.1730.
[12] 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

JOGSZABÁLYOK

[13] *AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/ 1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)*
[14] *A TANÁCS 2008/114/EK IRÁNYELVE az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről.*
[15] *AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2557 IRÁNYELVE (CER) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről*.
[16] *2007. évi LXXXVI. törvény a villamos energiáról*.
[17] *2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről*.

[18] *1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról*.
[19] *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról*.
[20] *65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról*.
[21] *187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról*.
[22] *271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól*.
[23] *374/2020. (VII. 30.) Korm. rendelet az energetikai létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről*.
[24] 2020. évi CLXXVI. törvény a villamos energiáról szóló 2007. évi LXXXVI. törvény módosításáról.
[25] *2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról*.
[26] *526/2022. (XII. 16.) Korm. rendelet a villamos energiáról szóló 2007. évi LXXXVI. törvény veszélyhelyzet ideje alatt történő eltérő alkalmazásáról*.
[27] *2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről*.
[28] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/881 RENDELETE az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály.

KÖSZÖNETNYILVÁNÍTÁS

Egyetemi Kutatói Ösztöndíj Program-Kooperatív Doktori Program keretében megvalósuló kutatás, amelyet az Óbudai Egyetem Kutatási és Fejlesztési Alapból finanszírozott.

DIFFERENT CULTURES IN SAFETY AND NON-SAFETY PROFILE COMPANIES

ELTÉRŐ KULTÚRÁK BIZTONSÁGI ÉS NEM BIZTONSÁGI PROFILÚ VÁLLALATOKNÁL

KERTAI-KISS Ildikó[1]

Abstract

The evolution of safety and security culture is changing from risk avoidance to preventive, proactive and, as a new approach, positivist (maximizing improvement security mechanisms) thinking is becoming the guiding attitude. It is also a change of mindset that, in addition to the safe internal functioning of companies, external influences are becoming increasingly important in efforts to maintain normal functioning. Safety and security have become a discipline and economic sector in their own right, but the issue of safety and security is also a major challenge for companies and employees with a non-safety profile. The objective of my research is to assess and analyse the perceptions, attitudes and motivations based on value preferences of employees of companies operating in Hungary regarding organisational safety and through this to identify the elements of safety culture specific to the company. In the present study, I will present the most important differences based on the safety vs. non-safety profile category variables.

Keywords

organizational profiles, culture elements, value preferences, applied psychology

Absztrakt

A biztonsági kultúra fejlődésében változás, hogy a kockázatok elkerülése helyett, a megelőző, proaktív, új szemléletként pedig a pozitivista (jobbító biztonsági mechanizmusok maximalizálása) gondolkodás irányadó attitűddé válik. Szemléletváltás az is, hogy a vállalatok biztonságos belső működése mellett a szervezeten kívüli befolyásoló tényezők is egyre nagyobb hangsúlyt kapnak a normál működés megőrzése érdekében tett erőfeszítések során. A biztonság (Safety) és a védelem (Security) önálló tudományág és gazdasági szektor lett, azonban a biztonság kérdése a nem biztonsági profilú vállalatoknak és munkavállalóknak is komoly kihívást jelent. Kutatásom célkitűzése, hogy megvizsgáljam és elemezzem a Magyarországon működő vállalatok munkavállalóinak szervezeti biztonsággal kapcsolatos percepcióit, attitűdjeit, értékpreferenciáin alapuló motivációit és ezen keresztül azonosítsam az adott vállalatra jellemző biztonsági kultúra elemeket. Jelen tanulmányban a biztonsági, vs. a biztonsági profiltól eltérő kategória változók alapján mutatom be a legfontosabb különbségeket.

Kulcsszavak

vállalati profilok, kultúra elemek, értékpreferenciák, alkalmazott pszichológia

[1] kertai.kiss.ildiko@gmail.com | ORCID: 0000-0002-0981-2385 | PhD candidate, PhD School of Safety and Security Sciences, Óbuda University | PhD jelölt, Biztonságtudományi Doktori Iskola, Óbudai Egyetem

ELMÉLETI HÁTTÉR

A biztonsági kultúra koncepciója

A biztonsági kultúra fogalomkörében, a vállalatok szerepe és felelőssége különösen nagy, hiszen saját biztonságos működésükön túl, hatással vannak a fenntarthatóság minden aspektusára, többek között a társadalmi folyamatokra, a környezetvédelemre és a békére. Ezt az állapotot a vállalat rendeltetésszerű működését veszélyeztető tényezők hiánya, valamint a kockázatok minimalizálása érdekében alkalmazott védelmi erőforrások együttese határozza meg. [1] Ehhez pedig olyan szervezetekre van szükség, amelyekben prioritás, ugyanakkor érték is a biztonság.

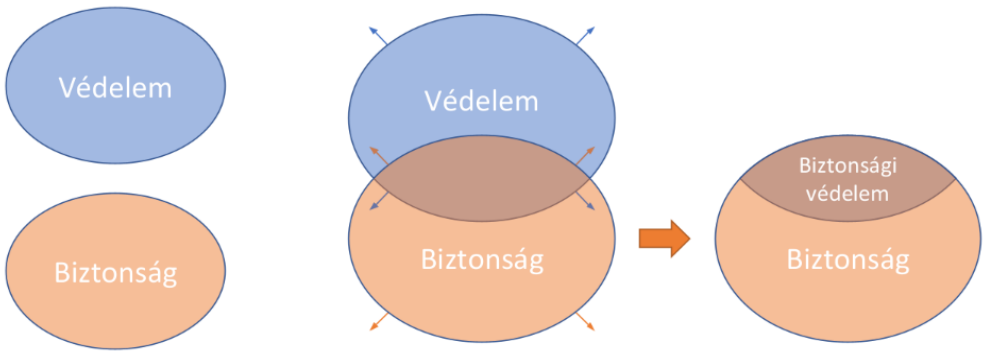
A biztonsági kultúra fogalma először az 1986-ban bekövetkezett csernobili katasztrófa okainak kivizsgálása során merült fel. A Nemzetközi Atomenergia Ügynökség Nemzetközi Nukleáris Biztonsági Tanácsadó Csoportjának szakértői elemezték a katasztrófát és arra a következtetésre jutottak, hogy az események nem tulajdoníthatók csak az emberi hibának, technológiának vagy a szocio-technikai rendszernek. Az azonosított ok egy sor szervezeti és irányítási tényező volt, amelyeket biztonsági kultúraként jelöltek meg [2]. A vizsgálatokból kiderült, hogy önmagában a technológiát, vagy kizárólag az emberi tevékenységeket már nem lehet úgy értelmezni, hogy képesek baleseteket előidézni, hanem ezekkel kölcsönhatásban a vállalati működés mélyrétegeit is figyelembe kell venni. (pl. értékpreferenciák, meggyőződések, hiedelmek, attitűdök, identitás stb.) Az első definíciót is ekkor fogalmazta meg a Nemzetközi Atomenergia Ügynökség (IAEA) nukleáris létesítmények biztonságával foglalkozó tanácsadó bizottság humán faktor munkacsoportja (ACSNI, Advisory Committee on the Safety of Nuclear Installations study group on human factors): *egy szervezet biztonsági kultúrája az egyén és a csoport értékek, attitűdök, felfogások, kompetenciák, viselkedési minták összessége, amelyek meghatározzák a szervezet egészsége és biztonsága iránti elkötelezettségét, stílusát és a menedzsment ebben való jártasságát.* [3] A vállalati biztonság kulturális megközelítése tehát kronológiailag a nukleáris iparhoz, ill. a nagykockázatú iparághoz kapcsolható, azonban ma már valamennyi ágazatban szerepe van, ezért kutatása elengedhetetlen.

A további biztonsági kultúra koncepciók nagyrészt azokból a szervezeti kultúra definíciókból származnak, amelyet a társadalom- és menedzsmenttudományban használnak. Antonsen [4] például úgy véli, hogy a biztonsági kultúra fogalmi címke, amely a kultúra és a biztonság közötti kapcsolatot jelöli. Egyes kutatások azt sugallják, hogy a biztonsági kultúra egy adott szervezeti kultúra kifejeződése, vagy megnyilvánulása, amely aztán egy biztonságirányítási rendszerben kristályosodik ki [5]. Mások kiemelik, hogy a biztonsági kultúra egyfajta szervezeti kultúra, amely szorosan összefügg a szervezeti kultúrával, azonban a biztonsági kultúrának saját identitása van. [6]

A különböző megközelítéseket összefoglalva, a legtöbb kutató a biztonsági kultúrát az adott szervezeti kultúrában, kifejezetten a biztonságra összpontosító szempontként határozza meg [7], más szerzők szerint alárendelt vagy másodlagos elem [8], illetve aldimenzió [9] vagy részhalmaz [10], amely a munkavállalói funkciókkal kapcsolatos egészségügyi és biztonsági faktorokra, jellemzőkre utal [11].

A legújabb korszak un. Safety II koncepciója mellett, melynek lényege, hogy míg a hagyományos biztonságirányítási technikák arra koncentrálnak, hogy megelőzzék a dol-

gok lehető legrosszabbra fordulását, az újabb megközelítés, a rendszer működését befolyásoló „jobbító" tényezők maximalizálását szorgalmazza [12], megjelenik egy másik nézőpont is. A vállalatok biztonságos belső működésén túl a szervezeten kívüli hatótényezők is nagyobb prioritást kapnak, ezért a biztonság és a védelem fogalmát a kutatók új, összetettebb megközelítési rendszerbe helyezték. Ennek értelmében a 21. század másik paradigma váltása, hogy a biztonságtudomány (Safety and Security Sciences) védelemmel foglalkozó ága (biztonságtechnika) a biztonságtudomány szerves részeként szintén nem hagyhatja figyelmen kívül a kulturális megközelítést, hiszen a biztonságos és védett működést elsősorban nem a beépített technológia határozza meg, hanem azok az egyének és a szervezeten belüli irányítási rendszerek, amelyeket az emberek hoznak létre. Az alábbi ábra ezt a folyamatot mutatja be.



a) Hagyományos megközelítés: védelem és biztonság elkülönülő területként

b) A védelem és biztonság területek növekedése és ebből eredő metszetük. A biztonság területén e metszet a biztonsági védelem alterületnek felel meg

1.ábra A biztonsági védelem bevonása a biztonságtudomány területére, in: N.H. Carreras Guzman et al. Safety Science 144 (2021) [13]

Biztonsági kultúra elemek

A szakirodalomban számos szerző, különböző modelleket javasol a biztonsági kultúra megragadására, fő jellemzőinek, mérhető indikátorainak bemutatására, azonosítva ezzel a biztonsági kultúra összetevőit. Kutatásomban az általam szerkesztett elmélet alapú kérdőívben szereplő kérdések (alapváltozók) a releváns szervezeti kultúra, valamint a biztonsági kultúra modelljeiből származtatott elemekből tevődnek össze. Ezek közül a biztonsági vs. a biztonságitól eltérő profilú vállalatok és munkavállalók esetében kinyert eredményekhez kapcsolódó modellek elemeit ismertetem.

McKinsey féle 7S modell

Ez a modell [14] a szervezeti kultúra elemeit két csoportba rendezi. A „kemény" elemek a szervezet szabályozási keretrendszeréhez tartoznak. Pl. stratégia, szervezeti struktúra, menedzsment eszközök, termelési rendszerek stb. Ezekben a dimenziókban a gazdasági haszonelvűség, hatékonyság, technológiai szükségszerűség és praktikum elvei érvényesülnek. Ezzel szemben a „lágy" elemek nehezebben ragadhatók meg és többnyire nem számszerűsíthetők, jelentőségük azonban ugyanolyan meghatározó a szervezeti kultúra ala-

kításában. Ide tartoznak például a képességek, munkaerő, (vezetési) stílus elemei, az alkalmazottak, vezetők képességei, explicit és implicit tudásai, képzettsége, ismeretei, valamint a szervezet értékrendje, normái. A biztonsági kultúra esetében a központi értékek: az elkötelezettség, a tudatosság és a „biztonság, mint érték" („safety first") szemlélet.

A modell alapján a biztonsági kultúra elemei hasonló analógia szerint oszthatók fel:

- *kemény elemek*: szabályozási keretrendszer, törvények, irányelvek, jogszabályok, szabványok, ellenőrzési stratégiák, biztonságirányítás, módszerek, menedzsment, stratégia, informatikai rendszerek, biztonsági szakrendszerek, minőségbiztosítási rendszerek stb.
- *lágy elemek*: szervezeti magatartást alakító tényezők, attitűdök, a biztonság tudatosságot elősegítő intervenciók, módszerek, oktatás, képzés, tréningek, „érzékenyítések", értékrend stb.

Westrum modell

Ez a koncepció azt a kérdést teszi fel, hogy a szervezetben ki, hogyan kezeli a biztonsággal kapcsolatos információkat és a felelősséget. Ennek megfelelően három típust határoz meg: (1) patologikus, (2) bürokratikus, (3) fejlődő kultúra. Például, hogy a biztonságra vonatkozó információkat aktívan keresik, (fejlődő) vagy inkább eltitkolják (patologikus), hogy hiba esetén a felelősség alól kibújnak (patologikus), vagy megosztják és tanulnak belőle (fejlődő), hogy az új elképzelések csak zavart okoznak, ezért szabályozzák (bürokratikus), vagy a biztonságos megoldásokkal kapcsolatos innovációkat bátorítják (fejlődő). Az összefoglaló táblázat a három kultúra típus jellemzőit mutatja be.

Hogyan kezelik a biztonsággal kapcsolatos információkat és a felelősség kérdését?		
Patologikus kultúra	***Bürokratikus kultúra***	***Fejlődő kultúra***
a biztonsági vonatkozású információkról tudni sem akarnak	a biztonsági vonatkozású információkat valószínűleg nem találják	a biztonsági vonatkozású információkat aktívan keresik
a biztonsági vonatkozású információk hírnökeire „lőnek"	a biztonsági vonatkozású információk hírnökeit, ha jönnek, meghallgatják	a biztonsági vonatkozású információk hírnökeit jutalmazzák
a felelősség alól kibújnak	a felelősséget kategóriákba sorolják	a felelősséget megosztják
a kudarcot büntetik vagy eltitkolják	a kudarcok kisléptékű helyi korrekciókat eredményeznek	a kudarcok messze ható, átfogó reformokat eredmé-

Hogyan kezelik a biztonsággal kapcsolatos információkat és a felelősség kérdését?		
Patologikus kultúra	***Bürokratikus kultúra***	***Fejlődő kultúra***
az új elképzeléseket rosszallással fogadják és ellenzik	az új elképzelések gyakran zavart okoznak.	az új elképzeléseket üdvözlik és bátorítják
a felelősség alól kibújnak	csak a szűken vett, formálisan előírt felelősséget vállalják	a felelősséget megosztják és elkötelezetten vállalják

1.Táblázat: Biztonsági kultúra jellemzőinek csoportosítása (Westrum, 1992) [15]

Reason modell

Reason [16] meghatározása szerint a biztonsági kultúrát a "krónikus nyugtalanság" és a lehetséges egészségügyi és biztonsági veszélyekkel kapcsolatos tudatosság, valamint éberség fenntartása jellemzi. A biztonsági kultúra elméleti hátterének egyik legmeghatározóbb modellje, amely négy szorosan összefüggő elem együttes meglétét emeli ki a hatékony szervezeti biztonság eléréséhez. Az elemek a következők: (1) jelentő kultúra (reporting), (2) igazságos kultúra (just), (3) alkalmazkodó kultúra (flexible), (4) tanulni képes kultúra (learning).

1. A jelentő kultúra abban áll, hogy a kisebb meghibásodásokat és a "majdnem eseményeket" (near misses) a működőképes biztonsági kultúrával rendelkező szervezetek olyan szimptómának tekintik, melyeket a komolyabb események elkerülésére lehet felhasználni. Ennek megfelelően fontos, hogy az összes „tanulságos" eset jelentése és kivizsgálása, valamint értékelése megtörténjen. Más szóval ez a *„Ne söpörd a szőnyeg alá!"* kultúra, amelyhez elengedhetetlen a bizalmi légkör, az elfogadó magatartás, a jóhiszeműség, a retorzióktól való félelemmentes kommunikáció és a konstruktivitás, valamint a *„fontosabb, hogy tudjunk róla, mint, hogy büntessük"* szemlélet érvényesülése.
2. Az igazságos kultúra azt jelenti, hogy a biztonsági aggályok és problémák jelentése nyitott és bátorított [17]. Ez magában foglalja, hogy a vezető „meghallja a rossz hírt", a problémákról szóló jelentéseket és a megoldás elősegítése érdekében jutalmazza, így a szervezet tagjai felhatalmazást kapnak arra, hogy segítsenek beavatkozni, megváltoztatni és javítani a biztonsági problémákat [18]. Az igazságos kultúra elfogadja és elismeri, hogy nem szándékos emberi hibák be fognak bekövetkezni [19], ezért olyan kultúra kialakítására van szükség, amelyben a munkát nem büntető környezetben végzik és az információk nyilvánosságra hozatala nem lesz negatív hatással a munkavállalók előmenetelére, vagy karrierkilátásaira. Az igazsá-

gos kultúra magában foglalja, hogy a problémákról szóló jelentéseket a vezetés jutalmazza és a szervezet minden tagja felhatalmazást kap arra, hogy segítsenek beavatkozni, megváltoztatni és javítani a kialakult problémát. Ahhoz, hogy ez működjön, magas szintű bizalomra és átláthatóságra van szükség: a munkavállalók tevékenységüket "*nem büntető jellegű környezetben végzik*", tudatában vannak annak, hogy az információk közzététele nem lesz negatív hatással karrierjükre, munkalehetőségeikre, vagy nem jelenti azt, hogy „hűtlenek lesznek a kollégákhoz, főnökükhöz, szervezetükhöz" [20], valamint létezik egy bizalmas jelentési rendszer, amely nemcsak lehetővé teszi, hanem ösztönzi a szervezet valamennyi tagját a hibák, vagy biztonságot veszélyeztető jelenségek feltárására. Az ilyen kultúra jellemzői a méltányosság, az elfogadó magatartás, a hibáztatás mentes kivizsgálás. Empirikus vizsgálataim igazolták, hogy a biztonsági vezetők tudatában vannak az igazságos kultúra hiányából fakadó kockázatoknak, amikor azt mondják, hogy Magyarországon a társadalmi beágyazottság akadályozza a just kultúra működését, beépülését a szervezeti (biztonsági) kultúrába, mert túl nagy a „hierarchia gradiens" (ld. hatalmi távolság index), aminek következménye a *„nem merünk szólni"* szemlélet. A biztonsági területek vezetői elkötelezettsége meghatározó, de önmagában nem elég. Ahhoz, hogy az igazságos kultúra működjön, ki kell alakítani egy deklarált szervezeti biztonság politikát és biztosítani az anonim bejelentés lehetőségét, alapszemlélet kell legyen, hogy *„rendszerhibát keresünk és nem embert".* A primer kutatás többek között azt is bizonyította, hogy mind a rendszerszemlélet, mind a hibakultúra területén a magyar vállalatoknak még sokat kell fejlődniük.

3. A rugalmas kultúra a szervezeten belüli döntéshozatal merevségének a hiánya, valamint az, hogy egyre nagyobb szükség van a termelés nyomására adott válaszának felülvizsgálatára a fokozott biztonság érdekében. A különböző szervezeti és egyéni szinten születő, a biztonság elsődlegességét szem előtt tartó döntések szabadságfoka a rendszer alkalmazkodóképességének mutatójaként is felfogható. [21] Ezenkívül a tartalékos erőforrások, például az anyagok, a tervezés orientált erőforrások, vagy az emberek reagálásához szükséges további idők rendelkezésre állása lehetővé teszi a szervezet számára, hogy megbirkózzon az előre nem látható problémákkal, gyorsan reagáljon, ha ismeretlen zavarok fordulnak elő [22]. A rugalmas ellenálló képesség (reziliencia) lehetővé teszi a szervezet számára, hogy megbirkózzon az előre nem látható problémákkal, illetve gyorsan reagáljon a zavarokra, valamint, hogy a normák és szabályok maguk is lehetővé tegyék a rugalmas megközelítést és a döntéshozatal decentralizált megvalósulását. Ennek alapja, hogy a felső vezetés a biztonságot tekinti a szervezet alapvető értékének, amely mellett elköteleződik. Az elkötelezettség a vezetés tartós és pozitív hozzáállásában tükröződik a kommunikáció és a gyakorlat szintjén: (a) következetesen hangsúlyozzák a biztonság fontosságát, (b) a biztonság előnyben részesítése a termeléssel szemben minden helyzetben, (c) megfelelő források biztosítása a biztonsági előírások, tevékenységek megvalósítására, (d) a biztonság aktív előmozdítása a szervezeten belül minden szinten.
4. A tanuló kultúra azzal a kérdéssel foglalkozik, hogy egy szervezet tagadással, javítással vagy valódi reformmal reagál-e a váratlan, nem kívánatos eseményekre, illetve hogyan kezeli és oldja meg a biztonsági problémákat. Fontos továbbá, hogy *a szervezet „ne pihenjen a babérjain"* és hogy a múltbeli sikereket ne tekintsék a

jövőbeli sikerek garanciájának [18]. A biztonsággal kapcsolatos jelenségeknek az egész szervezetben jelzésértékűnek kell lennie, az incidensekből és más eseményekből levont tanulságokat komolyan kell kezelni, és visszajelzést adni a szervezet minden szintjén. Biztosítani kell azt is, hogy a biztonságról és a kockázatokról szóló megbeszélések továbbra is megtörténjenek, akkor is, ha nem tapasztalnak például balesetet. Emellett az is kiemelt szempont, hogy az egyes szervezeti biztonsági szubkultúrák jó, ha különböznek egymástól, mert a túlzott homogenitás kedvezőtlenül hathat a szervezeti tanulásra. ami azt jelenti, hogy minden részegységnek fel kell ismernie a saját szerepét abban, hogy miként tud hozzájárulni a biztonsághoz mindezt oly módon, hogy megfelelően lép kölcsönhatásba a többi résztvevővel.

Schwartz-féle érték dimenziók modell

Schwartz elgondolása alapján a különböző értékdimenziók két nagyobb értéktengely mentén tíz értékosztályba rendeződnek. [23] Az elmélet lényege, hogy a validált értékteszt segítségével meghatározhatók és sorrendbe állíthatók az emberek értékpreferenciái és ezeknek az aggregálásával a különböző kultúrák értékrendszerei leírhatók és összehasonlíthatók. A 10 univerzális érték a biztonsági kultúra kapcsán is releváns: (1) hatalom, (önmegvalósítás), (2) teljesítmény, (önmegvalósítás), (3) jóakarat, altruizmus (önmeghaladás), (4) univerzalizmus, (önmeghaladás), (5) konformitás, (konzerválás), (6) hagyomány, (konzerválás), (7) biztonság, (konzerválás), (8) önállóság, (nyitottság a változásra), (9) stimuláció, kockázatvállalás, (nyitottság a változásra), (10) hedonizmus.

PRIMER KUTATÁS

A kutatásban résztvevő szervezetek

A biztonsági kultúra felméréssel kapcsolatban 41 szervezetet kerestem meg, (szektorok: biztonsági, védelmi, szolgáltatás, energia, közlekedés, IT, tanácsadó, kereskedelmi, infokommunikációs, gyógyszeripar, vegyipar). Kérdőíves adatfelvételt 8 vállalatnál készítettem, (biztonsági, védelmi, szolgáltatás, kereskedelem, közlekedés, energia szektor, nukleáris ipar). A kérdőívet összesen 301 munkavállaló töltötte ki, ebből 280 volt értékelhető. A megkérdezettek célzottan, szakértői mintavételi eljárás alapján vettek részt a kutatásban.

Biztonsági kultúra kutatásom komplex szemléletű megközelítés (kvantitatív, kvalitatív, interszubjektív), a szervezeti kultúra biztonság fókuszú vizsgálata. Ebből jelen kutatásban a kvantitatív szakasz biztonsági, vs. biztonságitól különböző területen dolgozók összehasonlításának eredményeit ismertetem.

Kutatási kérdőív

Kutató munkám során, egy 45 itemből álló saját szerkesztésű kérdőívet dolgoztam ki, amely a biztonsággal kapcsolatos attitűdöket, motivációkat, értékrendeket, valamint a biztonsági kultúra modellekben megfogalmazott elemeket, tulajdonságokat tartalmazza. Mérőeszközöm a munkavállalók által észlelt szervezeti valóságra kérdez rá, valamint a szervezeti magatartást veszi alapul. A válaszadók 7 fokú ordinális skála segítségével dönthették el, hogy a kérdőív kijelentései mennyire jellemzőek a vállalati és saját működésükre. Az adatok feldolgozását, statisztikai elemzését IBM SPSS Statistics 20 software alkalmazásával végeztem.

A minta jellemzői

Az értékelhető kérdőívek (N=280) 70,4%-át nagyvállalatok munkavállalói (64,6% állami) 197-en töltötték ki, a többi résztvevő (83 munkavállaló) a KKV szektorban dolgozik, ebből 41,1% (N=113) vezető, 57,9% (N=162) nem vezetői feladatokat lát el. (Öt kérdőívben nem volt értékelhető az erre a kérdésre adott válasz.) A megkérdezett vállalatokra jellemző, hogy 85,4% magyar, 14,6% német tulajdonosi háttérrel rendelkezik. A kitöltők demográfiai megoszlása: legnagyobb arányban (63,8%) az X generáció, ezt követően csökkenő sorrendben 30,1% az y generáció, 5,1% baby boomer, 1,1% pedig Z generációhoz tartozik. A vizsgálatban részt vettek 91,1%-a a biztonság területén dolgozik, 8,9%-ban pedig a demográfiai kérdésre nem biztonsággal kapcsolatos szakmai területet jelöltek meg. Az összehasonlító vizsgálatok többek között arra a kérdésre keresték a választ, hogy van-e szignifikáns különbség a hazai biztonsági, illetve a biztonsági profiltól különböző munkavállalók biztonsági kultúra jellemzői között és ha van, mely elemek térnek el leginkább.

ÖSSZEFÜGGÉS VIZSGÁLAT T-PRÓBÁVAL

Kategória változók a vállalati profil alapján: biztonsági, vs. biztonságitól különböző

A statisztikai elemzések során megvizsgáltam, hogy milyen változók esetén van szignifikáns különbség az általam meghatározott alcsoportok között. Az elemzéshez a következő kategória változókat vizsgáltam:

(1) Tulajdonosi háttér: magyar / német, (2) Vállalati méret: KKV / nagyvállalat (3) Tulajdonos: privát / állami, (4) Hierarchia: vezető / beosztott (5) Vállalati biztonsági terület: biztonsági / biztonságitól különböző.

Jelen cikkben a „biztonsági, vs. a biztonságitól különböző” kategória változók alapján kinyert eredményeket ismertetem, amelyet az alábbi táblázatok foglalnak össze.

	Biztonsági (n=255)		Biztonságitól különböző (n=25)		Eltérés szignifikancia szintje
	átlag	szórás	átlag	szórás	
Ön ismeri a Szervezet biztonságpolitikáját.	4,21	1,725	3,32	1,749	**0,015****
A biztonsággal kapcsolatos utasítások, standardok, dokumentumok megfelelőek és naprakészen érvényesek.	4,34	1,416	3,16	1,650	**0****
A biztonság a standardoktól és a szabályozási rendszertől függ.	4,09	1,405	3,40	1,826	0,076
Kellő mértékben költ a Szervezet a biztonság növelésére.	4,08	1,345	2,76	1,665	**0****
Az Ön számára elsődlegesen fontos, hogy sok pénzt keressen a Vállalatnál.	4,29	1,237	4,08	,909	0,4
A biztonság érték.	5,29	,982	4,68	1,520	0,058
Fontosnak tarja, hogy biztonságos körülmények között dolgozzon.	5,52	,778	5,48	,823	0,8
A biztonsági standardok, előírások és a Szervezetben alkalmazott technológia összhangban vannak.	4,15	1,255	3,36	1,630	**0,004****

	Biztonsági (n=255)		Biztonságitól különböző (n=25)		Eltérés szignifikancia szintje
	átlag	szórás	átlag	szórás	
A hibázás hátterében szervezeti folyamatproblémák állnak.	3,39	1,403	3,56	1,502	0,557
A munkahelyi körülmények hozzájárulnak a hibázáshoz.	3,61	1,563	3,36	1,630	0,452
Vezetői időnként tudatosítják Önben a Szervezet biztonságpolitikáját.	4,11	1,610	2,64	1,777	**0****
Ön alkalmazza a Szervezet biztonságpolitikájában meghatározott irányelveket a napi munkája során.	4,60	1,424	3,76	1,739	**0,006****
A biztonságra vonatkozó előírásokat számonkérik a Szervezetben.	4,18	1,633	2,92	1,801	**0****
A biztonsági képzés hozzájárul a Szervezet biztonsági céljainak. eléréséhez	4,68	1,321	3,60	1,936	**0,011****
A biztonságért mindenki felelős.	5,45	,933	4,36	1,997	**0,012****
Kockázat, „biztonsági rés”, ha a Szervezet nem képes tanulni a hibázásból.	5,35	,966	4,76	1,451	0,056
A nem megfelelően felkészített munkavállaló hozzájárul a hibázáshoz.	5,40	,845	5,32	1,108	0,646
A vállalati biztonsági szabályokat, alkalmazásokat meg lehet tanulni, de a bizonytalan, váratlan szituációk megoldásához nem mindig állnak rendelkezésre kész útmutatások.	4,38	1,383	4,48	1,388	0,732
A szervezet minden szintjén aktívan keresik a biztonságos működéshez szükséges megoldásokat.	4,07	1,386	2,92	1,605	**0****
Elvárják Öntől, hogy a szabályokat „vakon” tartsa be.	3,74	1,562	3,56	1,828	0,597

2.Táblázat A „biztonsági és a biztonságitól különböző” kategóriák esetén (1-20 alapváltozóval), a két csillaggal jelölt értékek a biztonsági profilú munkavállalókra jellemző szignifikánsan nagyobb értékeket mutatják

	Biztonsági (n=255)		Biztonságitól különböző (n=25)		Eltérés szignifikancia szintje
	átlag	szórás	átlag	szórás	
Ön a biztonsággal tudatosan foglalkozik.	4,47	1,419	3,68	1,909	0,054
Jellemző Önre, hogy törődik mások biztonságával.	5,20	,948	5,44	,917	0,219
Komoly meggyőződése, hogy az embereknek óvniuk kell a környezetüket. A környezeti kockázatok megelőzése elsőbbséget élvez.	5,21	1,009	5,20	1,000	0,956
Az Ön környezetében dolgozók akkor is betartják a biztonsági eljárásokat, ha a felettesük nem tudja ellenőrizni.	4,39	1,229	3,64	1,705	**0,042****

	Biztonsági (n=255)		Biztonságitól különböző (n=25)		Eltérés szignifikancia szintje
	átlag	szórás	átlag	szórás	
Fokozza a kockázatot, ha a hibázások kezelése nem igazságos.	4,91	1,171	4,60	1,581	0,218
Az egyes személyiség jellemzők, tulajdonságok befolyásolják a biztonságot.	4,72	1,136	4,56	1,387	0,517
Befolyásolja az egyén nem megfelelő motivációja és felkészültsége az emberi hibázást.	5,15	1,049	4,92	,997	0,305
Fontos Önnek, hogy szerény és visszafogott legyen. Megpróbál úgy dolgozni, hogy ne vonja magára mások figyelmét a biztonság megteremtésében.	4,12	1,473	3,56	1,873	0,157
Fontos Önnek, hogy tiszteljék mások. Azt akarja, hogy azt csinálják, amit mond, amikor a helyzet bizonytalan	4,23	1,335	4,36	1,524	0,643
Fontos Önnek, hogy új megoldásokat találjon ki, amikor egy biztonsági problémával találkozik.	4,38	1,422	4,60	1,258	0,45
Fontos, hogy jól érezze magát, még akkor is, ha ezzel bizonytalanságot. teremthet.	2,52	1,622	2,04	1,881	0,166
Ön dönthet önállóan a biztonság kapcsán felmerülő problémák megoldásában.	2,43	1,788	2,40	1,958	0,942
Keresi a kalandokat és szeret kockázatot vállalni.	2,19	1,676	1,96	1,767	0,524
Fontos Önnek, hogy megmutassa képességeit a biztonsággal kapcsolatos szervezeti kérdések megoldásában.	3,68	1,597	3,20	1,708	0,158
Veszély esetén minden feltétel (emberi, technikai) rendelkezésére áll a hiba elhárítására.	4,05	1,425	3,12	1,509	**0,002****
Jellemző, hogy egy biztonsági probléma megoldásához segítséget kap.	4,37	1,463	4,00	1,658	0,231
A menedzsment elkötelezett és mindent megtesz a biztonság érdekében.	4,43	1,453	4,00	1,633	0,162
Növelik a kockázatokat a szervezeten belüli hatalmi különbségek.	3,53	1,753	3,68	1,952	0,682
Az Ön Szervezetében a biztonsággal kapcsolatos információkat megosztják.	4,28	1,561	3,16	1,886	**0,001****
Ön szerint jellemző a szervezeti tagok együttműködése a hibák megelőzésében	4,41	1,333	3,60	1,658	**0,005****
Kockázatos szituációkban inkább másoknak segít.	5,10	,971	4,88	1,201	0,295
Fontosnak tartja, hogy minden munkavállaló egyenlő bánásmódban részesüljön, ha biztonságról van szó.	5,47	,868	5,48	,714	0,941
A nem kívánatos biztonsági események őszinte feltárását jutalmazzák, a Szervezet javadalmazási rendszerébe beépül a biztonsági események megfelelő kezelése.	3,01	1,838	1,80	1,732	**0,002****

	Biztonsági (n=255)		Biztonságitól különböző (n=25)		Eltérés szignifikancia szintje
	átlag	szórás	átlag	szórás	
A Szervezeten kívüli tényezők (társadalmi, gazdasági, politikai, sajtó, közvélemény, hatóságok stb.) erősen befolyásolják a biztonságot.	3,69	1,561	2,88	1,965	0,056
Befolyásolja a kockázatokat, ha a Szervezet rugalmas és képes alkalmazkodni a külső és belső környezethez.	4,41	1,554	3,92	1,778	0,137

3.Táblázat A „biztonsági és a biztonságitól különböző" kategóriák esetén (21-45 alapváltozóval), a két csillaggal jelölt értékek a biztonsági profilú munkavállalókra jellemző szignifikánsan nagyobb értékeket mutatják

A kérdések alapján, a szervezeti terület *„biztonsági" kategóriájába* tartozó munkavállalók esetében a szignifikánsan nagyobb értékű elemek a következők: a biztonság érték, amelyért mindenki felelős, ezzel összefüggésben a szervezet minden szintjén aktívan keresik a működéséhez szükséges megoldásokat. A kutatás szintén kvantitatív szakaszában vizsgált állami vállalatokhoz hasonlóan a biztonsági területen dolgozók percepciói a biztonság vonatkozásában az un. erős kultúrával [24] rendelkező vállalatok jellemzőit mutatják, ami egyrészt azt jelenti, hogy (1) a munkavállalók akkor is betartják az előírásokat, ha a felettesük nem tudja ellenőrizni (konformitás), (2) a nem kívánatos biztonsági események őszinte feltárását jutalmazzák (igazságos kultúra), (3) az információkat megosztják (tanuló kultúra), (4) együttműködnek a hibák megelőzésében (kooperáció), (5) valamint a célok eléréséhez fontos a képzés és az előírások számonkérése is (tanuló kultúra). A lágy elemek mellett a biztonságos szervezeti működés kemény elemei közül a következők mutatnak szignifikánsan nagyobb értéket: (1) a biztonságpolitika ismerete és tudatosítása, illetve alkalmazása a napi munka során, (2) a standardok, dokumentumok naprakész érvényessége, (3) a költségek biztosítása a biztonság növelése érdekében, valamint (4) a biztonságos munkakörülmények. Mindezek lehetővé teszik, hogy veszély esetén mind a technikai, mind az emberi feltétel rendelkezésre álljon a hiba elhárítására, vagy megelőzésére. Ezek az elemek azt mutatják, hogy a biztonsági területen dolgozók, annak ellenére, hogy vállalatuk nem a biztonsági / védelmi, vagy nagykockázatú iparágakban tevékenykedik, de fókuszterület a biztonság (ld. közlekedés) az erős kultúra jellemzőit érzékelik, amely magában foglalja a konzisztencia, konszenzus és egyértelműség fogalmát, amelyek stabilitást teremtenek azáltal, hogy a struktúra, szervezeti folyamatok, vezetői szerepek, hatalmi viszonyok belső ellentmondásoktól menetesen működjenek a szervezetben.

A t-próbák további eredménye, hogy nemcsak az „állami vállalatok", hanem a „vezetők" kategória változók esetében vannak közös pontok a biztonsági kutúra elemei kapcsán, hanem a biztonsági területen is, azonban a biztonsági területen dolgozók attitűdjében kevéssé jellemzőek az altruizmus, univerzalizmus, önmegvalósítás érték dimenziók. Ide sorolhatók például, hogy míg a vezetők jellemzően nyitottak a változásra, tehát lényegesnek gondolják, hogy új biztonsági megoldásokat találjanak ki (önállóság), valamint, hogy megmutassák képességeiket a biztonsággal kapcsolatos szervezeti problémák megoldásában

(stimuláció), addig ez az attitűd szignifikánsan kisebb értéket mutat a biztonsági területen dolgozók magatartásában. Másrészről a vezetők a biztonság érdekében, fontosnak tarják az önmagán túlmutató vállalati célokat is: a társadalmi felelősség vállalást, ezen belül a környezet védelmét, amivel kapcsolatban szignifikánsan nagyobb értékek nem jelentek meg a biztonság területén dolgozók működésében. Az, hogy a vállalati biztonság területén dolgozók erős biztonsági kultúrát érzékelnek nem meglepő, hiszen a szervezeti profil és a munkakörük jellegéből logikusan következik, azonban további kérdéseket vet fel, hogy a nem biztonsági terület munkavállalói hogyan tudják működőképessé tenni a biztonság érdekében az olyan alapvető kultúra elemeket, mint például az információ megosztás (tanuló), a hibák megelőzésében a kooperáció képessége, vagy az igazságos kultúra. Jelen kutatás eredményei egyéni és szervezeti szinten is értelmezhetőek, hiszen azok a munkavállalók, akik nem biztonsági területen dolgoznak, olyan vállalathoz tartoznak, amelyben nem fókusz terület a biztonság, szemben a többi résztvevővel, azonban ez a kérdés mélyebb elemzést igényel. A kutatás eredménye rávilágít a biztonsági kultúra egyik sajátos jellemzőjére, az un. „foltosság" kérdésére is („patchiness' of organisational safety cultures"), amely szorosan kapcsolódik az egyenszilárdság problémájához. Ez azt jelenti, hogy a biztonsági kultúra nem fejlődik ugyanolyan ütemben minden szervezetben. Sőt bizonyos szervezeti egységek, még egyetlen szervezeten belül is eltérő ütemben fejleszthetik biztonsági kultúrájukat, mint mások. Ennek magyarázata többek között az, hogy a biztonsági kultúra javítására irányuló intézkedések egyes részterületeken hatékonyabbak lehetnek. Azonban, ha a szervezetek nem alakítanak ki egységes biztonsági kultúrát, az konfliktushoz vezet [25], mert a szervezet különböző szintjein eltérő értelmezések, percepciók lehetségesek a biztonság vonatkozásában, ami akadályozhatja a biztonsághoz szükséges erős kultúra stabilitását.

ÖSSZEFOGLALÁS

Kutatásom alkalmazott kutatás, amelynek fő célja az új ismeretek gyakorlati felhasználása. A biztonsági kultúra témakörét releváns tudományterületek összekapcsolásával vizsgáltam: alkalmazott pszichológia, szociológia, szociálpszichológia, közgazdaságtan, vezetés –és szervezés tudomány. Az elmélet alapú kérdőív változóinak szignifikáns különbségeit statisztikai módszerrel elemeztem (t-próbák), több kategória változóra, ebből jelen tanulmányban a biztonsági, vs. biztonságitól különböző területen dolgozók alcsoportjainak fő jellemzőit mutattam be. Ennek alapján összességében megállapítható, hogy a jelen vizsgálatban részt vett, Magyarországon működő biztonsági területen dolgozók és a biztonsági területtől eltérő munkavállalók vállalati kultúra jellemzői, percepciói jelentősen különböznek egymástól. Míg a biztonsági területen tevékenykedők esetében nagy hangsúlyt kap a fejlődő (információ megosztás), bürokratikus (standardok, irányelvek, szabályzatok), jelentő, igazságos (retorziómentes, jutalmazó hibajelentés), tanuló kultúra (hibákból való szervezeti szintű tanulás) kultúra elemek, addig a biztonsági profiltól eltérő munkakörben dolgozóknál ezek az összetevők kevésbé jellemzőek, ezért a jövőben érdemes nagyobb hangsúlyt fektetni például a vállalati biztonságpolitika irányelveinek tudatosítására, alkalmazására, a naprakész dokumentumok érvényességére, vagy a hibákból való tanulás képességére egyéni és szervezeti szinten. Ehhez jól működő jelentő és igazságos kultúrára van szükség, melynek alapja a bizalom. Az eredmény felhívja a figyelmet arra is, hogy a biztonsági terület munkavállalói számára is van még tennivaló, például az innovatív megoldá-

sok megkeresése a biztonsági problémák megoldásában, vagy egyes esetekben a környezetvédelem, valamint az egyenszilárdság kérdésében. Az eredmények alapján további vizsgálatokat igényel az erős kultúrát meghatározó faktorok mélyebb vizsgálata is, abból a szempontból, hogy a munkavállalók mennyire azonosulnak a közös, konszenzuson alapuló értékrenddel [26], amely befolyásolja gondolkodásukat, cselekvésüket és vajon mennyire elkötelezettek a biztonság mellett.

FELHASZNÁLT IRODALOM

[1] Berek, L. et al., SZEMÉLY-ÉS VAGYONBIZTONSÁG, ÓE-BGK 3071, Budapest, 2016, ISBN 978-615-5460-94-4
[2] NAÜ, 75-INSAG-1, 1986
[3] Great Britain Health and Safety Commission, ACSNI Human Factors Study Group. Third report. Organising for safety, H.M.S.O., London, 1993
[4] Antonsen, S., Safety Culture Theory, Method and Improvement, Ashgate, 2009
[5] Guldenmund, The nature of safety culture: a review of theory and research Safety Science, 2000 február, Volume 34, Issues 1-3
[6] Díaz-Cabrera, et al., An evaluation of a new instrument to measure organisational safety culture values and practices, Accident Analysis and Prevention 2007, november Volume 39, Issue 6
[7] Richter, A and Koch, C, Integration, differentiation and ambiguity in safety cultures, 2004. *Safety Science*, (42)
[8] Kennedy, Kirwan, B., Development of a Hazard and Operability-based method for identifying safety management vulnerabilities in high risk systems, Safety Science, Volume 30, Issue 3, 1998, December
[9] Cooper, M D, Towards a model of safety culture, 2000, *Safety Science*, (36)
[10] Reiman, T., Rollenhagen, C, Safety Culture, in: Handbook of Safety Principles, Book, 2017, Editor(s): Niklas Moller, Sven Ove Hansson, Jan-Erik Holmberg, Carl Rollenhagen,
[11] López de Castro, Gracia, Peiró, Pietrantoni, Hernánde, Testing the validity of the International Atomic Energy Agency (IAEA) safety culture model, Accident Analysis and Prevention, 2013, November, Volume 60
[12] Hollnagel, E., Safety-I and safety–II: the past and future of safety management. 2014. London; Ashgate Publishing, Ltd.
[13] N.H. Guzman et al., An integrated safety and security analysis for cyber-physical harm scenarios, *Safety Science* 144, 2021
[14] Peters, T. J., Waterman, R. H. Jr. In search of excellence: lessons from America's best run companies. 1982, New York: Harper & Row
[15] Westrum, R., A typology of organisational cultures, 2004, Qual Saf Health Care. 13.
[16] Reason, J., Managing the Risks of Organizational Accidents, 1997, Ashgate Publishing: Aldershot
[17] Wreathall, J., Properties of resilient organizations: An initial view, *Resilience Engineering: Concepts and Precepts*, 2006, eds: E Hollnagel, S W A Dekker and N Leveson, Ashgate Publishing: Aldershot

[18] Dekker, S W A, Resilience engineering: Chronicling the emergence of confused consensus, Resilience Engineering: Concepts and Precepts, 2006, (eds: E Hollnagel, D D Woods and N Leveson), Ashgate Publishing: Aldershot
[19] Horvath, D., Klamar , A., Keith, N., Frese, M., Are all errors created equal? Testing the effect of error characteristics on learning from errors in three countries, European Journal of Work and Organizational Psychology, 2020
[20] Whittingham, R. B., Preventing Corporate Accidents: An Ethical Approach, Elsevier: Burlington, 2008
[21] Woods, D D and Hollnagel, E., Prologue: Resilience engineering concepts, *Resilience Engineering: Concepts and, Precepts*, 2006, (eds: E Hollnagel, D D Woods and N Leveson), Ashgate Publishing: Aldershot
[22]Wreathall, J. Properties of resilient organizations: An initial view, Resilience Engineering: Concepts and Precepts, 2006, eds: E Hollnagel, S W A Dekker and N Leveson, Ashgate Publishing: Aldershot
[23] Schwartz, S.H., Universals in the Content and Structure of Values: Theoretical Advances and Empirical Tests in 20 Countries December 1992, Advances in Experimental Social Psychology, In book: Advances in Experimental Social Psychology Volume 25, Academic Press
[24] Schein, E. H., Organizational Culture and Leadership (Vol. 2). 2010., San Francisco, CA: John Wiley & Sons.
[25] Richter, A. & Koch, C., Integration, differentiation and ambiguity in safety cultures. Safety Science, 2004, 42(8),
[26] Lazányi, K., Mire jó a biztonsági kultúra? TAYLOR. Gazdálkodás- és szervezéstudományi folyóirat. A Virtuális Intézet Közép-Európa Kutatására Közleményei, 2015, Szeged

STUDY OF CHEMICAL ACCIDENT IN LIGHT OF HAZARD ZONE CREATING

VEGYI HAVÁRIÁK VIZSGÁLATA A KÁRTERÜLET KIALAKULÁSÁNAK TÜKRÉBEN

NAGY Rudolf [1]

Abstract

The use of chemicals is found in all aspects of life. Chemical safety, as an interdisciplinary element of environmental safety, is particularly important in ensuring the safety of activities involving chemicals.
However, the risks posed by the application and use of chemicals are not the same in all spheres of application. One need only think of hazardous plants, where the increase in the associated technological scale and volumes leads to changes in safety levels. Moreover, other dangerous technical parameters associated with the operation of the plant, such as overpressure, high temperatures, etc., also have a significant influence on safety. These non-conformities can be the cause of accidents on a local or even regional scale, which can lead to damage areas of varying scale, not only geographically but also in terms of risk. The effects of the factors behind these possible differences are important criteria for the way in which the assessment of the situation and the response to chemical accidents should be carried out.

Keywords

chemicals, hazard zone, safety, pollution, impact

Absztrakt

A vegyi anyagok felhasználása az élet minden területén megtalálhatók. Az ezekkel folytatott tevékenységek biztonságának megőrzésében különösen fontos szerepet tölt be a kémiai biztonság, mint környezetbiztonság egyik interdiszciplináris eleme.
A vegyi anyagok alkalmazása, felhasználása teremtette kockázatok azonban a felhasználási területek nem minden szférájában tekinthetők azonosnak. Elegendő csak a veszélyes üzemekre gondolnunk, ahol a kapcsolódó technológiai méretek és mennyiségek növekedése a biztonsági szintek változását eredményezi. Sőt az üzemvitelhez társuló olyan egyéb veszélyes műszaki paraméterek, mint a túlnyomás, magas hőmérsékletek stb. is jelentős befolyással vannak az üzembiztonságra. Az itt mutatkozható nemmegfelelőségek lokálisan, de akár regionális méretű balesetek kiváltói is lehetnek, melyek ezen körülményekkel arányban nem csak földrajzi értelemben, de kockázatok szintjén is eltérő léptékű kárterületek létrejöttét eredményezhetik. A lehetséges eltérések mögött meghúzódó tényezők keltette hatások fontos kritériumai a vegyi balesetek nyomán végzendő helyzetértékelés és kárelhárítás miként jének.

Kulcsszavak

vegyi anyag, kárterület, biztonság, szennyezés, hatás

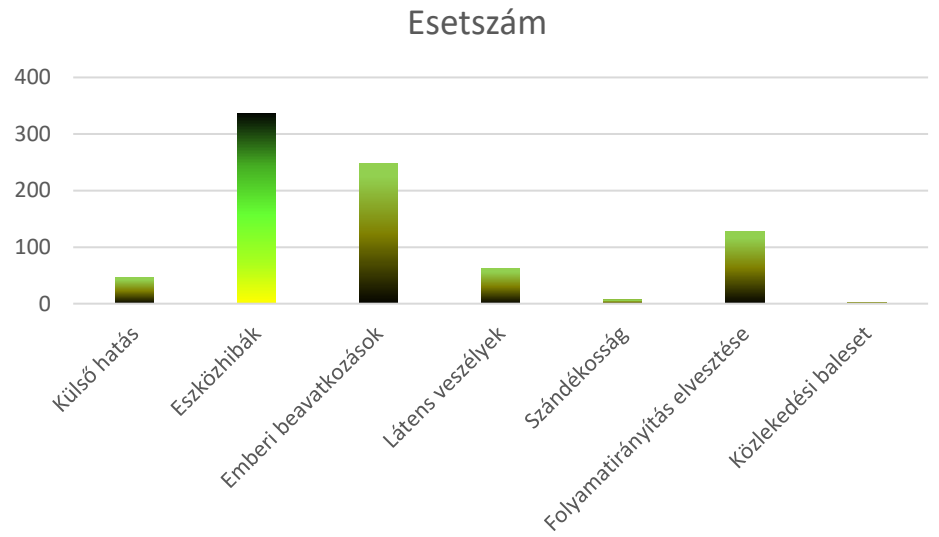
[1] nagy.rudolf@uni-obuda.hu | ORCID: 0000-0001-5108-9728 | habil. senior lecturer, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary | habil. adjunktus, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A kemizáció következtében széles körben elterjedt vegyi anyagok többsége kémiai, fizikai és élettani hatásaik révén potenciális veszélyforrásként azonosíthatók. Veszélyes tulajdonságaik sokasága magában hordozza az egészséget, környezetet fenyegető balesetek lehetőségét. Kritikus, nagy volumenű ellenőrizetlen szabadba jutásuk katasztrofális eseményeket előidézni képes súlyos ipari balesetekké szélesedhetnek.

A súlyos ipari balesetek a veszélyes anyagok ipari felhasználásához köthetők főként, azonban a vegyi anyagok okozta katasztrófák a veszélyesáru szállítással érintett közlekedési rendszerek területén is bekövetkezhetnek. Tehát a lakosságot és a környezetet fenyegető vegyi balesetek és katasztrófák, melyek eredményeként súlyos káresemények keletkezhetnek nem korlátozódnak kizárólag a veszélyes anyagok ipari üzemekben való alkalmazására a vegyi szennyezések következményeivel akár jóval tágabb térségekre kiterjedően is számolni lehet.

A vegyi anyagok kiszabadulásával járó havária jellegű ipari eseményeknél megfigyelhető, hogy rendre valamely eszközhöz köthető részfolyamat szabályozatlanná válva a technológiai környezet közvetlen közelében veszélyes szennyezésekkel járó környezeti állapotok állnak elő [1], ahogyan arra az 1. ábra is rámutat.



1. ábra: A vegyi balesetek kiváltó okai
Forrás: Szerkesztette [2] nyomán a szerző

Ezek egyéb kockázati tényezőkkel kombinálódva a szabadban uralkodó befolyásolhatatlan körülmények miatt akár nem várt kémiai, fizikai, de akár mechanikai kölcsönhatásokat is elindíthatnak. Amennyiben ezekben szerepet játszó hatástényezők egymást iniciálva jelentkeznek, úgy a vegyi anyagok veszélyes tulajdonságai is könnyen kritikus és spontán tovább fejlődő folyamatok egyik lehetséges kockázataként mutatkozhatnak meg. [3]

Mint kémiai kockázati tényezők a veszélyes anyagokkal végzett minden tevékenységet, ideértve előállításukat, kezelésüket, készletezésüket és mozgatásukat lehetséges veszélyforrásként kell számon tartani. Az ennek során kiszabaduló vegyi anyagok a technológiai rendszer nyújtotta ellenőrzött körülmények megszűnése folytán, veszélyeztetik a biztonságot. [4] Az ilyen üzemzavaroknál a kárelhárító és mentési feladatokat azonnal meg kell kezdeni.

Az ilyen havária események bekövetkezését összetett műszaki-technikai és szervezési intézkedésekkel lehet elejét venni, melyek a megfelelő technológiai szabályzó és biztonságtechnikai, valamint munkavédelmi előírások betartásával realizálható. Technológiai rendszerelemek tekintetében ezek érintik egyebek mellett az energetikai berendezéseket, nyomástartó edényeket [5], valamint a logisztikai rendszer eszközeit [6], nem utolsó sorban pedig veszélyes anyagokkal tárolótályait idesorolva azok üzemi kármentőit is. [7], [8]

Ezekhez már a vegyi anyagok kezelésével járó tevékenység létesítéskori üzemszervezési információkból kiindulva ki kell dolgozni a lehetséges kárfelszámolási feladatok tervét. Adekvát módon ezt csak a technológiai üzemviteli előívásainak ismeretében határozhatók meg. Ugyanakkor a kárelhárítás terveit a technológiai dokumentációkban is meg kell jeleníteni. Az adott technológiai részleg érintett munkavállalóinak az üzemzavari helyzetben végzendő feladataikat ismerniük szükséges és ezekre fel kell készülniük. Ehhez megfelelő kárelhárító és mentő eszközöket rendelve végezhetők el csak sikeresen a mentési és a helyreállítási munkák. A hatékonyság javítása és a szervezetlenség miatti bizonytalan kimenetelű ad hoc végrehajtás kizárása érdekében szükség esetére a munkavédelmi szaktevékenység körébe tartozó mentési tervet is el kell készíteni és az abban foglaltakat gyakoroltatni kell a munkavállalókkal. [9]

Azért is indokolt ezekre felkészülni, mert az elmaradó vagy késlekedés miatti előre nem látható véletlen hatásoknak kitett vegyi anyagok megfékezhetetlen reakciói robbanási láncreakciókhoz, tűzek heves kitöréséhez, valamint az esemény hatókörében tartózkodók fokozott expozíciójához, súlyosabb esetben akár halálához is vezetnek. [10]

A veszélyes anyagok felhasználása terén a leggyakoribb káreseményt kiváltani képes hatások a robbanások, tüzek, káros anyagok okozta környezetszennyezés. Előbbiek kárfelszámolása kapcsán - a sérültek elsődleges mentésén kívül - jellemzően az ipari objektumok, lakó- és középületek, valamint az infrastruktúrák rongálódása miatti műszaki feladatokkal szembesülhetnek a mentő erők.

Ezzel szemben a vegyi anyagokkal szennyezett területen alapvetően a veszélyes anyagok kémiai, toxikológia sajátosságához igazodó vegyivédelmi szakmai tudást igénylő vegyi felderítési és vegyi mentesítési munkálatok elvégzésére van szükség. Azzal a korántsem elhanyagolható nehezítő tényezővel, hogy ezeket a feladatokat veszélyes vegyi anyagok egészségre ártalmas hatásai elleni védelem miatt légzőkészüléket és bőrvédelmet egyaránt kell alkalmaznia a beavatkozóknak. A védelem szintjét is a vegyi anyagról felderítéssel szerzett információk alapján kell meghatároznia a mentést irányító kárhelyparancsnoknak. [11]

Az erős hatású mérgező, korrozív anyagok jelenlétében végzett beavatkozásoknál a legmagasabb, „A” szinthez igazodó védőeszközökben lehet csak a kárelhárítást végezni. Az olyan esetekben, amikor a vegyi anyag nem beazonosítható mindig a biztonság konzervatív szakmai megközelítéséből kiindulva ugyancsak a legmagasabb fokozatú védelmet kell előírni.

A kiszabadul veszélyes anyag hatásterülete által érintett övezetben a szennyezettség mértéke korántsem egyenletes. Ez a baleset következtében a vegyi anyag környezetbe kerülését okozó sérült berendezéstől kiindulva térben és időben, illetőleg más minőségjelzőket nézve változó jelleget mutat. A vegyi szennyezés kialakulásával együtt járó körülmények alapvető jellegüket tekintve megegyeznek más vegyi anyagok kisebb dimenzióban történő alkalmazásánál fellépő jellegzetességekkel. A vegyi anyagok a szennyezett területen ezektől befolyásolva fejtik ki hatásukat, veszélyeztetik az érintett területen tartózkodókat. [12]

VEGYI BALESETEK KELETKEZÉSÉNEK FAKTORAI

A vegyi anyagok megjelenése az ipari folyamatokban töretlen technológia fejlődés eredménye, mégis a mind magasabb szintű mérnöki tudás ellenére is mindig rávetült az ipari szerencsétlenségek árnyéka a műszaki haladás ezen területére. A technológia folyamatokban számos hiba, léphet fel és minél bonyolultabb rendszereket kell felügyelnie a biztonságirányításnak mindinkább nő a tévedés lehetősége. Ráadásul a természeti környezet éghajlatváltozással összefüggésbe hozható egyre intenzívebb jelenségei sem kedveznek a váratlan elemi csapások pusztító hatásai elleni védelem elvárt szintje megőrzésének. Ráadásul az emberi hibák változatlanul kiválthatják ezeket, de tovább is tetézhetik a károk mértékét.

Ahhoz hogy elkerülhessük ezeket, széleskörű ismeretekre van szükség nem csak a kémia és technológiai biztonság, de sok más kapcsolódó diszciplína szintetizáló képességével ötvözve. Ennek kezdeteit teremti meg az iparbiztonság, amelynek nem csak jogszabályokban leírtak adják, hanem a szükséges műszaki hozzáértés is ezzel szinkronban kell, hogy fejlődjön. Nem elegendő csak egy-egy veszélyeztető tényezőt és annak hatásait ismerni. Hisz például egy tűzesetet egy sor más a káresemény kiinduló állapotát felülírni képes másodlagos változást is elindíthat. Az ilyen helyzet akár látens, késleltetett módon is vezethet eszkalációhoz, amit a beavatkozó tűzoltók felderítése sem biztos, hogy képes detektálni. Rendszerint ilyenkor történnek a tragédiák és nem csak a kárelhárítást végzők körében. Példaként említhetjük a nagy koncentrációjú veszélyes gázok bevetési ruházat szövetén való adszorbeálódásának jelenségét, ami fokozatosan desszorbeálódva a légzésvédő eszköz levétele után is súlyos mérgezést okozhat a ruházatot viselő személynél. [13] Másfelöl ez a szennyezett zónából kimentett sérültek ruházatával is hasonlóan bekövetkezhet. [14]

Viszont a veszélyes anyagok kiszabadulásának súlyos ipari balesetek során előforduló szennyezései okozta körülmények az ilyen egyedi jelenségektől jelentősen eltérőek. A súlyos balesetek bekövetkezése okainak vizsgálata arról tanúskodik, hogy az egyes veszélyeztető tényezők és azoknak a külső befolyásoló körülményekkel való kölcsönhatása minden káreseti szituációt egyedivé tesz.

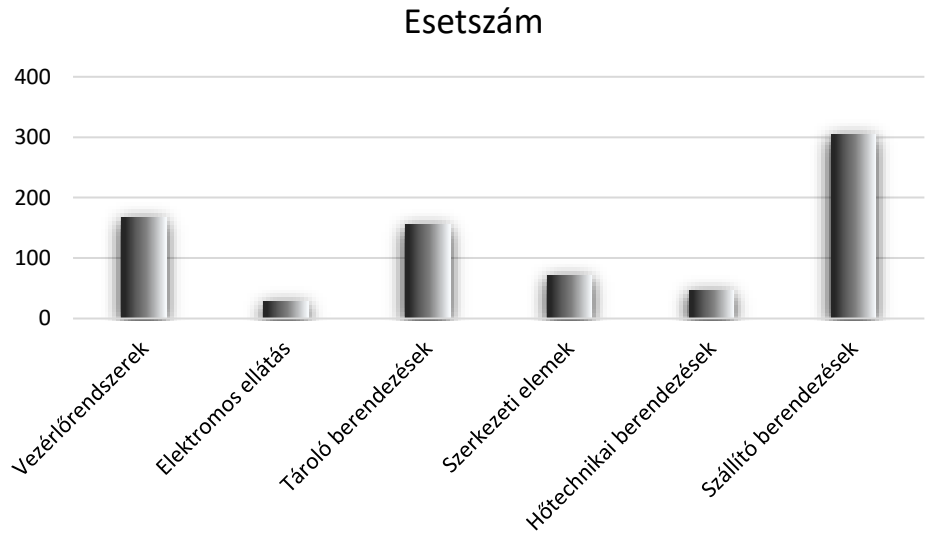
Ezen felül nem egyedül megjelenésük igen különféle, de az azokat eredményező tényezők lényegében jelentős részben determinálják is a szennyezés kialakulását. A lehetséges vegyi szennyezés kialakulását, melyek során veszélyes vegyületek a szabadba juthatnak, az alábbi a jogszabályban[2] rögzített technológiai ciklusokhoz kötődően azonosíthatjuk:

- előállítás,
- felhasználás,
- tárolás,

[2] Katasztrófavédelmi Törvény (továbbiakban: Kat. Tv.). 3. § 27.

- szállítás. [15]

Ezért olyan rendszerekben, ahol veszélyes technológiai folyamatok lezajlására kell számitani, hatékony biztonságtechnikai és szabályozó rendszert kell beépíteni. Habár ezek mára rendkívül megbízhatókká váltak, mégis pusztán csak ezekre hagyatkozni nem lehet a technológiai biztonság garantálásában, mivel a gépek, berendezések és egyéb termelő eszközök meghibásodásai továbbra sem zárhatók ki, amint azt a 2. ábra mutatószámaiból is kiolvashatjuk.



2. ábra: Kiváltó technológiai elemek megoszlása a vegyi balesetekben
Forrás: Szerkesztette [2] nyomán a szerző

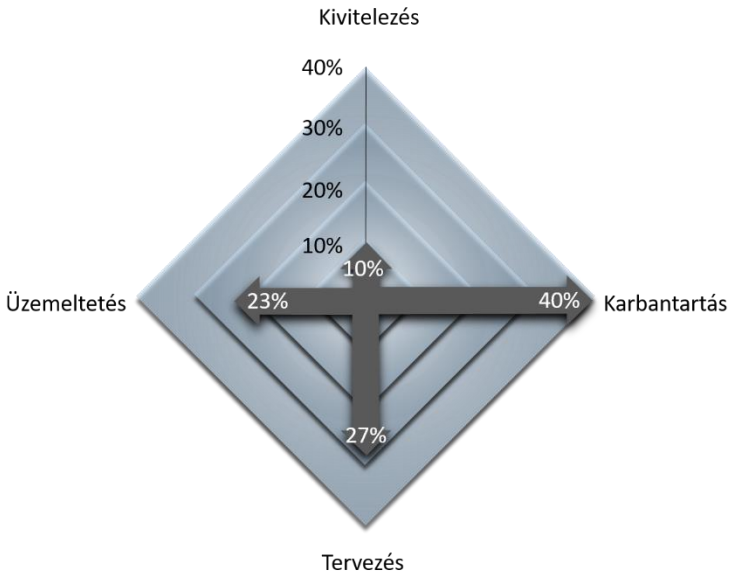
A technológiai berendezések meghibásodásával összefüggő vegyi balesetek sokféle üzemtípusban előfordulhatnak, azonban mindegyikük közös ismérve, hogy valamely rendellenes tevékenység vagy folyamat generálta a veszélyeket. Rendeltetésszerű működési folyamatok, csak elvétve rendkívüli körülmények, mint például rejtett anyaghibák csekély számú esetben vezethetnek súlyos balesethez. Vagyis a berendezések tervezéskor kialakított műszaki-technikai paraméterei szavatolni képesek, hogy működés közben fellépő terek és hatások jelentette igénybevételnek ellenálljanak és a veszélyes vegyi anyagokat biztonságosan elhatárolják a környezettől és akár még a bennük zajló heves vegyi reakciók ellenére is megtartsák integritásukat. Persze ez csak abban az esetben igaz, ha méretezésüknek és szerkezeti anyagaiknak megfelelő technológiai rendszerbe illesztve alkalmazzák őket, valamint az előírt technikai kiszolgálás és karbantartási műveletek a technológiai utasításokat követve történik.

Persze ez utóbbi igaz valamennyi berendezésre és nem csak a speciálisan egy-egy konkrét gyártási folyamathoz speciálisan megválasztott változatra. A más általánosan felhasznált berendezésekkel, mint például tárolótartályokkal és termékvezetékek minden üzem és folyamat elemeként szintén igénylik az időszakonkénti felülvizsgálatot és az azok nyomán szükségessé válható javítások elvégzését, hisz meghibásodások a normál üzemvitel mellett is bekövetkeznek. [16]

Érdemes tehát röviden feltérképezni a berendezések lehetséges hibaforrásait, amelyek balesetek kiindulópontját képezhetik. Ezek felosztásában a hibahatásoknak a havária esemény kibontakozásában két kategóriát azonosíthatunk. Ennek alapján közvetett és közvetlen kiváltó okokról beszélhetünk. Előbbinél valamely egyéb körülmény is megszakítja a hatásláncot. A balesetek kiváltásában tapasztalható arányaikat tekintve az ilyen mögöttes tényezők a baleseti kivizsgálásokkal felderíthetők. Például a szivárgást eredményező csőtörések viszonylatában is azonosítható, hogy az alábbi:

- Tervezés
- Kivitelezés
- Üzemeltetés
- Karbantartás

között ezek a hibaokok hogyan oszlanak el. Ezt vázoltam a 3. ábrán.



3. ábra: Hibaokok megoszlása a szivárgást eredményező csőtöréseknél
Forrás: Szerkesztette [17] nyomán a szerző

Túl ezen előfeltételeken persze gyakorta egyéb a balesethez szorosan köthető történés is megmutatkozik a vegyi anyagok technológiai térből történő kijutásában a normál üzemi feltételektől való eltérések szemszögéből. Különösen a technológiai paraméterek részéről, melyeket a folyamatok érzékenységétől függően szűk vagy tágabb határértékek között nivelláló tartományban kell tartani:

- bemeneti paraméterek téves megállapítása,
- alapanyagok helytelen betáplálása,
- energetikai zavarok beállása,
- műveleti fázisok sikertelen váltása,
- konverziók félresiklása, stb.

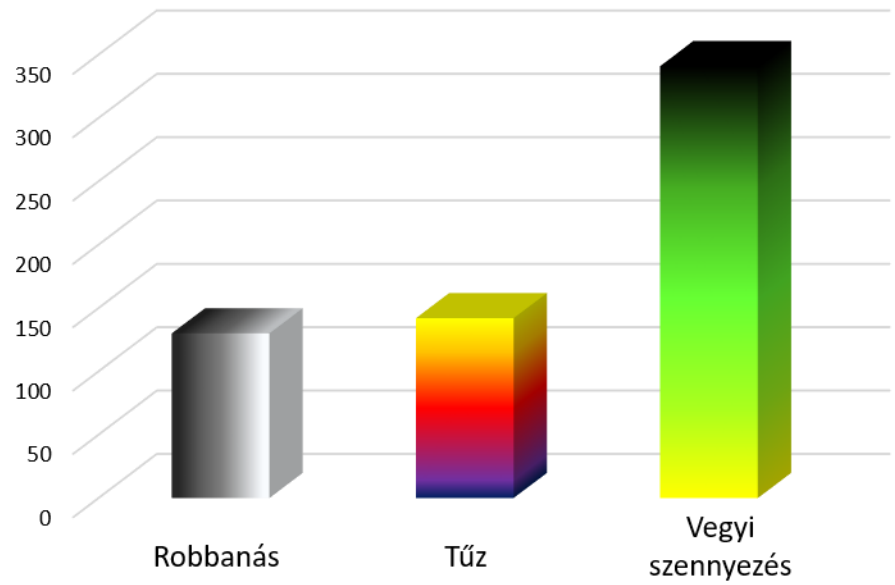
Persze ezekben olykor emberi gondatlansággal vagy még akár ártó szándékkal is találkozhatunk.

Az eddig felsoroltakból is láthatóan, bár a lehetséges hibák száma a technológia összetettségével arányban mind inkább hatványozódik, ellenben szisztematikus biztonsági irányítási rendszerek felállításával a veszélyes folyamatok kockázatait megfelelő szintre csökkenthetjük. Tekintve azonban, hogy ugyan a védelmi intézkedések rendszere is igen bonyolult és a biztonságot befolyásoló tényezők is változhatnak, emiatt a veszélyeztetettség állapota sem konstans.

Azonban a technológiai hibák jellegzetességeit ismerve következtethetünk az azok nyomán előállható baleseti kibocsájtások várható lefolyására és a fellépő szennyezések sajátosságaira. Mivel a hibák műszaki-technikai jegyei és a berendezésben, valamint a környezetben uralkodó környezeti állapotok jelentősen kihatnak a vegyi anyag transzportfolyamataira is, azokat együtt értékelve kell feltérképezni a kiszabaduláskor és azt követően is.

A VEGYI KÁRTERÜLET KIALAKULÁSA

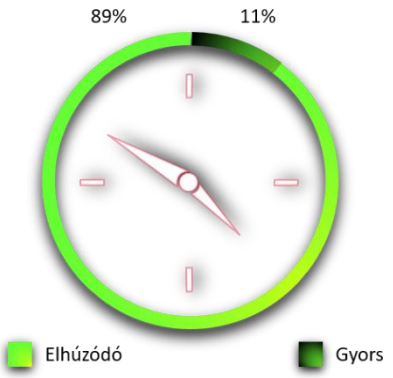
A vegyi anyag kiszabadulásának következtében többféle veszélyeztető tényező léphet fel, de köztük dominálnak a szennyező hatások, amint azt a 4. ábra szemlélteti.



4. ábra: A fő veszélyeztető tényezők megoszlása vegyi baleseteknél
Forrás: Szerkesztette [2] nyomán a szerző

A szennyezés kockázatait a vegyi anyag tulajdonságai, mennyiségi viszonyai és kiszabadulásának körülményei határozzák meg, amely a lassú szivárgásos jelenségektől egészen a nagy koncentrációjú szennyezett gázfelhő messze a telephely határain túlra sodródásáig terjedhet. Egyértelmű, hogy a koncentráltan megjelenő vegyi anyag jóval nagyobb

károk kiváltására képes. Mégis mi különíti el egy-egy vegyület esetében a kibocsátási jelenségeket, és mikor hozhat létre ilyen súlyos katasztrófával fenyegető helyzetet, azt elsősorban a kibocsátás paramétereiben kell keresni. Ezek közül szembe ötlő, hogy az egyes vegyi balesetnél észlelhető töménység növekedés a károkozás potenciálját is fokozza. Ráadásul ezek az elhúzódó, és ezért nagyon sokszor igen nagy mennyiségű veszélyes anyag kibocsájtással is járó vegyi balesetek vannak többségben az esetszámokat megvizsgálva, amit az 5-ös ábra statisztikailag is alátámaszt.



5. ábra: A vegyi balesetek kibocsájtási jellege intenzitás szerinti bontásban
Forrás: Szerkesztette [2] nyomán a szerző

A gyors kibocsátással a környezetbe kerülő veszélyes vegyi anyagokról elmondható, hogy azokat az eseményeket kísérik ilyesfajta jelenségek, ahol gáz és folyadékok hírtelen elpárolgása vagy halmazállapotának váltása következik be. A normál környezeti viszonyok mellett gázhalmazállapotú vegyi anyagok esetében ez utóbbi cseppfolyósított formában, nyomás alatti tárolásnál adódhat elő. Ilyenkor a nyomástartó edényen, berendezésen felhasadó burkolaton át tör ki a gáz. Folyadékoknál viszont az alacsony forráspont az egyik lényeges kritérium a fázisváltás bekövetkezésének. Amennyiben az ezzel az anyagi minőséggel rendelkező vegyület kiszabadulása közben a környezeti hőmérséklet a forráspont fölötti tartományba esik, akkor a hirtelen felforrt folyadék gőzeinek térfogatnövekedése gyorsítja a sérült berendezésből való kijutását az anyagnak.

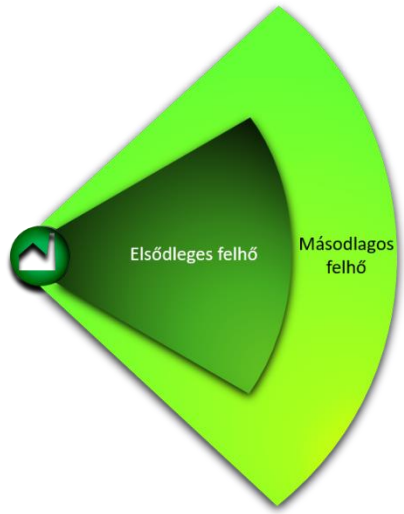
Persze a kiáramlás közben számottevően közrejátszik a szerkezeti anyagokok keletkező sérülés milyensége is. Hisz technikai értelemben egy felhasadó tartálypalástból való kiszabadulásának lezajlása a vegyi anyagnak jócskán különbözik egy korrózió okozta pontszerű nyíláson át történő nyomásvesztéstől. Utóbbinál a Joule-Thomson effektus miatti lefagyás is elképzelhető. Emellett még a nagyon gyors anyagáramban létrejöhető töltésleválások miatti statikus feltöltődés lehetősége is felvetődhet, ami éghető anyagoknál kritikus lehet és robbanáshoz vezethet. Mindezeket persze a konkrét vegyi anyag és előálló állapotjelzők kölcsönhatásában vizsgálva lehet műszaki biztonsági oldalról pontosan definiálni. Nem is beszélve az esetleges további veszélyes kölcsönhatásokról. Összegezve kijelenthető, hogy a gázok vagy gőzök pillanatszerű kitörése rövid, de igen heves és romboló hatással van a környezetére, ami másodlagos káreseményeket is könnyedén elindíthatnak. Ettől füg-

getlenül amennyiben a feltételek adottak, hogy egyben tartsák a gázfelhőt, úgy gyors kibocsátásnál is képződhet szennyezőképes légtömeg. Például a nagy koncentrációjú gőzök kondenzációja miatti ködképződés jóvoltából is teszem azt.

A vegyi szennyezések többnyire nem ilyen típusú folyamatként veszélyeztetik környezetüket. Az ide sorolt kibocsájtást tipikusan nem feltétlenül nyomáskiegyenlítődés okozza, mint inkább a nagy átmérőjű, például felnyílt dómfedélen, stb. át kijutó vegyi anyag és a környezete közötti hőmérsékletkülönbség okozta sűrűségkülönbség hajtja a gázok, gőzök kibocsátását.

AZ ELSŐDLEGES ÉS MÁSODLAGOS FELHŐK TERJEDÉSE

Az ilyen és az előzőkben leírt primer eseményeknél kialakuló szennyezett légtömeget hívjuk elsődleges felhőnek. A baleseti kibocsátás forrásával szoros összefüggésben innen ered a szennyezés első hulláma, amely folytonos hullámban, de szünet nélkül hígulva terjed. Azonban ennek mélysége nem jelenti a végső határát a vegyi anyag szennyezőképes transzportfolyamatainak. Mivel erre a követő fázisban újabb, de már kisebb töménységű felhő szennyezési hulláma rakódik rá, ahogyan az megfigyelhető a 6-os ábrán vázoltakon.



6. ábra: A baleseti vegyi szennyezés felhőinek terjedési vázlata
Forrás: Szerkesztette [18] nyomán a szerző

Az említett követő hullámban útjára induló vegyi anyag felhőt nevezzük másodlagosnak. A szennyező anyag koncentrációja ebben a terjedés irányában vett egy adott ponton nézve általában kisebb, mint az elsődleges felhőben. A másodlagos felhő azonban elhúzódóan vonul végig a talajfelszín felett, mivel annak utánpótlásaként viszonylag lassan, de állandó intenzitással szabadul fel a vegyi anyag. Ennek magyarázata a keletkezésének körülményeiben keresendők. Eltérően az elsődleges kibocsájtásban keletkezettől, itt a kiömlő folyadék halmazállapotú vegyi anyag nagyfelületen szétterülő felszínéről ütemesen párolgó gőzök képezte felhőről van szó. A párolgás sebességét:

- a folyadék tenziója,
- a talaj megkötőképessége,
- a talaj és a levegő hőmérséklete,
- és a légmozgás határozza meg.

Tehát a képződő tócsa felett létrejövő másodlagos felhő koncentrációviszonyait a tócsával érintkező talaj és levegő vegyi anyaggal való kölcsönhatása döntően befolyásolja, az egyéb légállapotokat leíró tényezők, stb. mellett. Vagyis a szennyező anyag felhőinek haladását a talaj felett - az anyagi minőségen túl - környezeti tényezők befolyásolják, köztük:

- a szélirány és sebesség,
- a levegő függőleges stabilitása,
- a csapadékviszonyok,
- a topográfia,
- a vegetáció,
- és a beépítettség.

Az elmondottak rávilágítanak, hogy a vegyi anyagok baleseti kibocsájtása miatt bekövetkezett káresemények során nem csak az üzemi terek és telephelyi környezet, hanem a szomszédos lakott területek szennyezésével is számolni kell. A vegyi szennyezés miatti katasztrófák várható hatásait a súlyosabb eszkaláció megakadályozása céljából minél hamarabb ki kell értékelni. A védelmi intézkedések gyors meghozatalát szolgáló előzetes értékelés megkerülhetetlen és elsődleges szegmense a vegyi helyzet értékelése, melyhez ismerni kell a baleset helyszíne környezetében uralkodó és előzőekben felsorolt időjárási körülményeket.

A légmozgás jelentős befolyást gyakorol a vegyi szennyezések terjedésének irányára. Azok képzeletbeli tengelye egybeesnek a széliránnyal, amely így egy-egy védelmi tervezési folyamatban vett szimulált szcenárióban is az uralkodó szélirányba történő haladással modellezhető. Széllel szállított szennyező légtömegek haladási sebessége a feltételezett szennyezett zóna egy pontjára való várható beérkezésének idejét is determinálja. Persze ezt felülírja, ha heves szélrohamok sújtják a kibocsátás környezetét, mert akkor nagyon gyorsan kisöprik és feloszlatják a vegyi anyagot. Ugyanakkor a szél okozta áramlás bármilyen lassú tempójú legyen is legyen az, valamilyen mértékben mindig eredményez felhigulást, amely mind függőleges, mind pedig a szélirányra merőlegesen fokozatos szétterülést vált ki. Ezért is ábrázolja a 6-os ábrán szereplő vázlat legyezőszerűen széttartó egyenesektől közrefogva a vegyi felhőket.

Emellett az időjárási tényezők sorában központi kérdés, hogy azok együtthatása a közvetlen talajközeli légrétegben milyen befolyást gyakorolnak a terjedési folyamatokra. A tajalmenti hőmérséklet és szél összevetése alapján három fő légállapotot különböztetik meg a levegő függőleges stabilitását érintően:

- inverzió,
- izotermia,
- konvekció.

Az inverzió és az izotermia elősegíti a kiszabadult vegyi anyagok felhőinek tartós megmaradását és így a veszélyes koncentrációk igen lassú csökkenését. Ezért azok veszélyeztető hatásukat megőrizve a szennyezés forrásától jóval nagyobb távolságra juthatnak el.

A jellemzően a nyári derűs napokon tapasztalható konvekció viszont az erőteljesen felmelegedő talajfeletti légrétegben ébredő felszálló légáramlatoknak köszönhetően viszonylag gyorsan szétoszlatja a szennyezett levegőt és a vegyi anyagok koncentrációja rohamosan csökken, szinte csak a kiömlés helyén mérhetünk veszélyes koncentrációkat.

A csapadék tevékenység is kedvez a védekezésnek, mivel intenzitásának függvényében előbb-utóbb teljesen kimossa a vegyi anyagokat a levegőből. A talajba juttatva azokat, és elősegítve a nedvesség hatására bekövetkező hidrolízis miatti kémiai átalakulásukat. Persze ennek átalakulási viszonyait a szennyező vegyület kémiai stabilitása igencsak meghatározza. Ez a folyamat is tovább csökkenti az adott helyen fellépő szennyezés mértékét.

A növénytakaró (erdő, bokrok, sűrű fák) a beépítés sűrűsége és a domborzat jelentős tagoltsága jelentősen visszafoghatják a szennyezett felhők terjedésének ütemét, mindazon által elősegítik a szennyezett levegő megrekedését ezekben a zónákban és tartósabb, illetőleg veszélyesebb szennyezettséget válthatnak ki. Erősen szabdalt terepen található vízmosásokban, a völgyekben, valamint a magas építményekkel sűrűn beépített utcákon hosszanti irányban a légáramlatokkal szállított szennyezések terjedésének mélysége megnövekszik a nyílt terephez viszonyítva. Ez azért lehetséges, mert a szél szétoszlató hatása ilyen helyen kevésbé tud érvényesülni és a szennyező anyag hosszabb ideig megreked a felhőben.

Magától értetődően a vegyi kárterület környezetében uralkodó időjárási viszonyok egyáltalán nem változatlanok és akár markáns eltérések is adódhatnak az előzetesen kialakított helyzetértékeléshez képest. Továbbá a vegyi anyagnak a felhőkből történő kiülepedése sem a szimulációkban alkalmazott, szabályos eloszlási görbéket követi. Ezért aztán szennyezés valós helyszíni mértékének detektálása is megköveteli, hogy a vegyi balesetek környezetében szisztematikus felderítéssel és mintavételezéssel közvetlenül szerezzünk információkat a kárterületet érintő prognózisaink pontosítása érdekében.

KÖVETKEZTETÉSEK

A veszélyes üzemek bekövetkezett balesetei, melyek következtében fenn áll a vegyi anyagokkal való szennyezés veszélye. A vegyi anyagokkal történő baleseteknél számításba kell venni a kiszabaduló veszélyes anyagok lehetséges környezetbe kerülését. A következmények sorában számolni kell azzal, hogy azok fenyegetik a lakosságot és a környezetet. [19]

A vegyi anyagok kiszabadulása elsősorban lokális fenyegetettséget hordoz magában, azonban az uralkodó meteorológia helyzettől függően ez kiterjedt térségben is okozhat súlyos katasztrófát. Ennek megelőzésére az üzemeltetők a vegyi veszélyeztetés kockázatának csökkentésére védelmi tervet készítenek, melyre alapozva történik az élet- és vagyonbiztonság szervezése haváriák során.

Bár az üzem üzemeltetője folyamatos tájékoztatást biztosít a helyzet mérlegeléséhez, a kárelhárítási tevékenység sikere továbbra is kárterület hozzáértő értékelésén múlik, amit megfelelő műszaki ismeretekkel rendelkező szakemberekre lehet csak bízni. Fontos tehát, hogy ne csak a paragrafus betűin keresztül lássuk az idevonatkozó iparbiztonsági és polgári védelmi kérdéseket, de a mögöttük meghúzódó műszaki biztonsági és veszélyhelyzetkezelési kompetenciákkal is felvértezzék magukat a védelem szervezésében érintettek.

Ezt eredményesen szolgálhatja a fejlett országokra jellemző jól szervezett közigazgatás által felállított szabályrendszer és az ahhoz társuló a hatósági tevékenység mellett a

cikkben is felvillantott ismeretek elsajátítása. Az itt tetten érhető műszaki szemlélet a nagyarányú technológiai fejlődéssel együtt járó kemizáció árnyoldalaként esetenként megjelenő vegyi baleseteknél fellépő kémiai kockázatoknak és a biztonságnak a társadalmi elvárásokkal való összhangját hivatott szolgálni a vegyi balesetek helyzetértékelésénél.

FELHASZNÁLT IRODALOM

[1] Szakál Béla: *Veszélyes anyagok és kárelhárításuk* I-III. Főiskolai jegyzet, Ybl Miklós ÉK 2005;

[2] ARIA, Online Database, French Ministry of Environment, Bureau for Analysis of Industrial Risks and Pollutions. Analysis, Research and Information on Accidents, https://www.aria.developpement-durable.gouv.fr/?lang=en&s=&fwp_recherche=chemical%20accident, (letöltve: 2024. 08. 02.);

[3] Haubert G., *A munkahelyi kockázatértékelés és -kezelés gyakorlati kézikönyve*, Munkavédelmi Kutatási Közalapítvány, Budapest, 2003, ISBN: 963-206-499-2;

[4] Kápolna F., Vegyipari technológiai alapismeretek, OMKT., Budapest, 2001., 72. o.;

[5] Kemencés J.: *Nyomástartó berendezések biztonságtechnikája*, OMKT Kft, Budapest, 2010. ISBN 978-963-89258-2-0, 44. o.;

[6] Sárosi Gy., *Veszélyes áru raktárlogisztika - korszerű követelmények*. Budapest, 2006. Complex Kiadó, ISBN 963-224-869-1;

[7] Berger Á.: *A veszélyesanyag-tárolótartályok tervezésének iparbiztonsági aspektusai*. Hadmérnök, 2021.,16 (3), pp. 81–96. https://doi.org/10.32567/hm.2021.3.5;

[8] Berger Á.: *Veszélyesanyag-tároló tartály üzemeltetésének iparbiztonsági feltételrendszere*. Műszaki Katonai Közlöny, 2021., 31 (3), pp. 17-31. https://doi.org/10.32562/mkk.2021.3.2;

[9] Fölkl R. et al.: Munkaegészségügyi és Munkavédelmi Enciklopédia, Budapest I.-III. OMIKK, Bp. 1986-89. ISBN 963-592-433-X;

[10] Halász L. - Földi L.: *Környezetvédelem – környezetbiztonság* egyetemi jegyzet, ZMNE, Budapest, 2000.;

[11] Nagy K. – Halász L.: *Katasztrófavédelem*, egyetemi jegyzet, ZMNE, Budapest, 2002.;

[12] Négyesi Gy.: *Vegyi balesetek*. VÉDELEM, Katasztrófa-, Tűz-, és Polgári Védelmi Szemle, 1995., II : 2. évf. (3) 50. o.,

[13] ROGULA-KOZŁOWSKA W., PIĄTEK P., KOZIELSKA B., WALCZAK A., *Off-gassing from firefighter suits (nomex) as an indoor source of BTEXS*, Chemosphere, 2024, 350, 140996. DOI: 10.1016/j.chemo sphere.2023.140996.

[14] Okumura S, Okumura T, Ishimatsu S, Miura K, Maekawa H, Naito T. *Clinical review: Tokyo - protecting the health care worker during a chemical mass casualty event: an important issue of continuing relevance*. Crit Care. 2005 Aug;9(4):397-400. doi: 10.1186/cc3062. Epub 2005 Feb 17. PMID: 16137390; PMCID: PMC1269427.

[15] A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény,

[16] Kletz T. A. *What went wrong? Case Histories of Process Plant Disasters and How They Could Have Been Avoided*. 5th ed. 2009. ISBN 978-1-85617-531-9

[17] Kletz T. A. *Learning from Accidents* 3 trd ed. 2001. ISBN 0 7506 4883 X, 194. o.

[18] H. B. F. Gow, R.W. Kay (szerk.) *Emergency Planning for Industrial Hazards*. Proceedings of the European Conference on Emergency Planning for Industrial Hazards,

held at the Congress Centre, Villa Ponti, Varese, Italy, 4-6 November 1987. CRC Press, 2003. 122 o.
[19] Kátai-Urbán L., *Handbook for the Implementation of the Basic Tasks of the Hungarian Regulation on „Industrial Safety”.* Nemzeti Közszolgálati Egyetem, KVI, Budapest, 2014. ISBN 978-615-5491-70-2
[20] Kátai-Urbán L., Súlyos ipari balesetek elhárítását és helyreállítását célzó jogintézmények egységes rendszerbe foglalása. Hadmérnök, 20014., IX. évf. (4) 106. o.

THE PLACE AND IMPORTANCE OF EU REGULATIONS ON THE DIGITAL MARKETS AND SERVICES IN THE EU AND NATIONAL LAW

A DIGITÁLIS PIACOKRÓL ÉS DIGITÁLIS SZOLGÁLTATÁSOKRÓL SZÓLÓ EURÓPAI UNIÓS RENDELETEK HELYE ÉS JELENTŐSÉGE AZ UNIÓS ÉS HAZAI JOGBAN

KOLEJANISZ Márk[1] – RÉTI Zsófia[2]

Abstract

Recognizing the risks of the new technologies and the online space, the European Union in the recent years has embarked on regulation process to reduce them. These risks are including the strong competitive advantages, and considerable economic power gained by some of the service providers in the online market, the growing of the infringements of the users' rights, and the issues related to the use of the Artificial Intelligence. Although – as we will refer to that later – there were already rules in the European Union, specifically regulating the online world, thus we can see that the rapid and dynamic development of this field requires the continuous revision of the legislation and the introduction of new provisions. In this paper we focus on two EU regulations of particular importance for businesses: the Digital Markets Act and the Digital Services Act. These regulations are relatively recent pieces, they have not been in force for a long time, but they are also mandatory in our country.

Keywords

DSA, DMA, EU, regulation, digital

Absztrakt

Az Európai Unió felismerve az új technológiákban és az online térben fellelhető kockázatokat az elmúlt években egy olyan rendeletalkotási folyamatba kezdett, amelynek célja ezek csökkentése. Ilyen kockázati tényezőként értékelhetjük többek között az egyes szolgáltatók által szerzett nagymértékű versenyelőnyt, gazdasági potenciált, az online piacon, a személyiségi jogok megsértésének egyre növekvő tendenciáját, vagy éppen a mesterséges intelligencia használatához kapcsolódó kérdéseket. Habár – ahogyan arra később utalni fogunk – korábban is voltak már kifejezetten az online világot rendező szabályok az Európai Unióban, mégis azt láthatjuk, hogy ezen területnek a dinamikus és gyors fejlődése igényli a jogszabályok folyamatos átdolgozását, új rendelkezések bevezetését. Jelen tanulmányban a vállalkozások szempontjából két kiemelkedő jelentőségű rendelettel foglalkozunk: a digitális piacokról szóló rendelettel, valamint a digitális szolgáltatásokról szóló rendelettel. Ezek viszonylag fiatal, nem régóta hatályban lévő jogszabályok, amelyek hazánkban is kötelezően alkalmazandók.

Kulcsszavak

DSA, DMA, EU, rendelet, digitális

[1]mark@kolejanisz.hu I ORCID: 0009-0008-6121-5976 I Lawyer, Ügyvéd I Kolejanisz Law Firm, Kolejanisz Ügyvédi Iroda
[2]retizsofia@kolejanisz.hu I ORCID: 0009-0004-7379-7572 I Expert, Szakértő I Kolejanisz Law Firm, Kolejanisz Ügyvédi Iroda

BEVEZETŐ GONDOLATOK

A DSA és a DMA rendeletek az Európai Unió legújabb kori jogalkotási termékei. Ezek azonban nem előzmény nélküli jogszabályok, a digitális életviszonyok, a digitális világ szabályozása, jogi, normarendszerbeli lenyomata immár huszonöt-harminc évre visszatekintő alapokkal rendelkeznek a közösségi jogban. [1]

Miért merült fel egyáltalán a közösségi jog jogalkotójában a digitális világ normarendszerének közösségi jogi szabályozása? Erre a válasz az életviszonyok megváltozásában, méghozzá gyors megváltozásában keresendő. Ma már triviálisnak tetszik, de a számítógépek az 1990-es évek közepétől egyre inkább felgyorsuló terjedése és technológiai fejlődése magával hozta azt a jelenséget, hogy az emberiség feladatai megoldásakor, munkája végzésekor egyre inkább támaszkodott, támaszkodni kezdett a számítógépek segítségére. A számítógépek beépültek az oktatásba, az egészségügyi ellátásba, a különböző fehérgalléros munkavégzési folyamatokba. Az 1990-es évek közepétől nemcsak a számítógépek kezdtek el rohamosan fejlődni és terjedni, de az internet is hozzáférhetővé vált az Európai Unió területén egyre szélesebb felhasználói kör számára.

Manapság a tartalomgyártás az internetes világ természetes velejárójaként tartható számon, ugyanakkor ez korántsem volt mindennapi jelenség néhány évtizeddel ezelőtt. Az 1990-es évek végétől tömegével jelentek meg az ún. közösségi oldalak, amelyek már a Web 2.0 szerinti működést tették lehetővé. Ez azt jelenti, hogy ezek az oldalak a szemlélődő felhasználókból egy aktív, tevékeny tartalomgyártó közösséget hoztak létre, azaz a felhasználók innentől már nem csak, mint olvasók, hanem mint a közösségi diskurzus alakítói, formálói tudtak ezeken az oldalakon tevékenykedni. [2](Ebben az esetben tekintsünk el attól, hogy a tartalomgyártás milyen minőségű tartalom kibocsátását jelenti, azaz a fogalmat a hétköznapokban elfogadott jelentéstartalma alapján alkalmazzuk és nem a tartalom minősége szempontjából.) A tartalomgyártás körén belül exponenciálisan növekedett az interneten keresztül, online térben lebonyolított kereskedelmi ügyletek száma is. [3] Természetesen az új technológia elterjedése maga után vonta egy új típusú szabályozás megjelenését is.

Mi következett ebből, hova vezetett ez a folyamat? A kereskedelem, különösen a kiskereskedelem üzletkötései először megjelentek, majd tömegessé váltak az interneten. Mindez növelte a távollévők között kötött szerződések [4] hányadát a polgári jogi jogviszonyokban. Bár a távollévők között kötött szerződések a polgári jog immanens részét képezték korábban is, gondoljunk csak a telesales módon kötött szerződésekre, ugyanakkor felmerült az igény a tömeges, és egyre inkább elterjedő internetes vásárlások polgári jogi szabályozására.

A távollévők között az interneten keresztül megvalósult és kötött tömeges ügyletekből az következett, hogy megjelent az igény az általános szerződési feltételek [5] szabályozásának változtatására is, valamint megjelentek az első adatbázisok, melyek léte átalakította a marketinget, a gazdasági reklámtevékenységet, az értékesítés folyamatát.

Mindezek együtt értelemszerűen életre hívták a közösségi jogalkotás feladatát, hiszen az Európai Unió alapszerződésekben kiindulva, élve a termékek és a munkaerő szabad áramlásával, az értékesítések egyre inkább tagállamköziek lettek. [6] A digitális területen keletkezett első közösségi jogi jogszabály tehát a kereskedelem életviszonyait megváltoztató interneten keresztül zajló értékesítést állította a fókuszába és a címe röviden elektronikus kereskedelemről szóló irányelv lett (az Európai Parlament és a Tanács 2000/31/EK

irányelve a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól, a továbbiakban: e-kereskedelmi irányelv). Ez az irányelv a tömeges internethasználatból eredő egyes kihívásokra kívánt reagálni, ezzel biztosítva az egységes belső piac működését. Fontosabb rendelkezései közül kiemelendő a „származási ország elve", valamint az értesítési-eltávolítási rendszer, mint jogellenes online tartalmakra vonatkozó alapvető szabály. [7]

Az irányelvet az Európai Unió Parlamentje és Tanácsa 2000-ben bocsátotta ki, és jól nyomon követhető, hogy kettőezerben milyen digitális kihívásokra kellett válaszolnia, fókuszálnia a jogalkotónak. Nyoma sem volt ebben az időszakban az adatvédelem fontosságának, az interneten való visszaélésekkel szembeni fellépésnek, könnyen beátható, hogy a világ és benne az Európai Unió még nem tartott ott, ahol ma. Léteztek adatbázisok (amit szabályoztak is a tagállami jogalkotók), de nem volt tagállamokon átnyúló jellegük, létezett gyűlöletbeszéd, ami az interneten keresztül valósult meg de még nem érte el azt a volument, amit ma és nem volt feltétlenül tagállamközi jellege.

Az irányelv létrehozásának fő igényként a jogalkotó legfőképpen a belső piac működésének hatékonyabb biztosítását jelölte meg, lásd az irányelv célkitűzéseinek 5. cikkelyét mely így szól:

„(5) Az információs társadalommal összefüggő szolgáltatások fejlődését a Közösségben a belső piac megfelelő működésének számos jogi akadálya nehezíti, amelyek eredményeként kevésbé vonzó a letelepedés és a szolgáltatásnyújtás szabadságának gyakorlása; ezek az akadályok a jogi szabályozás eltéréseiből fakadnak, valamint a jogbiztonság hiányából azzal kapcsolatban, hogy mely nemzeti szabályok vonatkoznak az ilyen szolgáltatásokra; amíg az érintett területeken nem valósul meg a jogszabályok összehangolása és kiigazítása, az akadályok indokoltak lehetnek az Európai Közösségek Bírósága esetjogának tükrében; hiányzik a jogbiztonság abban a tekintetben, hogy a tagállamok milyen mértékben ellenőrizhetnek más tagállamból származó szolgáltatásokat."

A magyar országgyűlés az irányelvet az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvénnyel ültette át a magyar jogrendbe, és ezt a törvényt is módosítva, valamint egy új törvényt elfogadva [8] emelte be a DSA rendelet egyes elemeit. Megjegyzendő emellett, hogy a DSA az e-kereskedelmi irányelv módosítása is egyben.

A 2000-es évek közepétől, majd a 2010-es évek elejétől a technológia gyorsulásával együtt a közösségi jogalkotás üteme is felgyorsult, és más irányt vett a korábbiakhoz képest. Más kihívások, más életviszonyok vezettek ahhoz, hogy a 2010-es évek derekán megszületett az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről, azaz általános adatvédelmi rendelet, (a továbbiakban: GDPR), és ezt követték a mai kor problémáira válaszokat kereső az Európai Parlament és a Tanács (EU) 2022/1925 rendelete (2022. szeptember 14.) a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (digitális piacokról szóló jogszabály) (a továbbiakban: DMA) és az Európai Parlament és a Tanács 2022. október 19-i (EU) 2022/2065 rendelete a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet) (a további-

akban: DSA) rendeletek, valamint a kibervédelemmel összefüggésben az Európai Parlament és a Tanács 2019/881 rendelete az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (a továbbiakban: Cybersecurity Act) vagy az Európai Parlament és a Tanács 2024/1689 RENDELETE a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a továbbiakban: MI rendelet).

Remekül nyomon követhető a közösségi jogalkotás alapján a világ technológiai megváltozásának felgyorsulása. Míg a 2000-es irányelv a belső piac akadályainak lebontását célozta, ma már az EU jogalkotási célkitűzései gyökeresen eltérnek ettől, hiszen ma már az a feladat, hogy a technológiai versenyt kiegyenlítsék, a fogyasztókat, különösen a gyermekeket megvédjék, és a különböző dezinformációs veszélyeket mérsékeljék. Az, hogy ez milyen sikerrel jár arra az elkövetkezendő évek fogják megadni a választ.

Az elmúlt években a digitalizáció, valamint a digitális biztonság megteremtése kiemelt jelentőségű programja volt az Európai Uniónak. Ahogyan azt látni fogjuk, az EU számos területen igyekezett és igyekszik ennek kereteit megteremteni. A digitális biztonsággal összefüggő kihívásokat felismerve az Európai Parlament és a Tanács 2022-ben egy határozattal döntött egy olyan szakpolitikai program létrehozásáról, amely mind az uniós polgárok, mind pedig a vállalkozások jólétét hivatott előmozdítani. [9] Ez a program számos olyan általános célkitűzést tartalmaz, amelyet az EU 2030-ig meg kíván valósítani, így egyebek mellett egy átlátható és inkluzív digitális környezet megteremtését, a tagállamok kollektív rezilienciájának megerősítését, a digitális különbségek áthidalását, valamint a szabályozási környezet olyan irányba terelését, amely hozzájárul a kis- és középvállalkozások tisztességes versenyben való részvételéhez. [10] Lényeges részét képezi mind a szakpolitikai programnak, mind pedig az EU stratégiáinak az online platformok, online közösségi terek megfelelő szintű szabályozása is, valamint nem utolsó sorban az egyre inkább népszerűvé váló, ugyanakkor meglehetősen alulszabályozott mesterséges intelligencia alkalmazásának keretek közé szorítása is.

Ahogyan azt láthattuk már az említett szakpolitikai programot megelőzően is elindult egy olyan jogalkotási folyamat az EU-ban, amely a digitalizációval és az online platformokkal összefüggő egyes kihívásokra kíván reagálni részben a tagállamokra bízva a szabályozás részletes megteremtését, részben pedig tőlük függetlenül, rendeleti szinten egységesen szabályozva azt. Ezen törekvések és szabályozási kezdeményezések több szakpolitikát fognak át, így külön szakpolitikaként tartják számon például a mesterséges intelligenciát, a kiberbiztonságot, a digitális szolgáltatásokat, valamint az adatgazdaságot is. [11]

Addig is, bár az MI rendelet, a GDPR rendelet vagy a Cybersecurity Act kifejtése, vagy ezeknek a DSA-val, illetve a DMA-val való kapcsolata jelentősen meghaladná jelen tanulmány kereteit, röviden bemutatjuk a fentiek célkitűzéseit. Tanulmányunkban ugyanakkor a DSA és a DMA rendeletek rövid, gyakorlati bemutatásán kívül a fentiekre csak hivatkozunk, fentiek mélyebb összefüggéseinek feltárására e tanulmány keretei között nincs lehetőség.

Jogszabályok	Célok röviden
e-kereskedelmi irányelv	belső piaci akadályok lebontása, áruk és szolgáltatások tagállami határokon átnyúló mozgásának biztosítása
DSA	fogyasztók védelme, kisebb platformok szabályozása, kkv-k és induló, start-up vállalkozások növekedésének, terjeszkedésének elősegítése
DMA	tisztességes piaci környezet megteremtése, innovátorok előtt új lehetőségek megnyitása, fogyasztók számára szélesebb körű választási lehetőségek megnyitása, valamint a szolgáltatások tekintetében, kapuőrök szabályozása
GDPR	adatkezelési tevékenységek tekintetében a természetes személyek alapvető jogainak és szabadságainak védelme, valamint annak biztosítása, hogy a személyes adatok tagállamok közötti szabadon áramolhassanak
MI rendelet	mesterséges intelligencia kockázatainak kezelése, valamint kkv-k és induló vállalkozások költségeinek csökkentése
Cybersecurity Act	az ENISA szervezetének megerősítése, átalakítása, valamint egy európai kiberbiztonsági tanúsítási keretrendszer létrehozása

1.táblázat: Az egyes EU-s szabályok céljai röviden

AZ UNIÓS SZINTŰ SZABÁLYOZÁS ÉS A VÁLASZTOTT JOGFORRÁS OKA

Tekintettel az EU sajátos helyzetére, valamint a szabályozás szupranacionális jellegére, hangsúlyt kell fektetnünk annak vizsgálatára is, hogy milyen szabályozási módot vá-

laszt az EU az egyes kérdések tisztázása és a jogharmonizáció biztosítása tekintetében. Ahogyan arra már korábban rámutattunk a 2000-es évek elején egy irányelvvel kívánta az Uniós jogalkotó elektronikus kereskedelmet szabályozni, ma a digitális biztonság megteremtésére, valamint a digitális Európa előmozdítása érdekében hozott jogszabályok döntő többsége rendeleti formában történik. A jogszabályalkotás megértése érdekében lényeges tisztázni azt, hogy az EU milyen esetekben és hogyan alkothat a tagállamokra is kötelező jogszabályt.

A hatáskör-átruházás elvének figyelembe vételével az Európai Unió szervei által alkotott jogszabályok az ún. másodlagos uniós jogforrások. Jelen tanulmány szempontjából a jogforrások közül az irányelv és a rendelet bírnak döntő jelentőséggel. A két jogszabály közötti különbség abban áll, hogy míg az irányelv a tagállam jogalkotása tekintetében fogalmaz meg egy iránymutatást, amely alapján a jogalkotónak az irányelv szabályai mentén kell eljárnia (és jogszabályt alkotnia), addig a rendelet minden külön aktus nélkül is kötelezővé és ezáltal alkalmazhatóvá valamennyi tagállamban. Ellentétben a nemzetközi szerződések, egyezmények szabályaival ezek a jogforrások azonban nem válnak a belső jogrendszer részévé, hanem egy, a tagállamok felett álló jogrendszert hoznak létre, amely kötelezően alkalmazandóvá válik valamennyi Uniós tagállamban. [12] [13]

A tanulmány alapjául szolgáló két jogszabály (a DSA és a DMA) rendeleti szinten történő szabályozása egyértelműen arra vezethető vissza, hogy az Uniós jogalkotó maga kívánta meghatározni az online, digitális világ ezen szabályozási kereteit. Tekintettel arra, hogy hatáskör-átruházás elve alapján az EU alkothat közvetlenül a tagállamokban alkalmazandó rendeletet a tárgyban, hiszen olyan új jogterületről van szó, amelyre – figyelembe véve a szubszidiaritás elvét is – a tagállamokon felüli jogalkotásra lehet szükség (hiszen a digitális piac nincs tekintettel a tagállami határokra). A rendeletalkotás természetesen nem működhet külön felhatalmazás nélkül hiszen az Európai Unió szervei csak és kizárólag az EUMSz. rendelkezéseinek megfelelően alkothatnak a tagállamokra kötelező jogszabályokat. A DSA preambuluma ennek körében utal az EUMSz. 114. cikkére, amely rendelkezései szerint a 26. cikkben foglalt – a belső piac megteremtésével és fenntartásával összefüggő – célkitűzések megvalósítása érdekében az Európai Parlament és a Tanács rendeletalkotási jogkörébe tartozik a DSA megalkotása is. Hasonló rendelkezést találhatunk a DMA preambulumában, hiszen ez a rendelet is a belső piac biztonságos és a tisztességes verseny követelményének való megfelelést szolgálja.

AZ EURÓPAI UNIÓ ÚJ, DIGITÁLIS VILÁGOT SZABÁLYOZÓ NORMÁI, AZAZ A DMA ÉS A DSA RÖVID BEMUTATÁSA

Amint láthattuk az EU a digitális társadalom megteremtése érdekében számos területen alkot jogszabályokat, standardokat. A jelen tanulmány célja, hogy bemutassa azokat a lényegesebb szabályokat, amelyek a kis- és középvállalkozások, valamint az induló, start-up vállalkozások szempontjából kiemelkedő jelentőségűek. Természetesen ez nem azt jelenti, hogy a fentebb bemutatott további jogszabályok - így kifejezetten a kiberbiztonsági szakpolitika, vagy éppen az adatgazdasági szakpolitika keretén belül alkotott szabályok - ne tartalmaznának előírásokat a vállalkozások vonatkozásában. Ugyanakkor a két jogszabály, jelesen a DMA és a DSA olyan, közérdeklődésre is számot tartó, jelentős újítást hozó szabályok, amelyek nagy hatást gyakorolnak az említett vállalkozások piacra lépésére, valamint a versenyben való részvételük biztosítására. Ezek a rendeletek más jogszabályok mellett egy digitális jogszabály-csomag részét képezik, melynek fő célja egy biztonságos

digitális tér megteremtése és egyenlő versenyfeltételek biztosítása [14], egy biztonságos online, digitális tér megteremtése, ahol egyfelől védelemben részesülnek a felhasználók alapvető jogai, másrészt a versenyjogi szempontból egyenlő feltételeket teremtenek az innovációban és növekedésben a vállalkozások számára. [15] Bár a két jogszabály eltérő logikával szabályozza részben ugyanazokat a jogalanyokat, részben eltérőeket, a két rendelet értelmezése csak részben képzelhető el a másik nélkül.

A digitális piacokról szóló rendelet célja, lényeges fogalmai

Elsőként az Európai Parlament és a Tanács 2022/1925. rendeletével, ismertebb nevén a digitális piacokról szóló jogszabállyal (továbbiakban: DMA) foglalkozunk. Az EU felismeri és elfogadja azt, hogy a digitális szolgáltatások és hozzájuk kapcsolódva az online platformok lényeges szerepet töltenek be mind a felhasználók, mind a vállalkozások tekintetében a belső piacon, ugyanakkor rámutat arra, hogy milyen árnyoldalai, hátrányai lehetnek ezeknek a közegeknek. Így magában a rendeletben is utal a jogalkotó az online platformok adta lehetőségek eltérő kihasználására, valamint az egyes, nagy versenyelőnyre szert tett vállalkozások létére. [16] E körben említi meg először azt a kulcsfogalmat is, amely az egész jogszabályt áthatja, nevezetesen a kapuőrt. A kapuőr az a vállalkozás, amelyet egyfelől a DMA 3. cikk értelmében ennek minősítenek és alapvető platformszolgáltatást nyújt. [17] E fogalom kapcsán tehát két további kérdést szükséges tisztáznunk. Egyrészt azt, hogy mely esetekben minősítenek egy vállalkozást kapuőrnek, másrészt pedig, hogy mely szolgáltatások minősülnek alapvető platformszolgáltatásoknak.

Kapuőrré akkor válik egy vállalkozás, amennyiben (1) jelentős hatást gyakorol a belső piacra, (2) olyan alapvető platformszolgáltatást nyújt, amely kapuként szolgál az üzleti felhasználóknak ahhoz, hogy elérjék a végfelhasználóikat, valamint (3) tartós pozíciót élvez a működése során vagy várhatóan ilyen pozícióra tesz szert. A DMA 3. cikke nem csupán ezeket a kritériumokat határozza meg a kapuőrök minősítése vonatkozásában, hanem olyan feltételeket is felsorol, amelyek esetében vélelmezi, hogy a feltételeknek megfelelő szolgáltatás kapuőrnek minősül. Ilyen vélelem áll fenn abban az esetben, hogyha a vállalkozás az Unióban legalább 7,5 milliárd euró éves forgalmat bonyolított le az elmúlt három pénzügyi év mindegyikében. [18]

A másik tisztázandó kérdés vonatkozásában a DMA fogalommeghatározások keretében lefektetett rendelkezése keretében taxatíve tartalmazza azokat a szolgáltatásokat, amelyek az alapvető platformszolgáltatások körébe tartoznak. Ilyen szolgáltatásnak minősülnek többek között az online közvetítő szolgáltatás - amelyekről még később a digitális szolgáltatásokról szóló rendelet keretén belül szó lesz -, az online keresőprogram, közösségi hálózati szolgáltatás vagy a webböngésző. [19]

Ahogyan arra már utaltunk, a 3. cikkben foglalt feltételek megvalósulása esetén ennek tényét a vállalkozásnak két hónapon belül jeleznie kell a Bizottság felé. Ebből is látszik, hogy a rendelet szabályainak végrehajtása az Európai Bizottság feladata. A Bizottság hivatott arra is, hogy az egyes szolgáltatókat kapuőrnek minősítse a DMA 4. cikke alapján. [20]

A DMA megalkotásának hátterében tehát az az elképzelés áll, miszerint a kapuőrök lényegesen jobb alkupozícióban vannak a többi, hasonló szolgáltatást nyújtó vállalkozással szemben, s ezt a pozíciójukat közvetett vagy közvetlen eszközökkel fel is használják. [21] A DMA célja egy versenyképes és tisztességes digitális környezet, piac kialakítása, amely

keretében teret biztosít az innovatív vállalkozások növekedéséhez és biztosítja a felhasználók biztonságát is. [22]

A digitális szolgáltatásokról szóló rendelet célja, lényeges fogalmai

A korábban hivatkozott jogszabály-csomag másik lényeges eleme az Európai Parlament és a Tanács (EU) 2022/2065 rendelete, ismertebb nevén a digitális szolgáltatásokról szóló rendelet (a továbbiakban: DSA). Az új szabályozás szükségessége abban keresendő - ahogyan arra maga az EU is rámutatott -, hogy a már említett Eker. irányelv által lefektetett jogszabályi keretek már nem tudják kezelni azokat a kihívásokat, amelyek az elmúlt években megjelentek. Ilyen kihívásoknak bizonyultak az új és innovatív üzleti megoldások, az online kereskedelem még széleskörűbbé válása, valamint az online platformok napi szintű használata. [23] Ezen utóbbi kihívásban nagy szerepet játszanak a ma legnagyobbnak számító online platformok, a közösségi média platformok. Egy friss, 2024 júliusában készült felmérés alapján világszerte 5,17 milliárd közösségi média felhasználó van, amely a teljes populáció 63,7 százalékát teszi ki. Ezek a platformok ma már nem csak kapcsolattartásra, hanem kereskedelmi és marketing tevékenységre is használhatók. Ennek a tevékenységnek a jelentőségét jól mutatja, hogy a YouTube legutóbbi jelentése alapján 2,50 milliárd felhasználót érnek el reklámokkal havonta. [24]

A DSA egyik célja ezen digitális platformok működési alapelveinek megváltoztatása, a felhasználói jogok szélesítése, illetve a jogellenes tartalmakkal szembeni küzdelem az által, hogy a közvetítő szolgáltatók felelősségét növeli. [25] Ennek oka, hogy a közvetítő szolgáltatók által nyújtott szolgáltatások - amelyeket a későbbiekben bővebben is kifejtünk - exponenciális növekedése miatt ezen szolgáltatók szerepe egyre növekszik a jogellenes és káros tartalmak közvetítésében, tárolásában és terjesztésében. [26] Ahhoz, hogy eligazodjunk a DSA szabályai között az egyik legfontosabb kérdés, hogy ki minősül közvetítő szolgáltatónak és milyen szolgáltatásokat nyújtanak ők?

A DSA közvetítő szolgáltatásnak minősít három szolgáltatást, amelyek szorosan kapcsolódnak az információs társadalomhoz. Ezek (1) az egyszerű továbbítás, (2) a gyorsítótárazás, (3) a tárhelyszolgáltatás. Egyszerű továbbításról abban az esetben beszélhetünk, amennyiben a szolgáltatás lényege abban áll, hogy az igénybe vevő által küldött információt a szolgáltató továbbítja, valamint ahhoz hozzáférést biztosít hírközlő hálózaton keresztül. A gyorsítótárazás is részben az igénybe vevő által küldött információk továbbításából áll, ugyanakkor ez együtt jár ezen információ automatikus, közbenső, átmeneti tárolásával annak érdekében, hogy a szolgáltatás igénybevételének hatékonysága növekedhessen. Végül a tárhelyszolgáltatás pedig az egyes információk tárolására vonatkozik. [27] Az Európai Unió Bírósága több kérdéses ügyben is vizsgálta, hogy mely szolgáltatások tartoznak a tárhelyszolgáltatások közé. Így került megállapításra többek között az is, hogy a hirdetési szolgáltatások, az online piacterek, valamint az online közösségi platformok egyaránt adattárolási tevékenységet végeznek, így tárhelyszolgáltatónak minősülnek. [28]

A rendelet felépítését figyelembe véve az EU mindhárom közvetítő szolgáltatás vonatkozásában megállapít felelősségi szabályokat. Ezekben a rendelkezésekben a jogalkotó nem taxatív felsorolás alkalmazásával határozza meg azokat a körülményeket, amelyek fennállása esetén megállapítható a közvetítő szolgáltató felelőssége, hanem kivétel szabállyal rendelkezik minden olyan körülményről, amely esetben nem áll fenn a szolgáltató felelőssége. [29] Mindez joglogikai értelmezés alapján - *argumentum a contrario* - azt jelenti,

hogy a rendelkezésekben fel nem sorolt esetekben megállapítható a közvetítő szolgáltató felelőssége, ezzel elősegítve - többek között - egy biztonságos, kiszámítható és megbízható online környezet elősegítését. [30]

A DSA felelősségi szabályainak megértéséhez elengedhetetlen a jogellenes tartalom definiálása. A rendelet jogellenes tartalomnak minősít bármely információt, amely akár önmagában, akár egy tevékenységgel - ideértve a termékek értékesítését és szolgáltatások nyújtását - kapcsolatban nem felel meg az uniós jognak, vagy bármely tagállam jogának. [31] A DSA tehát nagyon széleskörűen értelmezi a jogellenes tartalom fogalmát, így nem csupán az uniós jogba, hanem bármely tagállam jogába ütköző tartalmat ekként minősíti, függetlenül az érintett jog tárgyától és jellegétől.

Éppen a fentiek miatt, jelesen az elvont, absztrakt fogalmi definíciók okán megnő a tagállami és EU bíróságok, illetve különböző más hatóságok jogértelmezési lehetősége és a jogértelmezés jelentősége. Végső soron a definíciók valódi, gyakorlati jelentőségét (és egyúttal a gyakorlati jelentéstartalmát) a joggyakorlat, a bírósági és a hatósági határozatok fogják kimunkálni.

ÚJ, VÁLLALKOZÁSOKAT ÉRINTŐ SZABÁLYOK

A DSA fentebb ismertetett szabályaiból jól látszik, hogy az EU bővíteni kívánta a közvetítő szolgáltatók felelősségét az általuk kezelt, tárolt, továbbított jogellenes tartalom vonatkozásában. Emellett viszont fontosnak tartjuk azt is megemlíteni, hogy ezen általános szabályok mellett olyan konkrét kötelezettségeket is előír ez a szabályozás, amelyek számos kis- és középvállalkozást érintenek. Ez azt jelenti, hogy például a tárhelyszolgáltatók - és köztük az online platformok - számára kötelező az olyan mechanizmus alkalmazása, amely lehetővé teszi, hogy bárki - legyen az személy vagy szervezet - konkrét információkat tudjon bejelenteni a szerinte jogellenesnek minősülő tartalommal kapcsolatban. [32] Ezen rendelkezés kapcsán lényeges megemlíteni az Ekertv. által szabályozott értesítési-eltávolítási kötelezettséget, amelyet Magyarország akképpen implementált, hogy a szerzői jogi igények és kiskorúak személyiségi jogát érintő esetekben van lehetőség ilyen eljárás kezdeményezésére a tárhelyszolgáltatónál. A DSA bejelentési mechanizmusa nem helyettesíti, sokkal inkább kibővíti a tárhelyszolgáltatónál indítható eltávolítási eljárások körét. [33]

Ezeknek a bejelentési mechanizmusoknak felhasználóbarátnak és hozzáférhetőnek kell lenniük, amely követelményekkel kapcsolatban a 16. cikkben további feltételeket határoz meg a rendelet, így egyebek mellett biztosítani kell azt is, hogy a bejelentés során a magánszemély vagy szervezet kellően részletesen elmagyarázza, hogy szerinte miért jogellenes a bejelentett tartalom. [34] Amennyiben a tárhelyszolgáltató megállapítja, hogy a bejelentés alapjául szolgáló tartalom jogellenes vagy beleütközik az általa megállapított szerződési feltételekbe, úgy egy konkrét és egyértelmű indokolás mellett lehetősége van dönteni különféle korlátozások alkalmazásáról. Ilyen korlátozásnak minősül a láthatóság korlátozása, ezen belül is a tartalom eltávolítása és a hozzáférés megszüntetése, emellett a szolgáltatásnyújtás teljes vagy részleges felfüggesztése, illetve a pénzkifizetések felfüggesztése, korlátozása. [35] Az említett indokolási kötelezettséggel kapcsolatban további részletszabályokat is tartalmaz a rendelet.

A bejelentési rendszer mellett lényeges röviden szót ejteni a bűncselekmények gyanújának bejelentéséről is, amely szintén egy többlet kötelezettséget ró a tárhelyszolgáltatókra. Amennyiben ugyanis a tárhelyszolgáltató tudomást szerez olyan információról,

amely alapján felmerül a gyanú, hogy mások életét és biztonságát veszélyeztető bűncselekményt követtek el, követnek el, vagy fognak elkövetni, úgy haladéktalanul jeleznie kell ezt az érintett tagállam bűnüldözési vagy igazságügyi hatósága felé, s e körben a hatóságok rendelkezésére kell bocsátania minden, az ügyben releváns információt. [36]

A DSA az egyes, online platformot üzemeltető szolgáltatókra vonatkozó szabályok közül kiemeli a mikro- és kisvállalkozásokat, így rájuk csupán a fent ismertetett bejelentési mechanizmus fenntartása válik kötelezővé. Ezen kivétel alkivételeként szabályozza a rendelet az óriásplatformnak minősített szolgáltatót, amelyre a vállalkozás méretétől függetlenül alkalmazandók a többletkötelezettségek. [37] Ezek a többletkötelezettségek többek között egy belső panaszkezelési rendszer fenntartására, a peren kívüli vitarendezés szabályaira, valamint a megbízható bejelentőkre vonatkoznak. [38]

EDDIGI EREDMÉNYEK, JOGGYAKORLAT

Ebben a fejezetben kitérünk azokra a kézzel fogható eredményekre, amelyek az új szabályok hatályba lépését követően realizálódtak, így például a TikTok-kal szemben indított eljárás a DSA szabályainak megsértése miatt, valamint a DMA-val összefüggésben indított eljárások.

Nagyon fontos, a helyzet megértését segítő körülmény, hogy a DSA és a DMA fogalomrendszerének nagyobbik része nem ismeretlen az európai közösségi jog számára, hiszen az Európai Bíróság (a továbbiakban: EUB) számtalan ítéletében kimunkálta már ezeket a fogalmakat, így egyebek mellett a tárhelyszolgáltatás fogalmát is.

A tárhelyszolgáltatás esetében a L'Oreal/eBay (C-324/09.) ügyben az EUB szerint „*az online piacot illetően nem vitatott, hogy az eBay tárolja, azaz a szerverének memóriájában elhelyezi az ügyfelei által szolgáltatott adatokat. Az eBay e tárolást minden egyes alkalommal elvégzi, amikor egy ügyfél eladói profilt hoz létre nála, és adatokat szolgáltat az eladásra való felkínálásairól*", azaz az eBay (vagy analógia alapján más hasonló piacterek), amit nem feltétlenül tárhelyszolgáltatóként ismerünk, a DSA szempontjából igenis tárhelyszolgáltatóknak minősülnek figyelemmel az EUB korábbi döntéseiben foglaltakra. [39]

Lényeges döntésnek minősül emellett az EUB Airbnb Ireland ügyben (C-390/18.) hozott ítélete. Tekintettel arra, hogy „*a bérbeadókat és bérlőket összekapcsoló elektronikus platform megfelel az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltatók fogalmának, és közvetítő szolgáltatónak minősíthető, mivel a platformon nyújtott szolgáltatás elválasztható a bérléstől."* Mindez tulajdonképpen azt jelenti, hogy a két szolgáltatás azért különböző – az EUB gyakorlata szerint –, mert maga a kínált szolgáltatás nem a szálláshely-szolgáltatás megvalósítására irányult, hanem arra, hogy a szálláskeresők részére meghatározott kritériumoknak megfelelően egy listát állítson össze ezzel is megkönnyítve a későbbi szerződéskötéseket. [40]

Fontos eredménynek tartjuk azt is, hogy Magyarországon megkezdte a munkáját az Online Platform Vitarendező Tanács (a továbbiakban: OPVT). Az OPVT a DSA 21. cikke alapján létrehozott tagállami vitarendező platform. Nem hatóság, nem a közigazgatás formális logikája alapján működik. A Tanács ajánlást tesz közzé az eljárás végén vagy elutasítja a panaszt. [41] A Tanács munkájától azt várhatjuk, hogy intézményesíti és meggyorsítja az online panaszokkal kapcsolatos vitarendezést, kiegészíti a joggyakorlatot, melyet a tagállami bíróságok és az EUB alakít ki véglegesen.

A DSA hatályba lépésétől kezdve egy új világ köszöntött be az online óriásplatformok életében. Habár alig egy éve lépett hatályba ez az új szabályozás, néhány hónapon belül a Bizottság eljárást indított a TikTok óriás videómegosztó közösségi platform ellen. Az eljárás oka, hogy a TikTok egy TikTok Lite applikációt tett elérhetővé a felhasználói számára Franciaországban és Spanyolországban. Tekintettel a DSA online óriásplatformokra vonatkozó szabályaira, ezen platform tekintetében is egy kockázatértékelési jelentést kellett volna benyújtani, amely tartalmazza az esetleges rendszerkockázatok csökkentésére irányuló intézkedéseket, figyelemmel arra, hogy olyan új funkciókat – így egyfajta jutalomrendszert – építettek a felületbe, amely káros hatást gyakorolhat a felhasználókra. [42] Az eljárást a Bizottság folytatja le, amely jogosult ideiglenes intézkedések megtételére és a megfelelés hiányáról szóló határozatok meghozatalára. Az eljárást a Bizottság 2024 áprilisában lezárta, amelyet követően a TikTok – egyetértve a Bizottság döntésével – véglegesen kivonta a TikTok Lite verziót az EU piacáról. Az eljárásról hozott döntés 2024 augusztusában emelkedett jogerőre. [43] Ebből is jól látható, hogy az óriásplatformok – tartva az 52. cikkben meghatározott szigorú szankcióktól – akár önkéntesen is kiküszöbölik a Bizottság elé került szabálysértéseket.

KILÁTÁSOK, HELYZETÉRTÉKELÉS

Nem utaltunk dolgozatunkban több, a digitális világ normarendszerbeli leképeződésére, lásd pl. a fintech szabályok bevezetésére (MiCAR), hiszen a kérdés jelentősen túlnőtte az egy rövidebb tanulmányban felölelhető szabályozás körét. Ugyanakkor azt nagyon fontos rögzíteni, hogy jelenleg egy – eddig – huszonötéves folyamatnak a kellős közepén vagyunk. Több jelentős és huszonöt-harminc éve nem létező jogviszony szabályozására sor került, mégis az EU még előtte áll lényeges jogviszonyok normarendszerbeli jelentőségének, helyének kidolgozásának. Nem pusztán jogalkotásra kell gondolni, de jelentősége van a tagállami és az EUB gyakorlatának is abban a tekintetben, hogy egy-egy jogintézmény milyen módon gyökeresedik meg a normák között, hogy milyen helyet foglal el az életviszonyok szabályozásában, illetve a technológia sebessége magával hozza a további szabályozási igényeket (lásd egyebek mellett a mesterséges intelligencia egyre kiterjedtebb szabályozása).

Hogy az EU-nak sikerül-e a kívánt céljait a jelenlegi jogszabályokkal úgy elérnie, mint huszonnégy éve az elektronikus kereskedelem esetén a belső piac védelmét célzó e-kereskedelmi irányelvvel, fogas kérdés, de az elkövetkezendő években folyamatosan láthatjuk kirajzolódni a választ.

FELHASZNÁLT IRODALOM

[1] Az Európai Parlament és a Tanács 2000/31/EK irányelve (2000. június 8.) a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem, egyes jogi vonatkozásairól (Elektronikus kereskedelemről szóló irányelv).

[2] J. T. PAPP, A közösségi média platformok szabályozása a demokratikus nyilvánosság védelmében, Budapest: Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Doktori Iskola, 2021.

[3] T. KLEIN, „Az elektronikus kereskedelmi szolgáltatás, mint platformszolgáltatás,” in KLEIN, Tamás; TÓTH, András (szerk.) Technológia jog - Robotjog - Cyberjog , Budapest, Wolters Kluwer Kft., 2018.
[4] G. WELLMANN, Polgári Jog I-IV. - új Ptk. - Kommentár a gyakorlat számára., Budapest: ORAC Kiadó Kft., 2024.
[5] A Polgári Törvénykönyvről szóló 2013. évi V. törvény 6:77.§ (1) bekezdés.
[6] Az Európai Unió működéséről szóló szerződés IV. cím.
[7] J. T. PAPP, „1. cikk. Tárgy.,” in KOLTAY, András; SZIKORA, Tamás; LAPSÁNSZKY, András; TÓTH, András (szerk.): Nagykommentár a DSA rendelethez, Budapest, Wolters Kluwer Kft., 2024, p. 11.
[8] Az internetes közvetítő szolgáltatások egyes szabályairól szóló 2023. évi CIV. törvény.
[9] Az Európai Parlament és a Tanács (EU) 2022/2481 határozata 3. cikk (1) bekezdés.
[10] Az Európai Parlament és a Tanács (EU) 2022/2481 határozata 3. cikk (1) bekezdés.
[11] „Európa digitális jövője,” [Online]. Available: https://tinyurl.com/3ayavt3u.
[12] M. PAPP és E. VÁRNAY, Az Európai Unió joga, Budapest: Wolters Kluwer Kft., 2017.
[13] K. GOMBOS, Európai jog - Az Európai Unió jogrendszere, Budapest: Wolters Kluwer Kft., 2020.
[14] „A digitális szolgáltatásokról szóló jogszabálycsomag.,” [Online]. Available: https://tinyurl.com/mwwcns6v.
[15] K. GOMBOS, „A Digital Services Act és a Digital Markets Act várható kihívásai a jogalkalmazásban,” In Medias Res, %1. kötet2, p. 94, 2023.
[16] DMA (1)-(3) preambulumbekezdések.
[17] DMA 2. cikk 1. pont.
[18] DMA 3. cikk.
[19] DMA 2. cikk 2. pont.
[20] DMA 4. cikk.
[21] F. BOSTOEN, „Understanding the Digital Markets Act,” Antitrust Bulletin, %1. kötet68(2), p. 266, 2023.
[22] „A digitális piacokról szóló jogszabály.,” [Online]. Available: https://tinyurl.com/yv37ha2b.
[23] DSA (1) preambulumbekezdés.
[24] „Global Social Media Statistics,” [Online]. Available: https://tinyurl.com/53uk6vdp.
[25] J. T. PAPP, „1. cikk. Tárgy.,” in KOLTAY, András; SZIKORA, Tamás; LAPSÁNSZKY, András; TÓTH, András (szerk.): Nagykommentár a DSA rendelethez, Budapest, Wolters Kluwer Kft., 2024, p. 12.
[26] DSA (5) preambulumbekezdés.
[27] DSA 3. cikk g) pont.
[28] T. SZIKORA, „3. cikk. Fogalommeghatározások.,” in KOLTAY, András; SZIKORA, Tamás; LAPSÁNSZKY, András; TÓTH, András (szerk.): Nagykommentár a DSA rendelethez, Budapest, Wolters Kluwer Kft., 2024, p. 24.
[29] DSA 4., 5. és 6. cikkek.
[30] DSA 1. cikk (1) bekezdés.
[31] DSA 3. cikk h) pont.
[32] DSA 16. cikk (1) bekezdés.

[33] G. F. LENDVAI, „16. cikk. Bejelentési és cselekvési mechanizmusok.,” in KOLTAY, András; SZIKORA, Tamás; LAPSÁNSZKY, András; TÓTH, András (szerk.): Nagykommentár a DSA rendelethez, Budapest, Wolters Kluwer Kft., 2024, p. 76.
[34] DSA 16. cikk (2) bekezdés.
[35] DSA 17. cikk (1) bekezdés.
[36] DSA 18. cikk.
[37] DSA 19. cikk (2) bekezdés.
[38] DSA 20., 21. és 22. cikkek.
[39] J. T. PAPP, „3. cikk. Fogalommeghatározások.,” in KOLTAY, András; SZIKORA, Tamás; LAPSÁNSZKY, András; TÓTH, András (szerk.): Nagykommentár a DSA rendelethez, Budapest, Wolters Kluwer Kft., 2024, pp. 23-24.
[40] J. T. PAPP, „2. cikk. Hatály.,” in KOLTAY, András; SZIKORA, Tamás; LAPSÁNSZKY, András; TÓTH, András (szerk.): Nagykommentár a DSA rendelethez, Budapest, Wolters Kluwer Kft., 2024, p. 15.
[41] „Mi történik az Online Platform Vitarendező Tanácshoz benyújtott kérelemmel? Milyen döntés várható?,” [Online]. Available: https://tinyurl.com/ztz5ja8z.
[42] „Commission opens proceedings against TikTok under the DSA regarding the launch of TikTok Lite in France and Spain, and communicates its intention to suspend the reward programme in the EU,” [Online]. Available: https://tinyurl.com/2c6485jt.
[43] „European Union: TikTok Agrees with Commission to Withdraw Rewards Program,” [Online]. Available: https://tinyurl.com/2x25kfue.
[44] Az Európai Parlament és a Tanács (EU) 2022/2481 határozata a Digitális évtized 2030 szakpolitikai program létrehozásáról.
[45] N. CHRONOWSKI, „Az Európai Unió jogának viszonya a magyar joggal,” [Online]. Available: https://tinyurl.com/yc3wmtt5.

PREVAIL OF SAFETY REQUIREMENTS FOR EXPLOSIVE INDUSTRIAL TECHNOLOGIES IN PRACTICE

ROBBANÁSVESZÉLYES IPARI TECHNOLÓGIÁK BIZTONSÁGI KÖVETELMÉNYEINEK ÉRVÉNYESÜLÉSE A GYAKORLATBAN

ZSARNOVSZKI Attila[1] – ELEK Barbara[2]

Abstract

Industrial production processes often result in potentially explosive areas. While the safety requirements for explosion protection are laid down in binding directives for the Member States of the European Union and the means to achieve these objectives are developed by the national authorities of the Member States, the requirements for the safety of explosive technologies are constantly changing. In recent years, this change has brought with it new risks of a new nature, the nature of which is not yet known. The aim of our research are to investigate how explosion protection safety aspects are prevailed in practice and to identify the causes of the non-compliances found. Our qualitative research was carried out as a retrospective case study. Among our results, we managed to identify patterns in the occurrence of non-compliances, revealing that the reasons for the existence of non-compliances are mainly rooted in human and organisational factors.

Keywords

explosion protection, explosive athmospheres, inspection and maintenance, human and organisation factor

Absztrakt

Az ipari termelési folyamatok gyakran potenciálisan robbanásveszélyes térségeket eredményeznek. A robbanásvédelemmel szemben támasztott biztonsági követelményeket az Európai Unió tagállamai számára kötelező érvényű irányelvekben rögzítik, a célok elérését biztosító eszközöket a tagállamok nemzeti hatóságai alakítják ki, azonban a robbanásveszélyes technológiák biztonságát szabályozó követelményrendszert folyamatos változás jellemzi. Az utóbbi években a változás újszerű, eddig nem létező kockázatokat hozott magával, aminek a természetét még nem ismerjük. Kutatásunk célja a robbanás elleni védelem biztonsági szempontok érvényesülésének vizsgálata a gyakorlatban, a talált nem megfelelőségek okainak azonosítása. Kvalitatív kutatásunkat retrospektív esettanulmányként valósítottuk meg. Eredményeink között sikerült mintákat azonosítani a nem megfelelőségek előfordulásában, feltártuk, hogy a nem megfelelőségek létezésének oka elsősorban az emberi- és szervezeti tényezőkben gyökereznek.

Kulcsszavak

robbanásvédelem, robbanóképes közegek, felülvizsgálat és karbantartás, emberi- és szervezeti tényező

[1] zsarnovszki.attila@stud.uni-obuda.hu | ORCID: 0009-0001-5337-4212 | PhD student, Óbuda University, Doctoral School on Safety and Security Sciences | PhD hallgató, Óbudai Egyetem, Biztonságtudományi Doktori Iskola

[2] elek.barbara@bgk.uni-obuda.hu | ORCID: 0000-0001-7515-6374 | associate professor, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Institute of Safety Science and Cybersecurity | egyetemi docens Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Biztonságtudományi és Kibervédelmi Intézet

BEVEZETÉS

A biztonságtudományoknak számos szakterülete ismert. Az Európai Uniós (EU) tagállamok többségében a robbanás elleni védelem, vagy robbanásvédelem szabályozása a biztonságtechnika két ágazata, a Munkavédelem és a Tűzvédelem kereteiben van kialakítva elsősorban. A szabályozások célja, hogy a potenciálisan robbanásveszélyes ipari technológiák vonatkozásában az élettartamuk során ne következzen be robbanás.

Ez a szabályozási kör és a körülötte kialakított harmonizált szabványok, rendeletek, ágazati irányelvek együttes alkalmazásának keretrendszere egy összetett hatásmechanizmust eredményez, amin keresztül kell kialakítani a védelmi megoldásokat és megvalósítani a robbanás elleni védelmet.

A kutatásunkban tárgyalt probléma megértéséhez szükséges körbejárni néhány robbanásvédelem tárgyköréhez tartozó szakmai alapfogalmat. A robbanásvédelem tárgyában írt publikációkban számos szakkifejezést alkalmaznak. Közérthetően, ugyanakkor kellően szabatosan ismertetik a robbanásvédelem alapelveit, legfontosabb fogalmait [1]. A robbanás elleni védelem hatásmechanizmusának egyik alappillére a veszélyes övezet kiterjedésének és milyenségének a kvantitatív meghatározása, amelyet térségek zónabesorolásának hívnak [2]. A robbanásveszélyes térségekben alkalmazható villamos gyártmányokkal szemben gyártmányvédelmi szintek vannak meghatározva [3], amelyek biztosítják, hogy az egyes gyártmányok a védelmi módjuk által milyen zónában alkalmazhatók. A gyártmányok védelmi módjának megfelelő alkalmazhatóságot szabvány rögzíti a tervezés, kiválasztás és szerelési követelmények szempontjából [4].

A potenciálisan robbanásveszélyes térségekben való alkalmazásra szánt berendezések és védelmi rendszerek alapvetően két jól elkülöníthető feladatot teljesítenek. Egyrészt magas (az átlagos ipari berendezésekhez képest magasabb) működési megbízhatóság mellett látják el feladatukat, másrészt különleges előírásoknak is eleget tesznek [4]. Ez utóbbiak betartásával biztosítható az, hogy különböző meghibásodások előfordulása esetén is a berendezések nem válnak gyújtóforrássá, megakadályozva ezzel az esetlegesen egy azon időben jelenlévő robbanásveszélyes atmoszféra gyújtását. Fontos rögzíteni azonban, hogy a berendezés hibátlan működéséből egyértelműen nem következik az, hogy a berendezés továbbra is robbanásbiztos. Mindezek figyelembevételével jogszabályi alapokon [5] [6] kötelező a robbanásbiztos berendezések és védelmi rendszerek felülvizsgálatainak szakképzett személyzet általi elvégeztetése, hogy a robbanásbiztonság szempontjából alapvető különleges tulajdonságok a teljes élettartam során változatlanul fennálljanak. Az MSZ EN 60079-17:2014 [7] szabványban meg van különböztetve az egyes felülvizsgálatok lehetséges fokozatai, lehetséges típusai, továbbá a követelmények az egyes gyártmányok védelmi módjaival szemben.

A szakirodalmakban főleg a robbanásvédelem hatásmechanizmusát keretező szabályozási rendszert, a keretrendszer alkalmasságának megfelelőségét éri kritika, hol szakmai oldalról [8], hol pedig a felhasználói oldalról [9]. A szakirodalmak egy másik része a robbanásveszélyes térségekben megtalálható nem megfelelőségek egyedi eseteinek problémakörét vizsgálja [10] [11].

Kutatásunk célja annak vizsgálata, hogy szélesebb összefüggéseiben, tehát nem csupán egy-egy esetet elemezve, hanem üzemeken és iparágakon is átívelő szélességben, mintázatok kutatásával és elemzésével kapjunk képet a megvalósított biztonság szintjével

kapocslatban, továbbá kapjunk választ azokra a kérdéseinkre, hogy milyen nem megfelelőségek és miért léteznek a potenciálisan robbanásveszélyes ipari technológiák tekintetében.

SZAKIRODALMI ELEMZÉS

A szakirodalmi elemzés keretében azt vizsgáljuk, hogy melyek az EU tagállamai számára kötelezően alkalmazandó, a témakörben releváns direktívák; ezt követően vizsgáljuk mely nemzeti törvények és/vagy rendeletek emelik e követelményt a hazai jogrendbe. A potenciálisan robbanásveszélyes technológiák műszaki biztonságának teljesülésével kapcsolatban elemezzük, hogy milyen módon van kialakítva a lehetséges megoldások alkalmazásának kötelme az elvárt biztonsági szint teljesülése érdekében. A publikációkban kutatjuk, hogy más kutatók milyen a témakört alátámasztó eredményekre jutottak a robbanásvédelem kialakított hazai és nemzetközi gyakorlati megfelelőségével kapcsolatban.

Az Európai Unió robbanásvédelmi irányelvei

A potenciálisan robbanásveszélyes térségekkel kapcsolatos védelmi intézkedések egységesítésének történelmi gyökerei vannak Európában. Már 1975-ben kialakultak az EU szellemiségében értelmezhető törekvések az egységes műszaki követelmények iránt, ennek eredménye a 76/117/EEC irányelv, a potenciálisan robbanásveszélyes környezetben használt elektromos berendezésekre vonatkozó tagállami jogszabályok közelítéséről [12].

Napjainkban nem számít újnak, a francia „ATmosphère EXplosible” kifejezésből alkotott ATEX mozaikszó, amely az Európai Unió (EU) robbanásvédelmet szabályozó irányelveire utal. Két ATEX-irányelv létezik: az ATEX 114 azaz a 2014/34/EU berendezés irányelv [13] (korábbi nevén ATEX 95, 94/9/EC) a gyártók számára, és az ATEX 153 (99/92/EC) munkahelyi irányelv [14] a potenciálisan robbanásveszélyes munkaterületekkel rendelkező munkáltatókra vonatkozóan.

Az ATEX 114 berendezés irányelv [13] támogatása céljából az Európai Bizottság kidolgozott egy határozatot [15] a robbanásveszélyes légkörben való használatra szánt berendezésekre és védelmi rendszerekre vonatkozóan harmonizált szabványokról, amely 91 szabvány alkalmazását teszi kötelezővé a tagállamok számára.

A magyar robbanásvédelmi alapkövetelmények

Az ATEX 153 munkahelyi irányelvet [14] a Munkavédelmi Törvény 23. §-ának (3) bekezdésében adott felhatalmazás alapján [16] a 3/2003. (III. 11.) FMM–ESZCSM együttes rendelet a potenciálisan robbanásveszélyes környezetben levő munkahelyek minimális munkavédelmi követelményeiről [17] emeli a magyar nemzeti jogrendbe.

Az ATEX 114 berendezés irányelvet a 35/2016. (IX. 27.) NGM rendelet a potenciálisan robbanásveszélyes környezetben történő alkalmazásra szánt berendezések és védelmi rendszerek vizsgálatáról és tanúsításáról [18] vezeti be a nemzeti szabályozásokba.

A potenciálisan robbanásveszélyes környezetben való alkalmazásra szánt gyártmányok, berendezések és védelmi rendszerek teljes élettartama során a robbanás elleni védelem műszaki követelményeknek való megfelelést az Országos Tűzvédelmi Szabályzatról (OTSZ) szóló 54/2014. (XII. 5.) BM rendelet alapján [19] biztosítani kell. Relevanciák (99.§, 276-281.§)

Az egyes veszélyes üzemekre vonatkoznak más szempontú követelmények teljesítési kötelmei is pl. egészségvédelmi, környezetvédelmi stb., de vannak specifikusabb, a biztonsági felülvizsgálatok kötelező elvégzésére vonatkozó előírások is. A kutatásunk szempontjából releváns, és nagy jelentőséggel bír a 40/2017. (XII. 4.) NGM rendelet az összekötő és felhasználói berendezésekről, valamint a potenciálisan robbanásveszélyes közegben működő villamos berendezésekről és védelmi rendszerekről [5]. A rendelet kötelezően előírja a robbanásveszélyes technológiák vonatkozásában új létesítést követően – még az üzembe helyezés előtt –, majd az élettartamuk során időszakosan az ún. villamos biztonsági felülvizsgálatok elvégzését az ipari létesítményekben.

A robbanásvédelem vonatkozásában kutatásunk szempontjából fontos irányelv a TvMI 13.4:2024.02.01. Tűzvédelmi Műszaki Irányelv, Robbanás elleni védelem [20], amelyet a Tűzvédelmi Törvény [21] 3/A. § (2) bekezdése alapján jött létre. Az irányelv alkalmazása önkéntes, azonban annak alkalmazásával az OTSZ [19] robbanás elleni védelemre vonatkozó követelményei teljesülnek.

A potenciálisan robbanásveszélyes térségek műszaki biztonsága szempontjából releváns előírásokat tartalmaz továbbá az OTSZ [19] mellé kiadott műszaki irányelvek sorozatából a TvMI 7.6.:2024.02.01. Tűzvédelmi Műszaki Irányelv, Villamos berendezések, villámvédelem és elektrosztatikus feltöltődés elleni védelem [22], valamint a TvMI 12.5.:2022.06.13. Tűzvédelmi Műszaki Irányelv, Ellenőrzés, felülvizsgálat és karbantartás [6] ebből a sorozatból .

Kutatásunk szempontjából legfontosabb műszaki szabvány az MSZ EN 60079-17 Robbanóképes közegek 17. rész: Villamos berendezések felülvizsgálata és karbantartása (IEC 60079-17:2013) [7], mert ez a szabvány rögzíti a potenciálisan robbanásveszélyes térségekben való alkalmazásra szánt villamos berendezések biztonságtechnikai felülvizsgálatának követelményeit, protokollját a különböző védelmi módú berendezésekre.

A tudományos szakirodalom elemzése

Szakirodalmi elemzésünk keretében ki kell emelnünk, hogy a kutatási témakört érintő hazai és nemzetközi publikációkat induktív gondolkodással elemeztük, mert a témakör más-más kutatók által elért eredményeinek ilyenmódon történő megismerésével, feldolgozásával a megfigyelés tárgyára összpontosíthatunk és ebben kereshetjük a mintákat, így általánosításokat fogalmazhatunk meg.

Kutatási célunk a potenciálisan robbanásveszélyes ipari technológiákkal szemben támasztott biztonságtechnikai követelmények érvényesülésének vizsgálata a gyakorlatban, a nem megfelelőségek lehetséges okainak kutatása, a nem megfelelőségek előfordulásának jellegével, gyakoriságával és milyenségével kapcsolatos tendenciák időbeli alakulásának megállapítása.

A publikációk kutatása során számos eredményt találtunk a közelmúltból és korábbi időszakokról egyaránt. Kutatásunk irányát illesztettük a kutatási területhez, ennek megfelelően a robbanásveszélyes ipari technológiák műszaki megközelítésével foglalkozó, a robbanásvédelmet szabályozó rendelkezéseket tanulmányozó, továbbá a bekövetkezett robbanással járó baleseteket feldolgozó publikációkra fókuszáltunk.

A magyarországi szabályozások robbanásvédelemmel kapcsolatos hatásosságát, a keretrendszer alkalmazásának megfelelőségét számos formában éri kritika. Parádi [9] 2022-ben írt a témakörben az „elmúlt 20 éve és a jövő feladatai” alcímmel. A szerző, mint

igazságügyi szakértő cikkében négy robbanással és emberi sérüléssel vagy halálos kimenetellel járó baleset hazai sajtószalagcímet idézi 2 év idősávból. A robbanás elleni védelem hatásmechanizmusának több szintjén tesz elmarasztaló tapasztalati megállapításokat a szerző, így a tervezéssel, a felülvizsgálatokkal kapcsolatban, de a szabályozás hibái, a hatósági szerepek, az oktatás és üzemeltetés problémái is azonosításra kerülnek. Király et al. [8] Parádihoz hasonlóan, de jobban a szabályozási keretrendszer problémáira fókuszál. A két cikk szerzői hazai, a gyakorlatban található problémákat emelik értekezési, problémafelvetési szintre.

A potenciálisan robbanásveszélyes térségekben való használatra szánt berendezések és védelmi rendszerekkel kapcsolatos szakmai, gyakorlati tapasztalatokra számos nemzetközi publikáció is megtalálható. 2008-ban egy olaj- és vegyipari konferencián Weimarban, Kelava et al. [10], mint robbanásbiztonsági felülvizsgáló számos problémás esetről írt a tervezés, telepítés és karbantartás területeinek vonatkozásában. A szerző által gyakorlatban talált nem megfelelőségi példákon szemlélteti megállapítását, hogy évtizeden át is csak lassan javul a robbanásveszélyes légkörben működő rendszerekkel foglalkozó szakemberek képzettsége, amit fő okaként azonosít a nem megfelelő állapotok létezésére. Ugyanakkor megemlítésre kerülnek szervezetbeli javaslatok is, miszerint a felülvizsgálatot végző személyzetnek kellő mértékben kell függetlennek lennie az üzemeltetésben érintett személyzettől. Egy évtizeddel később, napjainkban egymást érik a hasonló tartalmú, különféle konferenciákon bemutatott tapasztalatok. [11] [23] A jelen bekezdésben vizsgált publikációknak van egy párhuzama, miszerint mindössze egy-egy példák általi gyakorlatban talált nem megfelelőségekről számolnak be. Ezekhez hasonló konferencia előadás és cikk készült általunk is [24], ahol a talált állapotokban mintaszerűséget azonosítottunk, amit összefüggésbe hoztunk személyi is szervezeti tényezőkkel.

A szabályozások problémáját kutató értekezések szintén megtalálhatók a nemzetközi publikációk vonatkozásában is. Andris et al. [25] egy 2023-as Romániában megtartott munkavédelmi és biztonságtechnikai konferencián beszámol kutatásának eredményéről, miszerint a szabványok korszerűsítésével a műszaki megoldások összetettsége is növekszik, aminek alkalmazása a szabályozás részleteinek növelésével jár, és új robbanásvédelmi műszaki megoldásokat vezetnek be. A cikk szerzői a robbanási kockázat elemzésének érvelésében azonosítják, hogy a robbanásveszélyes légkörben való használatra szánt berendezések és védelmi rendszerek robbanásvédelmének megfelelősségét három tényező befolyásolja, nevezetesen:

- tervezési, összeszerelési és üzembe helyezési tevékenységek
- használati/üzemeltetési, ellenőrzési és karbantartási tevékenységek, továbbá
- olyan környezeti tényezők, mint a páratartalom, a hőmérsékleti tartomány, a maró anyagok és a por jelenléte

A cikkben megjelenő gondolattal egyetértünk, amely a személyi tényezők robbanásvédelemre befolyással bíró szerepét jeleníti meg egy grafikus ábrán. Az ábra segítségével válik szemléletessé és azonosíthatóvá, hogy kutatásunk vezérfonalában hangsúlyt kell fektetnünk az emberi tényezőkre, mint a robbanásvédelem megfelelőségére ható befolyásoló tényezőre a pusztán műszaki vagy környezeti tényezők mellett.

A személyi- és szervezeti tényezők azonosítása és figyelembevétele a robbanásvédelem területén újszerűnek számít. 2020-ban Geng at el. [26] egy eljárást dolgoztak ki,

ATEX (robbanásveszélyes légkör) kockázatértékelésre. A szerző véleménye és saját tapasztalatunk szerint is, annak ellenére, hogy a potenciálisan robbanásveszélyes térségekben számos munkavégzés történik, az emberi- és szervezeti tényezők (ESZT) hatásait az ATEX kockázatértékelés során többnyire figyelmen kívül hagyják. A cikkben ismertetett integrált módszertan két probléma megoldására tesz javaslatot: (1) a ESZT-hatás azonosítása az ATEX kockázatértékelésre, és (2) a ESZT-hatás számszerűsítése. A javasolt módszertan gazdagítja a hagyományos ATEX kockázatértékelési eljárást, amely négy lépésből áll: (1) zónabesorolás, (2) gyújtóforrás azonosítás, (3) kárelemzés és (4) ATEX kockázatértékelés. A cikkben rögzített módszertan alkalmazása, és az ESZT figyelembevétel a tervezési folyamatok során bizonyára jelentős előrelépést hozhat a kialakítandó robbanás elleni védelem mibenlétére.

KUTATÁSI CÉLOK MEGHATÁROZÁSA

A szakirodalmi elemzés alapján arra a következtetésre jutottunk, hogy a robbanás elleni védelem tárgyköre interdiszciplináris tudományterületet jelent. Megállapítottuk, hogy egy lehetséges robbanás elkerülésére tett törekvéseink párhuzamosan irányulnak az egyes diszciplínákra, ugyanakkor a védekezés hatásmechanizmusában kizárólag együttesen alkalmazva tudják kifejteni hatásukat. Az egyes tudományágak egymásba kapcsolódásával alakítható ki és így is van kialakítva a műszaki biztonság elvárt szintje a potenciálisan robbanásveszélyes térségek vonatkozásában.

Annak ellenére, hogy a robbanásvédelemmel kapcsolatos szakirodalmak bővelkednek a biztonság nem megfelelő szintjének különféle jelenlétével az ipari robbanásveszélyes technológiák gyakorlati alkalmazásában, még hiányoznak azok a kutatások, amelyek az egyes üzemekben a gyakorlatban létező robbanásbiztonsági állapotképet teljeskörűen volna képes meghatározni. A tanulmányok többségében beazonosításra kerül a robbanásbiztos berendezés vagy védelmi rendszer állapotának nem megfelelősége, részleteiben elemzik az adott egy-egy probléma mibenlétét. Azonban a teljes terjedelemben történő vizsgálati módszerek kidolgozása, adatok vizsgálata elmarad, amelyek segítségével a nem megfelelő biztonsági állapotok kialakulásának mibenlétét, okait, összefüggéseit volna lehetőség tovább vizsgálni.

KUTATÁSI KÉRDÉSEK

A potenciálisan robbanásveszélyes ipari technológiák biztonságtechnikai szempontjainak érvényesülésével kapcsolatban kutatási rést azonosítunk, aminek vizsgálatára az alábbi kutatási kérdéseket (KK) állítjuk fel.

- **KK1:** Miféle a robbanásvédelmet befolyásoló nem megfelelőségek vannak a különböző ipari létesítményekben?
- **KK2:** Miért alakulnak ki az egyes nem megfelelősségek a potenciálisan robbanásveszélyes térségekben való alkalmazásra szánt berendezések és védelmi rendszerek gyakorlati alkalmazásának vonatkozásában?
- **KK3:** Milyen arányban fordulnak elő az emberi- és szervezeti tényezők, valamint az ezektől független tényezők egymáshoz képest a nem megfelelőségek okaiban?

Kutatásunk fontos célja, hogy más okból gyűjtött nagymennyiségű tényadatok utólagos szempontok szerinti (szekunder) elemzésével legyünk képesek megállapítani az egyes üzemek nem megfelelőségei mögött meghúzódó okok közül melyek és milyen arányban függenek az emberi- és szervezeti tényezőktől, és mennyi előfordulással és milyen arányban találunk az ezektől független okra visszavezethető nem megfelelőségeket.

A KUTATÁSI MÓDSZERTAN

A kutatási módszertan kiválasztása során alapirányt adnak a szakirodalmi elemzés publikációinak módszertanai, amelyek jórészt esettanulmány formájában, időben visszatekintő, elemző módszerként valósultak meg. Egyet kell értenünk Incze [27] doktori értekezésének módszertani megközelítésével, miszerint a természet jelenségeit meg lehet magyarázni, ugyanakkor a viselkedés jelenségei csak megérthetők. Kutatásunkhoz olyan módszertant kellett választanunk, amely lehetővé teszi a nagyobb (több ezer) és kisebb (néhány száz) mennyiségű adatok feldolgozását is, ugyanakkor biztosítja a szabadabb megközelítést. Az esettanulmány módszere Incze [27] értekezése szerint főként a való életből vett gyakorlati jelenségek vizsgálatára alkalmas, ahol az eseményeket a kutató nem tudja befolyásolni (külső megfigyelői szerepben van), és alkalmas a hogyan? vagy a miért? jellegű kérdések megválaszolására. Kutatásunk megértésorientált, így a retrospektív jelleg hozzájárul a rendelkezésünkre álló nagy mennyiségű adat feldolgozásához. A kutatás alapvetően kvalitatív és kvantitatív megközelítést egyaránt alkalmaz. Ez a módszertan előnyös lehet, mert egyfelől lehetővé teszi a számszerű adatok elemzését, másrészt az adatok mögötti tényezők megismerését [28] [29]

A retrospektív esettanulmány módszertan kedvez a mélyebb megértésnek, és az okokozati összefüggések megállapítását is támogatja. A robbanás elleni védelem vonatkozásában kutatandó robbanásbiztonság-technikai nem megfelelőség esetei összetett jelenségek, emiatt részletekbe menő minőségi adatok összegyűjtésére és kvalitatív elemzésére törekszünk.

A potenciálisan robbanásveszélyes térségekben való alkalmazásra szánt villamos berendezések gyártóira, tervezőire, de az üzemeltetőkre is számos kötelező előírás, rendelet és szabvány alkalmazása vonatkozik. A kutatási kérdéseink megválaszolására az alapadatok halmazát az MSZ EN 60079-17:2014 Robbanóképes közegek: 17. rész: Villamos berendezések felülvizsgálata és karbantartása [7] c. szabvány által keretezett, felülvizsgálati és javító tevékenységek eredményeként korábban létrejött adatbázisok (vizsgálati eredmények, fényképek, feljegyzések) szolgáltatják. A szabványban rögzített felülvizsgálati protokoll részletes iránymutatást ad az egyes védelmi módok vizsgálati szempontjaira, és a felülvizsgálat fokozatának megfelelő részletességű ellenőrzési- és vizsgálati feladatokra. Ezeknek az adatoknak az elemzésével kutatjuk, hogy miféle nem megfelelőségek létezhetnek egyáltalán. A minták mindegyikének szabvány szerint típusa időszakos, amelyek 3 év elteltével ciklikusan ismétlődnek, fokozata jellemzően szemrevételezéses, ritkán közeli vagy részletes.

A szabvány a különféle védelmi módokhoz és a felülvizsgálat fokozatához illesztett felülvizsgálati programot rögzít. A felülvizsgálatok gyakorlati alkalmazásakor az ezekben a programokban írt feladatokat kell elvégeznie a képzett felülvizsgálónak az egyes helyszínen minden egyes gyártmány vonatkozásában, az adatokat fel kell jegyezni és vizsgálati

jelentésben kell dokumentálni. A nem megfelelőségek dokumentálása a vizsgálataink esetén a felülvizsgálati program táblázatának minden sorához rendel egy rövid kódot, amely kóddal vannak az adott gyártmány hibái azonosítva, és a nem megfelelősséget későbbi javító tevékenységet segítendő fényképpel, és feljegyzésekkel kerül további felvételre.

A jelentéseknek a minősítő részében a gyakorlati szempontok alapján a nem megfelelt állapotokat két fokozatban állapítja meg felülvizsgáló:

- **Súlyos**: a robbanás elleni védelem állapota súlyosan sérült, közvetlen gyújtásveszély van, a berendezést potenciális gyújtóforrás helyett hatásos gyújtóforrásként kell tekinteni, azonnali intézkedés szükséges,
- **Karbantartás**: a robbanás elleni védelem állapota biztonság szempontjából nem jelent közvetlen gyújtásveszélyt, de a támasztott követelményeknek nem tesz eleget maradéktalanul, így karbantartási feladat keretében a problémát adott időn belül el kell hárítani.

A felülvizsgálati adatok elemzésekor elvégeztünk egy kategorizálást, amely logikus következtetéssel meghatározta, hogy az adott hibakódnak megfelelő hiba származása milyen okra vezethető vissza:

- **Környezeti:** amely magában foglalja a berendezések természetes elhasználódásból történő avulást, állapotromlást, a környezeti tényezők hatásait
- **Emberi- és szervezeti:** amely magában foglalja az egyes emberek által végzett feladatkörökben való mulasztások, tévedések, szervezés béli anomáliák, hiányosságok bármely előfordulását
- **Bármely:** amely esetekben a nem megfelelőség előfordulhat egyik vagy másik okból egyaránt

A KUTATÁSI MINTA BEMUTATÁSA

A kutatás jelen keretében 10 minta kiválasztásáról döntöttünk. A minták származását tekintve saját munkánk eredményeiből az elmúlt 7 évből választottunk ki 10 komplett üzem robbanásbiztossági felülvizsgálati eredményét. Az üzemek mindegyike Magyarországon üzemelő potenciálisan robbanásveszélyes ipari technológia, amelyek széles spektrumát érintik a különböző iparágaknak. A kiválasztható eseteink közül elérhető esetszámok tekintetében akár a néhány száz darabszámú kis rendszerek, de a többezertől a húszezer eszközt tartalmazó nagyüzemig terjed a paletta. Törekvésünk szerint a tíz minta legyen különböző a felülvizsgálat alá vont gyártmányok darabszáma és az iparág szempontjából, továbbá az időbelisége is legyen eltérő. A kutatási minta főbb adatainak részleteit és összesítését az 1. táblázatban ismertetjük.

Srsz.	Iparág megnevezése	Vizsgálat ideje [év]	Robbanásbiztos kivitelű eszközök száma [db]
1	Vegyipari üzem	2021	5 366
2	Élelmiszeripari feldolgozó	2021	853

Srsz.	Iparág megnevezése	Vizsgálat ideje [év]	Robbanásbiztos kivitelű eszközök száma [db]
3	Gabonafeldolgozó üzem	2024	685
4	Erőmű	2022	160
5	Petrolkémiai üzem	2022	21 172
6	Kőolaj- és földgázbányászat	2017	1 744
7	Hűtőgépgyár	2022	886
8	Gázüzem	2019	9 159
9	Olajtechnológia	2018	237
10	Kokszoló	2018	2 362
11	**Robbanásbiztos berendezések összesen**		**42 624**

1. Táblázat: Kutatási minta ismertetése, saját szerkesztés.

KUTATÁSI EREDMÉNYEK

A kutatási eredményeket a kutatási kérdések mentén mutatjuk be. Az elsődleges mennyiségi adatok feldolgozását követően két eredményt vizsgálunk kvalitatív:

- A teljes robbanásbiztos berendezések vizsgálati mintákból mennyi a nem megfelelőségek aránya, továbbá mi a súlyos és karbantartásos hibák egymáshoz és a teljes egészhez való viszonya?
- Milyen hibákat rögzítettek egyáltalán a felülvizsgálatok alkalmával, és az egyes hibákból vannak-e mintaszerűen előforduló hibák?

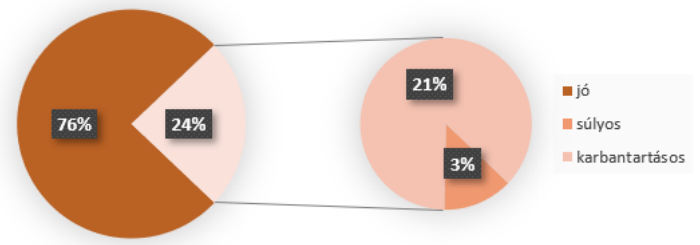
Az alábbi 2. táblázatban rögzítettük a talált hibák mennyiségi kimutatását, továbbá annak megoszlását a súlyos és karbantartásos hibák között.

Srsz.	Iparág	Robbanásbiztos kivitelű eszközök száma [db]	Hibák összesen [db]	Súlyos [db]	Karbantartásos [db]
1	Vegyipari üzem	5366	317	42	275
2	Élelmiszeripari feldolgozó	853	413	101	312
3	Gabonafeldolgozó üzem	685	171	5	166
4	Erőmű	160	56	5	51
5	Petrolkémiai üzem	21172	4674	265	4409
6	Kőolaj- és földgázbányászat	1744	255	126	129

Srsz.	Iparág	Robbanásbiztos kivitelű eszközök száma [db]	Hibák összesen [db]	Súlyos [db]	Karbantartásos [db]
7	Hűtőgépgyár	886	489	162	327
8	Gázüzem	9159	1514	198	1316
9	Olajtechnológia	237	23	6	17
10	Kokszoló	2362	1632	488	1144
11	**Robbanásbiztos berendezések összesen**	**42624**	**9544**	**1398**	**8146**

2. Táblázat: Kutatási eredmények, saját szerkesztés.

Az 1. ábra megmutatja, hogy a potenciálisan robbanásveszélyes üzemek 10 kiválasztott mintájának elemzését követően a 42 624 db üzemelő berendezéséből robbanásbiztossági szempontból minden negyedik érintett, ebből a közvetlen hatásos gyújtóforrásként azonosított nem megfelelőségek mennyisége 3%.

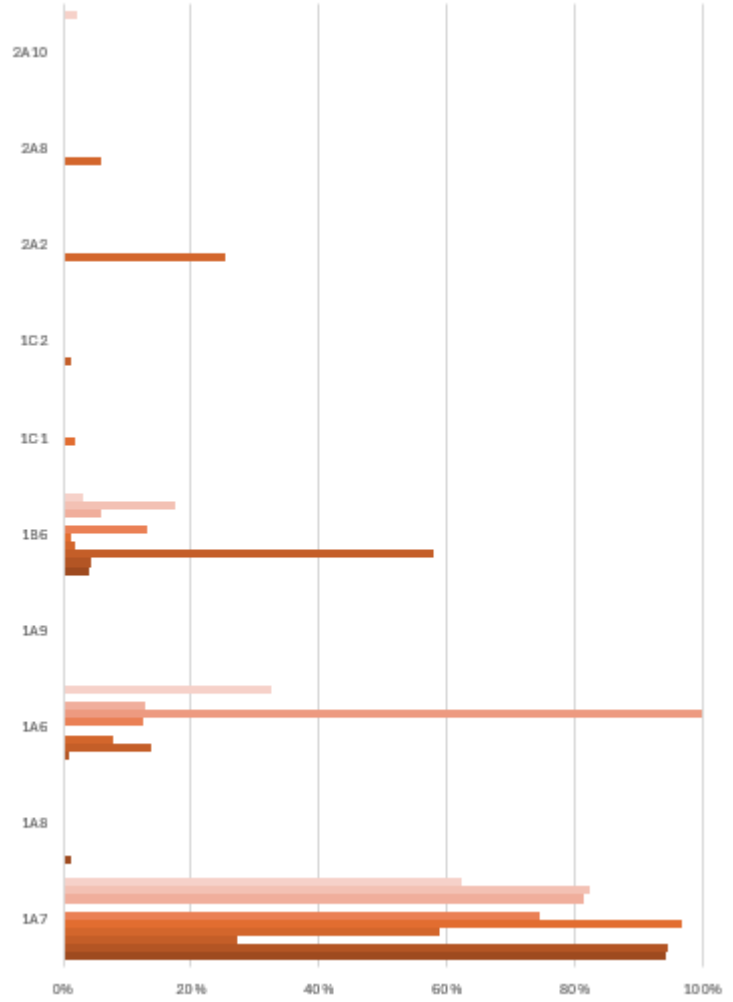


1.Ábra: Kutatási eredmények százalékos áttekintése, saját szerkesztés

Az alábbiakban ismertetjük miféle hibák fordulnak elő konkrétan a mintánkban. A felülvizsgálati szabvány [7] alapján képzett lehetséges hibák száma 116 db. A lehetséges hibákat rövid kódokkal azonosítjuk, az alábbi 2. ábrán az előfordult karbantartásos hibák előfordulását ábrázoljuk sávdiagrammon. Az egyes üzemekben az előfordulások egymáshoz képest viszonyított százalékos ábrázolását alkalmazzuk.

Az ábra alapján rögzíthetjük, hogy az előfordulható hibák mindössze 10 tétele jelenik meg, ebből is mindössze 3 mutat mintaszerű ismétlődést, a többi inkább szórványos, eseti jelleggel fordult csak elő. 1A7 hibakódra vonatkozó vizsgálati kérdés: „A gyártmány áramköreinek azonosítói rendelkezésre állnak”, 1A6 hibakód vizsgálati kérdése: ” A gyártmány áramköreinek azonosítása megfelelő”. Az 1B6 hibakód vizsgálati kérdése: „A földelés csatlakozásai, beleértve bármilyen kiegészítő földelés csatlakozásait is, kielégítők (pl. a csatlakozások szorosak és a vezetők keresztmetszete megfelelő)”. Kutatásunk további elemzésénél az elszórtan előforduló hibák vonatkozásában megállapítható, hogy az emberi- és

szervezeti tényezőkre visszavezethető okból jöttek létre vagy állnak fenn. Az 1B6 földelőcsatlakozó jóságára vonatkozó elemzésünkben, kiértékeltük a tervezés, létesítés, üzemeltetés és karbantartás kötelmeit, továbbá vizsgáltuk a fényképeket és feljegyzéseket. Arra a következtetésre jutottunk, hogy az 1B6 hibakód által rögzített nem megfelelőség létrejöttének hátterében az emberi tényező áll. Az 1A6 és 1A7 hibakódok esetében olyan gyakorlati előfordulásokat soroltak a felülvizsgálók e kategóriába, mint tervjel vagy adattábla hiányzik, tervjel vagy adattábla nehezen olvasható.

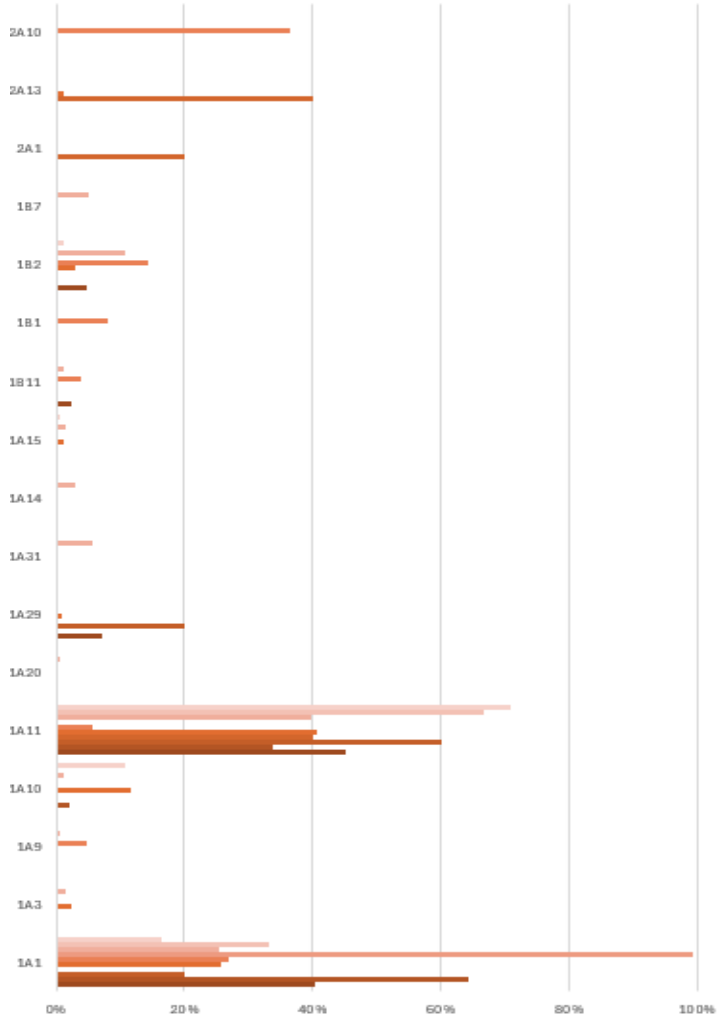


2.Ábra: Karbantartásos hibák előfordulásának százalékos megjelenítése, saját szerkesztés

Könnyen belátható, hogy pusztán az azonosítók hiánya, ha egyébként a felülvizsgáló más eszközeivel minden kétséget kizáróan tudja azonosítani a gyártmányt és ki tudja értékelni a szükséges szempontok alapján, úgy az nem jelent közvetlen gyújtásveszélyt, ugyanakkor feljegyzi karbantartásos hibának, mert a vonatkozó azonosítási követelményeknek a robbanásbiztonsági szempontok alapján nem felel meg. Ha ez a hiba tovább romlik,

úgy azonosíthatatlanná válhat, amely egy következő felülvizsgálat alkalmával már a súlyos hibák közé értékeli ugyanezt a berendezést. Mind a tervjelek, mind az adattáblák fényképeinek a vizsgálatával arra kerestük a választ, hogy annak az előfordulása mely tényezőre vezethető vissza? Néhány eset egyértelmű, pl. nincs adattábla vagy tervjel, vagy le van festve, ezek csak emberi tényezők miatt lehetségesek. A nem olvashatóság már inkább a felhasznált adattábla vagy tervjel azonosító gyártóra vonatkozó minőségére, az agresszív környezetre vezethető vissza, ezeket a helyzeteket pedig a környezeti tényezők okán azonosítjuk.

Vizsgáljuk meg a súlyos hibák mibenlétét, szintén a százalékos eloszlás ábrázolásában. A 3. ábra a súlyos hibák előfordulásának százalékos megjelenítését ábrázolja.



3.Ábra: Súlyos hibák előfordulásának százalékos megjelenítése, saját szerkesztés.

A súlyos hibák vonatkozásában is mintaszerűen megjelenő nem megfelelőségeket találunk. Az 1A1 hiba vizsgálati kérdése: „A gyártmány megfelel a telepítési helyére vonatkozó EPL/zóna követelményeknek", míg az 1A11 jelentése: „Csavarok, (közvetlen és közvetett) kábelbevezető eszközök és lezáróelemek megfelelő típusúak, sértetlenek és nincsenek kilazulva". Mindkét hiba előfordulása tömeges, jellemző, ez a két hiba kiteszi az összes előforduló súlyos hiba 77%-át. Az 1A1 hiba elemzésünk során az alábbi lehetőségek során léphet fel:

- A gyártmány egyszerűen nem robbanásbiztos kivitelű (ez akkor fordul elő, ha az üzem területén változás történik, és a korábban normál ipari térségnek tekintett üzemrészt robbanásveszélyes térséggé kell átsorolni, de a korábban ott lévő berendezéseket nem kezelik megfelelően)
- Robbanásbiztos kivitelű, de nem felel meg az adott készülékkategória követelményeinek
- Az adattáblája megsemmisült, így a felülvizsgáló nem tudja beazonosítani és ezt a minősítést kell dokumentálja

Akármelyik előfordulás történik, ezeket minden esetben emberi- és szervezeti tényezőkre tudtuk visszavezetni.

Az 1A11 hibakód esetének döntő többsége nem az adott védelmi mód működésében szerepet játszó pl. nyomásálló tokozat csavarjának elvesztése adja ki, hanem a kábelbevezetők hiánya, sérülése, kábelméretek hibája stb. Ezek a hibák nem fordulnak elő környezeti tényező okán, csak a személyzet által alakítható ki. A 2A10, 2A13 és a 2A1 előfordulások vizsgálatakor arra a következtetésre jutottunk, hogy ugyan az adott üzemben nagy arányú 20-40% előfordulási arányt tesznek ki, de ezek mégis eseti, adott helyen kialakult emberi mulasztásból létrejövő mintázat szerinti okra vezethető vissza.

ÖSSZEGZÉS

Kutatásunkban adatokat elemeztünk a robbanásveszélyes ipari technológiákon előforduló nem megfelelőségekkel kapcsolatban. Elsőként szakirodalmi elemzéssel vizsgáltuk, hogy a jogszabályi keretrendszer hatásmechanizmusa, illetve előforduló nem megfelelőségek között milyen összefüggések ismerhetők meg. Kutatási rést azonosítottunk, ami alapján vizsgáltuk egyáltalán miféle nem megfelelőségek vannak az üzemelő technológiákban aktuálisan, mi okból alakulnak azok ki, és milyen arányban vannak a környezeti vagy emberi- és szervezeti okok.

Kutatásunkban alkalmazott vizsgálat eredménye alapján elmondható, hogy a potenciálisan robbanásveszélyes technológiákon nagy arányban fordulnak elő különféle súlyú nem megfelelőségek. A nem megfelelőségek tömeges előfordulása mintaszerű és kevés változatban azonosíthatók. Ha ezektől eltérő – nem mintaszerű de – nagy esetszámú nem megfelelőségeket találunk egy-egy üzemben, megállapítható, hogy a hibák efféle tömeges és jellemző előfordulások okai elsősorban emberi- és szervezeti tényezőkre vezethetők vissza. A nem megfelelőségek elkerülésére a személyzet, továbbá a teljes robbanásvédelemmel kapcsolatban tevékenységet folytató szakemberek, döntéshozók és döntési mechanizmusok (szervezeti működési folyamatok) fejlesztése a célravezető.

Kutatásunkat a retrospektív esettanulmány módszerével egy-egy üzem adott időben való mintájával folytattuk le. A kutatási munkánkat az adatok elemzésének longitudinális

kiterjesztésével, azaz egy azon üzem több, egymást követő hároméves ciklusokból vett adatok ugyanilyen elemzésével célszerű kibővíteni. Ennek várható eredményeként egy adott üzem állapotváltozásáról kaphatnánk részletesebb képet, aminek segítségével lehetőség lenne vizsgálni egy üzem élettartama során lezajló robbanásbiztonsági állapotváltozás összefüggéseit. További kutatási potenciál az egyes emberi- és szervezeti tényezők, pontosabban az egyes munkafolyamatok és munkatársak kapcsolatrendszerének hálózattudományi megközelítésével történő vizsgálata a biztonságtechnikai szempontok érvényesülésének szempontjából.

FELHASZNÁLT IRODALOM

[1] O. Teruhito, M. Satoru, és F. Takashi, „Quantitative classification of equipment protection level in concept of zone classification with downtime of protective measures”, *Journal of Loss Prevention in the Process Industries*, köt. 89, 2024, doi: https://doi.org/10.1016/j.jlp.2024.105322.

[2] MAGYAR SZABVÁNYÜGYI TESTÜLET, „MSZ EN IEC 60079-10-1 Robbanóképes közegek 10-1. rész: Térségbesorolás. Robbanóképes gázközegek (IEC 60079-10-1:2020)”. 2021.

[3] R. Wilson és G. W. Lawrance, „Equipment protection levels (EPLs), equipment categories and area certification markings for zone classified locations”, előadás 2017 Petroleum and Chemical Industry Technical Conference (PCIC), Calgary, AB, Canada, 2017.

[4] MAGYAR SZABVÁNYÜGYI TESTÜLET, „MSZ EN 60079-14 Robbanóképes közegek. 14. rész: Villamos berendezések tervezése, kiválasztása és szerelése (IEC 60079-14:2013)”. 2014.

[5] Nemzetgazdasági Miniszter, *40/2017. (XII. 4.) NGM rendelet az összekötő és felhasználói berendezésekről, valamint a potenciálisan robbanásveszélyes közegben működő villamos berendezésekről és védelmi rendszerekről*. 2024.

[6] OTSZ, *TvMI 12.5.:2022.06.13. Tűzvédelmi Műszaki Irányelv, Ellenőrzés, felülvizsgálat és karbantartás*. 2022.

[7] MAGYAR SZABVÁNYÜGYI TESTÜLET, „MSZ EN 60079-17 Robbanóképes közegek 17. rész: Villamos berendezések felülvizsgálata és karbantartása (IEC 60079-17:2013)”. 2014.

[8] L. Király, Á. Restás, és Z. Címer, „ROBBANÁSVÉDELEM SZABÁLYOZÁSI JAVASLATA MAGYARORSZÁGON”, *Védelem Tudomány*, sz. III. évfolyam 3. szám, o. 50–64, 2018.

[9] E. Parádi, „A robbanásbiztonság-technika elmúlt 20 éve és a jövő feladatai”, *Villanyszerelők Lapja*, sz. XXI. évfolyam, 10. szám, o. 28–33, 2022.

[10] M. Kelava, I. Gavranic, és J. Deskin, „Practical experience with inspection in plants at risk of explosive atmospheres”, előadás 5th Petroleum and Chemical Industry Conference Europe - Electrical and Instrumentation Applications, Weimar, 2008. [Online]. Elérhető: https://www.researchgate.net/publication/4350478_Practical_experience_with_inspection_in_plants_at_risk_of_explosive_atmospheres

[11] T. Csaszar, S. Burian, C. Colda, és E. Ghicioi, „Practical aspects regarding the evaluation of explosion protected equipment”, előadás MATEC Web of Conferences,

UNIVERSITARIA SIMPRO 2021, 2021. [Online]. Elérhető: https://doi.org/10.1051/matecconf/202134201011

[12] EURÓPAI KÖZÖSSÉGEK TANÁCSA, *76/117/EEC irányelv, a potenciálisan robbanásveszélyes környezetben használt elektromos berendezésekre vonatkozó tagállami jogszabályok közelítéséről*. 1975.

[13] EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA, *2014/34/EU irányelv, a robbanásveszélyes légkörben való használatra szánt felszerelésekre és védelmi rendszerekre vonatkozó tagállami jogszabályok harmonizációjáról (átdolgozás)*. 2016.

[14] EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA, *1999/92/EK irányelv, a robbanásveszélyes légkör kockázatának kitett munkavállalók biztonságának és egészségvédelmének javítására vonatkozó minimumkövetelményekről*. 2000.

[15] EURÓPAI BIZOTTSÁG, *2022/1668 EU végrehajtási határozat, a robbanásveszélyes légkörben való használatra szánt felszerelésekre és védelmi rendszerekre vonatkozóan a 2014/34/EU európai parlamenti és tanácsi irányelv támogatása céljából kidolgozott harmonizált szabványokról*. 2022.

[16] Országgyűlés, *1993. évi XCIII. törvény a munkavédelemről*. 2024.

[17] FMM–ESZCSM, *3/2003. (III. 11.) FMM–ESZCSM együttes rendelet a potenciálisan robbanásveszélyes környezetben levő munkahelyek minimális munkavédelmi követelményeiről*. 2008.

[18] Nemzetgazdasági Minisztérium, *35/2016. (IX. 27.) NGM rendelet a potenciálisan robbanásveszélyes környezetben történő alkalmazásra szánt berendezések és védelmi rendszerek vizsgálatáról és tanúsításáról*. 2021.

[19] Belügyminisztérium, *54/2014 BM rendelet az Országos Tűzvédelmi Szabályzatról*. 2022.

[20] OTSZ, *TvMI 13.4:2024.02.01. Tűzvédelmi Műszaki Irányelv, Robbanás elleni védelem*. 2024.

[21] Országgyűlés, *1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról*. 2024.

[22] OTSZ, *TvMI 7.6.:2024.02.01. Tűzvédelmi Műszaki Irányelv, Villamos berendezések, villámvédelem és elektrosztatikus feltöltődés elleni védelem*. 2024.

[23] S. Burian, „General consideration regarding fault – find, tests and maintenance in the installations in hazardous areas”, előadás MATEC Web of Conferences, UNIVERSITARIA SIMPRO 2021, 2022. [Online]. Elérhető: https://doi.org/10.1051/matecconf/202237300019

[24] A. Zsarnovszki és B. Elek, „Changes in the Safety Level of Potentially Explosive Industrial Technologies in Practice”, *PCS Science 2023*, o. 57–69, 2023.

[25] A. Adriana és S. Burian, „Dynamics of the standardization process for explosive atmospheres”, előadás MATEC Web of Conferences, 11th International Symposium on Occupational Health and Safety (SESAM 2023, 2024. [Online]. Elérhető: https://doi.org/10.1051/matecconf/202438900052

[26] J. Geng, S. Muré, M. Demichela, és G. Baldissone, „ATEX-HOF Methodology: Innovation Driven by Human and Organizational Factors (HOF) in Explosive Atmosphere Risk Assessment”, *Safety 2020*, köt. 6, sz. 1, o. 21, 2020, doi: https://doi.org/10.3390/safety6010005.

[27] E. Incze, „A multinacionálissá válás útjai Magyarországon – a vállalatok nemzetköziesedésének időbeni alakulása”, in *PhD Disszertáció*, Budapesti Corvinus Egyetem, 2010, o. 200. [Online]. Elérhető: https://phd.lib.uni-corvinus.hu/607/

[28] A. Kelemen-Erdős, „Measuring Railway Market Attractiveness: Evidence from Visegrád Countries”, *Acta Polytechnica Hungarica*, köt. 8, sz. 5, o. 151–170, 2011.

[29] A. Kelemen-Erdős, „Sustainable public transport: A CentralEuropean Study”, *Periodica Polytechnica Social and Management Sciences*, köt. 20, sz. 2, o. 81–90, 2012, doi: 10.3311/pp.so.2012-2.03.

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